PHILIPP HACKER

Datenprivatrecht

Jus Privatum
244

Mohr Siebeck

JUS PRIVATUM

Beiträge zum Privatrecht

Band 244

Philipp Hacker

Datenprivatrecht

Neue Technologien im Spannungsfeld von Datenschutzrecht und BGB

Mohr Siebeck

Philipp Hacker, geboren 1985; Studium der Rechtswissenschaften, Philosophie und Neueren deutschen Literatur in München und Salamanca; 2014 LL.M., Yale Law School; 2016 Promotion, Humboldt-Universität zu Berlin; 2016/17 Max Weber Fellow, Europäisches Hochschulinstitut, Florenz; 2017/18 A.SK Fellow, Wissenschaftszentrum Berlin; 2019/20 AXA Postdoctoral Fellow, Humboldt-Universität zu Berlin; 2020 Habilitation, Humboldt-Universität zu Berlin; seit 9/2020 Inhaber des Lehrstuhls für Recht und Ethik der digitalen Gesellschaft, Europa-Universität Viadrina, European New School of Digital Studies.

Gefördert durch die Deutsche Forschungsgemeinschaft (DFG) – 452321320.

ISBN 978-3-16-159617-9 / eISBN 978-3-16-159618-6
DOI 10.1628/978-3-16-159618-6

ISSN 0940-9610 / eISSN 2568-8472 (Jus Privatum)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *http://dnb.dnb.de* abrufbar.

Das Buch wurde von epline in Böblingen aus der Stempel-Garamond gesetzt, von Gulde Druck in Tübingen auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Spinner in Ottersweier gebunden.

Printed in Germany.

Für Lena, Tim und Clara

Vorwort

Daten werden zu einem immer gewichtigeren Teil aller Austauschprozesse. In rechtlicher Hinsicht bedingt dies einerseits, dass das unionale Datenschutzrecht tief in das mitgliedsstaatliche Privatrecht hineinragt. Umgekehrt wirkt dieses aber, zumal wenn es unionsrechtlich harmonisiert ist, auch vielfältig auf das Datenschutzrecht zurück. Die vorliegende Arbeit vermisst dieses Spannungsfeld. Dabei fokussiert sie sich auf drei Basistechnologien: Tracking-Instrumente, künstliche Intelligenz und das Internet der Dinge. Sie lag im Sommersemester 2020 der Juristischen Fakultät der Humboldt-Universität zu Berlin als Habilitationsschrift vor. Das Manuskript ist auf dem Stand von Mai 2020.

Entscheidende Impulse hat die Arbeit von einer Reihe von Personen und Institutionen erhalten. Mein Dank gilt dabei in erster Hinsicht meinem akademischen Lehrer, Herrn Professor Stefan Grundmann, der mir für diese Untersuchung nicht nur alle erdenklichen Freiheiten gewährt hat, sondern auf dessen Freundschaft und umsichtigen Rat in allen Dingen ich jederzeit zählen konnte und kann. Dass wir nicht nur einige Jahre in Berlin, sondern auch ein Jahr in Florenz am Europäischen Hochschulinstitut gemeinsam verbringen konnten, war eine glückliche Fügung, welche die Forschung in meiner Postdoktorandenzeit sehr befördert hat. Herrn Professor Axel Metzger danke ich herzlich für die äußerst zügige Erstellung des Zweitgutachtens und wertvolle inhaltliche Hinweise. Insgesamt konnte ich aus dem Schwerpunkt, den die Juristische Fakultät der Humboldt-Universität zu Berlin auf die Erforschung der Digitalisierung legt, zahlreiche Anregungen mitnehmen, etwa aus Gesprächen mit Herrn Professor Lars Klöhn, Frau Professorin Eva Inés Obergfell, Herrn Professor Gerhard Wagner und Herrn Professor Herbert Zech sowie mit meinen Co-Habilitanden, Dr. Michael Denga, Frau Professorin Linda Kuschel, Dr. Jan-Erik Schirmer, Dr. Sven Asmussen und Dr. Valentin Jentsch.

Meine eigene Forschungstätigkeit im Schnittbereich von Recht und Technologie hat von einer Reihe von Förderungen profitiert, für die ich überaus dankbar bin. Forschungsstipendien der Humboldt-Universität, des Europäischen Hochschulinstituts und des Wissenschaftszentrums Berlin sowie Forschungsprojekte am University College London haben mir eine vertiefte und interdisziplinäre Beschäftigung mit den rechtlichen Herausforderungen digitaler Technologien ermöglicht. Dass die Arbeit selbst im Jahr 2019 zügig niedergeschrieben werden konnte, verdanke ich einem AXA Postdoctoral Fellow-

ship, mit dem ich an die Humboldt-Universität zurückkehrte. Der DFG danke ich für die Gewährung einer Publikationsbeihilfe, der Deutschen Stiftung für Recht und Informatik für die Auszeichnung dieser Arbeit mit dem DSRI-Wissenschaftspreis.

Zahllose Gesprächspartner haben die Arbeit und meine Forschung in dieser Zeit überaus befruchtet. Herr Professor Klaus Hopt hat meinen Werdegang immer wieder mit umsichtigen Ratschlägen begleitet. Gleiches gilt für Herrn Professor Hans-W. Micklitz, Herrn Professor Klaus Ulrich Schmolke und Herrn Professor Mattias Kumm. Frau Professorin Marietta Auer danke ich für ein weitsichtiges Gespräch am Wissenschaftskolleg. Technische und mathematische Problemstellungen konnte ich mit meinen interdisziplinären Co-Autoren angehen, dem Mathematiker Professor Emil Wiedemann und den Informatikern Professor Felix Naumann und Meike Zehlike, woraus mehrfach fruchtbare Kooperationen erwuchsen.

Besonders herzlich danke ich schließlich meinen Freunden und, vor allem, meiner Familie. Meine Mutter hat das gesamte Manuskript Korrektur gelesen – all errors remain entirely my own, wie man in amerikanischen Aufsätzen zu sagen pflegt. Meine Frau und meine zwei Kinder schließlich haben glücklicherweise immer wieder für die nötige Entschleunigung und die fröhlichste aller denkbaren Ablenkungen von der Wissenschaft gesorgt. Ihnen ist diese Arbeit gewidmet.

Berlin, im Mai 2020 Philipp Hacker

Inhaltsübersicht

Inhaltsverzeichnis

§1 Einführung

Das neue unionale Datenschutzrecht ist, entgegen mancher Befürchtung,[1] kein *law of everything*. Vielmehr müssen unterschiedliche Rechtsmaterien ineinandergreifen, um eine sachgerechte Regelungsstruktur im Schnittbereich von Datenschutzrecht und Privatrecht aufzubauen. Die Bestimmung des Verhältnisses dieser Rechtsmaterien, insbesondere von Datenschutzrecht und bürgerlichem Recht, ist ein zentrales Anliegen dieser Untersuchung. Denn die Verschränkung unterschiedlicher Technologieformen fordert mehr denn je ein rechtsbereichsübergreifendes Verständnis von juristischer Dogmatik und ein interdisziplinär fundiertes Konzept von Regulierung.

A. Daten in der Dauerschleife

Die Kombination unterschiedlicher Technologieformen schreitet rasant voran. Ob Tracking-Instrumente, künstliche Intelligenz oder das Internet der Dinge:[2] Neue Technologien konvergieren zunehmend gegen ein umfassendes *Internet of Everything*,[3] in dessen Rahmen nicht nur analoge und virtuelle Sphären kurzgeschlossen,[4] private und öffentliche Räume verschränkt,[5] sondern

[1] *Purtova*, 10 Law, Innovation and Technology 2018, 40 (41, 75 ff.); siehe auch *Lynskey*, 21 German Law Journal 2020, 80 (82); kritisch *Clifford*, The Legal Limits to the Monetisation of Online Emotions, 2019 Rn. 196–199.

[2] Zu diesen Basistechnologien ausführlich unten, §2 A.–C.

[3] Überblick über den Stand der Entwicklung bei *Breiner/Sriram/Subrahmanian*, AAAI Spring Symposium Series 2018, 107 (107 ff.); *Velasquez et al.*, 9 Journal of Internet Services and Applications 2018, 14 (14 ff.); *Di Martino et al.*, in: Di Martino et al. (Hrsg.), Internet of Everything, 2018, 1 (1 ff.); zum Entwicklungspotenzial *DeNardis*, The Internet in Everything, 2020, 3 ff.; *Shojafar/Sookhak*, International Journal of Computers and Applications 2019, DOI: 10.1080/1206212X.2019.1575621, 1 (1); *Miraz et al.*, 10 Future Internet 2018, Article 68, 1 (5); *Botta et al.*, 56 Future Generation Computer Systems 2016, 684 (688); *Miraz et al.*, IEEE Internet Technologies and Applications (ITA) 2015, 219 (220 f.); *Sriram*, 17(3) IT Professional 2015, 60; *Abdelwahab et al.*, 1 IEEE Internet of Things Journal 2014, 276 (276); *Jara/Ladid/Gómez-Skarmeta*, 4 Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 2013, 97 (98); *Evans*, The Internet of Everything, Cisco Internet Business Solutions Group (IBSG), Report, 2012, 3 ff.; siehe auch unten, §2 D.

[4] *DeNardis*, The Internet in Everything, 2020, 8–11; *Hildebrandt*, Smart Technologies and the End(s) of Law, 2015, 41 f.

[5] Siehe etwa *Hacker*, 7 International Data Privacy Law 2017, 266 (272); zur Smart City repräsentativ *Madaan/Ahad/Sastry*, 34 Computer Law & Security Review 2018, 125 (128 ff.);

auch Marktprozesse neu integriert werden.[6] Motor dieser Dynamik ist nicht zuletzt der bereits seit einigen Jahren zu konstatierende Einsatz personenbezogener Daten als funktionales Geldäquivalent.[7] Schon an der zunehmenden Nutzung von autonomen und vernetzten Fahrzeugen[8] oder von Gesichtserkennungssoftware durch private und öffentliche Akteure[9] zeigt sich jedoch, dass die technische Entwicklung mittlerweile weit darüber hinausgeht. Mit der wachsenden Vernetzung von Alltagsgeräten, onlinebasierten Dienstleistungen und öffentlichen Infrastrukturen entstehen genuin techno-physische Architekturen,[10] die durch eine Dauerschleife von einander durchdringenden, sich gegenseitig verstärkenden Analysesystemen gekennzeichnet sind:[11] Tracking-Technologien erheben Daten, die mithilfe von Techniken maschinellen Lernens analysiert und zur Steuerung von Geräten des Internets der Dinge eingesetzt werden, die ihrerseits wiederum neue Daten erheben und in den Zyklus einspeisen. Die Systeme sind entwicklungsoffen,[12] doch der Kreis der Daten schließt sich.

Die Integration dieser Prozesse in ein *Internet of Everything* ist nicht unumstritten. Die Utopie der einen[13] ist, wie so häufig, die Dystopie der ande-

---

Cobbe/Morison, in: Slautsky (Hrsg.), The Conclusions of the Chaire Mutations de l'Action Publique et du Droit Public, 2019.

[6] Siehe nur *Goldfarb/Greenstein/Tucker*, in: Goldfarb/Greenstein/Tucker (Hrsg.), Economic Analysis of the Digital Economy, 2015, 1, sowie die weiteren Beiträge in diesem Band; ferner *Urbach*, in Schmidt-Kessel/Kramme, Geschäftsmodelle in der digitalen Welt, 2017, 39; siehe auch die Nachweise in § 2, Fn. 99 zum *consumer preference modeling*.

[7] Siehe unten, § 3 A.II.

[8] Dazu etwa *Abeck et al.*, INFORMATIK 2019, 125 (125 ff.); *Crane/Logue/Pilz*, 23 Michigan Telecommunications and Technology Law Review, 2016, 191 (199 f.).

[9] Siehe nur die (kritische) Debatte über den zunehmenden Einsatz von Gesichtserkennungssoftware in westlichen Demokratien: *Europäische Kommission*, Weißbuch zur Künstlichen Intelligenz, COM(2020) 65 final, 25 f.; *Coester/Fuhlert*, DuD 2020, 48 (49 ff.); *Hill*, The Secretive Company That Might End Privacy as We Know It, New York Times (18.1.2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; *Garvie*, Garbage In, Garbage Out. Face Recognition on Flawed Data, Center on Privacy & Technology, Georgetown Law, Report, 2019; *Draper*, Madison Square Garden Has Used Face-Scanning Technology on Customers, New York Times (13.3.2018), https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html; *Garvie/Bedoya/Frankle*, The Perpetual Line-Up: Unregulated Police Face Recognition in America, Center on Privacy & Technology, Georgetown Law, Report, 2016; zur VR China *Zoll*, Überwachung mit Gesichtserkennung: Made in China, erprobt in Xinjiang und weltweit exportiert, NZZ (3.12.2019), https://www.nzz.ch/international/china-nutzt-gesichtserkennung-fuer-ueberwachung-und-exportiert-sie-ld.1525690; zur Technologie grundlegend *Lawrence et al.*, 8 IEEE Transactions on Neural Networks 1997, 98; siehe auch *Y. Sun et al.*, Deepid3: Face recognition with very deep neural networks, Working Paper, 2015, https://arxiv.org/abs/1502.00873; *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 23 f.; *Ranjan et al.*, 35 IEEE Signal Processing Magazine 2018, 66.

[10] Siehe nur *DeNardis*, The Internet in Everything, 2020, 25 ff.; vgl. auch *Grünberger*, AcP 218 (2018), 213 (235).

[11] Siehe unten, § 3 D.

[12] *Breiner/Sriram/Subrahmanian*, AAAI Spring Symposium Series 2018, 107 (107 f.).

[13] Repräsentativ *Evans*, The Internet of Everything, Cisco Internet Business Solutions

ren.[14] Welchen Weg die technische Entwicklung letztlich nehmen wird, lässt sich naturgemäß nur schwer prognostizieren; umso dringlicher ist jedoch deren rechtliche Begleitung. Gesichert scheint dabei einzig, dass die Tendenz zu einer zunehmenden Kombination von Datensätzen[15] und Technologieformen geht.[16] Man muss nicht das Menetekel des chinesischen Sozialkreditsystems[17] an die Wand malen, um zu erkennen, dass darin gesellschaftliche und ökonomische Kräfte liegen, denen nachgerade revolutionäres Potenzial innewohnt.[18] So hat etwa der Einsatz von Daten als Zahlungsmittel die unmittelbare Folge, dass – ökonomisch gesprochen – die Budgetrestriktionen von Verbrauchern erheblich erweitert werden.[19] Darin liegt nicht zuletzt ein tendenziell egalitärer Impetus: Daten kann jede Person in ähnlichem Umfang als Geldäquivalent einsetzen.[20] Zugleich stellt diese Entwicklung eine immense Herausforderung für ihre datenschutz- und freiheitskonforme Ausgestaltung dar, insbesondere auch deshalb, weil die Präferenzen hinsichtlich des Einsatzes von Daten als Zahlungsmittel erheblich zwischen den Nutzern divergieren.[21]

Zugleich ist der beschriebene Prozess durch die Besonderheit gekennzeichnet, dass die Selbstentäußerung von Privatheit in ganz erheblichem Maße durch eine (untechnisch gesprochen[22]) freiwillige Offenlegung von personenbezogenen Daten angetrieben wird.[23] Angesichts der zunehmenden Unentziehbarkeit aus der Dauerschleife von Datenerhebung, -analyse und datenbasierter Aktuation stellt sich jedoch die Frage, ob sich die bisherigen rechtlichen Kategorien, die selbstbestimmtes Handeln in digitalen Kontexten garantieren sollten – ins-

---

Group (IBSG), Report, 2012, 3 ff.; *Breiner/Sriram/Subrahmanian*, AAAI Spring Symposium Series 2018, 107 (107 f.).

[14] Siehe etwa *Zuboff*, The Age of Surveillance Capitalism, 2019, besonders deutlich in Kapitel 11 II. und Kapitel 12 VII.; *Auer*, Zum Erkenntnisziel der Rechtstheorie, 2018, 63; früh bereits nuanciert kritisch Picard, *Affective Computing*, 1997, 118 f., 244; Analyse des *Internet of Everything* als Machtstruktur und Governance-Herausforderung bei *DeNardis*, The Internet in Everything, 2020, 17 ff., 212 ff.

[15] *Bruneteau et al.*, Usage-Based Insurance. Global Study, 2016, 15.

[16] Siehe nochmals unten, § 2 D.

[17] Dazu nur *Liang et al.*, 10 Policy & Internet 2018, 415; *Genzsch*, in: Loitsch (Hrsg.), China im Blickpunkt des 21. Jahrhunderts, 2019, 129.

[18] *DeNardis*, The Internet in Everything, 2020, 59 ff.; *Hildebrandt*, Smart Technologies and the End(s) of Law, 2015, 45 ff.; kritische Zuspitzung bei *Zuboff*, The Age of Surveillance Capitalism, 2019, vor allem Kapitel 13.

[19] Siehe unten, § 3 B.I.1.c).

[20] Vgl. den provokativen Vorschlag bei *Arrieta-Ibarra et al.*, 108 AEA Papers and Proceedings 2018, 38 (39 f.) zu *data as labor*; dass manche personenbezogenen Daten stärker nachgefragt werden und mehr Wert haben als andere, ist zwar nicht in Abrede zu stellen, siehe nur *Bundesverband der digitalen Wirtschaft*, Data Economy, 2018, 15 f. sowie unten, § 3 A.II.1.b). Allerdings dürften diese Wertunterschiede tendenziell orthogonal zu den hergebrachten Kategorien sozio-ökonomischer Stratifikation liegen.

[21] Siehe unten, § 3 C.

[22] Zum spezifisch datenschutzrechtlichen Begriff der Freiwilligkeit in diesem Kontext näher unten, § 4 B.I.3.dd).

[23] *Auer*, Zum Erkenntnisziel der Rechtstheorie, 2018, 61 f.; siehe auch unten, § 4 B.I.5.

besondere die Einwilligung – nicht endgültig überholt haben. Die vorliegende Untersuchung wird zeigen, dass diese Frage, entgegen zahlreicher Grabesreden auf die Einwilligung,[24] nicht uneingeschränkt bejaht werden kann. Allerdings können und müssen die gesetzlich bereits angelegten Formen datensouveränen Handelns technisch und regulatorisch unterstützt werden, um wenigstens eine maschinell mediierte Residualform von Privatautonomie unter den Bedingungen der digitalen Wirtschaft, und zumal des sich ankündigenden *Internet of Everything*, zu erhalten.[25] Dies impliziert jedoch zugleich, dass neue, datenverarbeitende Technologien nicht nur als Risiko, sondern auch als Chance für Selbstbestimmung und Datenschutz angesehen werden sollten.

B. Datenprivatrecht

Diese Technologien machen an den etablierten Grenzen tradierter Rechtsgebiete keinen Halt. Vielmehr verlangen sie nach einer rechtsgebietsübergreifenden Integration ganz unterschiedlicher, teils rein national, teils unionsrechtlich geprägter Normgruppen. Einerseits ist dabei das Datenschutzrecht von unabweislicher Relevanz, da die genannten Technologien jedenfalls typischerweise mit der Verarbeitung personenbezogener Daten operieren. Zugleich werden sie jedoch, sofern sie von nicht-öffentlichen Akteuren verwendet werden, zur Strukturierung von marktförmigen Austauschprozessen genutzt, auf welche die klassischen Bereiche des Privatrechts Anwendung finden. Die Engführung von Datenschutzrecht und Privatrecht ist dabei besonders getrieben durch die Nutzung von Daten als funktionales Geldäquivalent, bleibt jedoch an diesem Punkt nicht stehen.

In jüngerer Zeit wird vor allem im zivilrechtlichen Diskurs zunehmend von der Notwendigkeit der Ausformung eines Datenschuldrechts gesprochen.[26] Allerdings erweist sich dieser Begriff letztlich als zu eng, da die privatrechtlichen

---

[24] Siehe etwa *Zuiderveen Borgesius*, 13 IEEE Security & Privacy 2015, 103 (104 f.); *Barocas/Nissenbaum*, 57(11) Communications of the ACM 2014, 31 (32); *Tene/Polonetsky*, 11 Northwestern Journal of Technology and Intellectual Property 2012, 239 (261 f.); vgl. ferner die Nachweise in § 6, Fn. 195 ff.

[25] Dazu näher unten, § 6 C.

[26] Begriffsprägend *Schmidt-Kessel*, Daten als Gegenleistung in Verträgen über die Bereitstellung digitaler Inhalte, Folien zum Vortrag vom 3.5.2016, Folie 7, https://www.bmjv.de/SharedDocs/Downloads/DE/Praesentationen/05032016_digitalesVertragsrecht_Schmidt_Kessler.html; bereits zuvor in der Sache *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (220 ff.); aufgegriffen bei *Wendehorst*, NJW 2016, 2609 (2610); *Sattler*, JZ 2017, 1036 (1036); *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (102 ff.); *Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder*, Bericht vom 15. Mai 2017, 2017, 16, 202 ff.; *Föhlisch*, CR 2018, 583 (583); *Gsell*, ZUM 2018, 75 (80 Fn. 64); *Sattler*, in: Ochs et al. (Hrsg.), Die Zukunft der Datenökonomie, 2019, 1 (3 ff.); *Datenethikkommission*, Gutachten der Datenethikkommission, 2019, 147; *Indenhuck/Britz*, BB 2019, 1091 (1091 ff.); *Staudenmayer*, NJW 2019, 2497 (2497); *Riechert*, DuD 2019, 353 (360).

Implikationen von Daten über die Wechselwirkungen des Datenschutzrechts mit dem Schuldrecht im engeren Sinne hinausgehen. Die zunehmende Integration digitaler Technologien in alle Lebensverhältnisse und Austauschprozesse macht daher die Entwicklung eines *Datenprivatrechts* notwendig, in dem auch das Datenschuldrecht als ein Spezialgebiet seinen Platz findet. Der Begriff des „Datenprivatrechts" wurde bislang, soweit ersichtlich, nur im Kontext des internationalen Privatrechts verwandt (internationales Datenprivatrecht),[27] dort jedoch als Chiffre für Fragen des internationalen Privat- und Zuständigkeitsrechts des Datenschutzrechts.[28] Bei Lichte betrachtet reicht das Datenprivatrecht aber, wie auch die Untersuchungen zum IPR schon andeuten,[29] über die DS-GVO und weitere Datenschutzrechtsakte weit hinaus. Letztlich steht der Begriff für ein interdisziplinär informiertes Privatrecht des Umgangs mit Daten. Zum Aufbau einer solchen Querschnittsmaterie kann eine einzelne Untersuchung naturgemäß nur einen Baustein liefern. Ausgespart werden muss vorliegend etwa die besonders vor einigen Jahren aktiv geführte und nun noch einmal von der WIPO[30] aufgegriffene Debatte um ein „Datenrecht" bzw. ein „Dateneigentum".[31]

Die zentrale Zäsur innerhalb des Datenprivatrechts stellt vielmehr die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten dar: Mit ihr steht und fällt die Anwendbarkeit des (unionalen und nationalen) Datenschutzrechts. Wie im Folgenden noch genauer darzustellen ist,[32] interpretiert der EuGH den Begriff der personenbezogenen Daten denkbar weit. Dies impliziert, dass die Wechselwirkungen zwischen Datenschutzrecht und Privatrecht einen Kernbereich des Datenprivatrechts ausmachen, für datengeprägte Austauschprozesse außerhalb der Industrie 4.0 vielleicht gar den relevantesten. Dieser Schnittbereich lässt sich, infolge der schon durch den Anwendungsvorrang des Unionsrechts bedingten Schlüsselstellung des Datenschutzrechts, als *Datenschutzprivatrecht* beschreiben.[33] Dabei muss jedoch, wie sich zeigen wird, neben dem klassisch-regulatorischen Zugriff des Datenschutzrechts immer zugleich die Perspektive eines Daten*ermöglichungs*rechts mitgedacht werden, welches die Nutzer in die Lage versetzt, mit ihren Daten, so weit als möglich, souverän zu verfahren und diese beispielsweise als funktionales Zahlungsäquivalent einzusetzen. Inwiefern solche autonomieförderli-

---

[27] *Lüttringhaus*, ZVglRWiss 117 (2018), 50; ihm begrifflich folgend *Thon*, RabelsZ 84 (2020), 24.

[28] *Lüttringhaus*, ZVglRWiss 117 (2018), 50 (52).

[29] Siehe etwa *Lüttringhaus*, ZVglRWiss 117 (2018), 50 (56 ff., 76 ff.).

[30] *WIPO*, Draft Issues Paper on Intellectual Property and Artificial Intelligence, WIPO/IP/AI/2/GE/20/1, 2019, Issue 10.

[31] Siehe dazu etwa *Zech*, CR 2015, 137 (144 ff.); *Fezer*, MMR 2017, 3; *Specht*, GRUR Int. 2017, 1040; *Denga*, NJW 2018, 1371; *Kühling/Sackmann*, ZD 2020, 24; *Pertot* (Hrsg.), Rechte an Daten (im Erscheinen).

[32] Siehe unten, § 4 A.II.2.

[33] So bereits *Hacker*, ZfPW 2019, 148 (150, 195 f.).

chen Ermöglichungsstrukturen im Datenprivatrecht, einschließlich des unionalen Datenschutzrechts, bereits jetzt angelegt sind bzw. ausgebaut werden können, wird eine zentrale Fragestellung der Arbeit ausmachen.[34]

Inhaltlich beschäftigt sich das Datenschutzprivatrecht also mit den Wechselwirkungen des Datenschutzrechts mit einer Reihe von Gebieten des Privatrechts, im Rahmen des bürgerlichen Rechts vordringlich etwa mit der Rechtsgeschäftslehre und dem Schuldrecht, letztlich aber mit allen Büchern des BGB.[35] Außerhalb des BGB stehen die Interferenzen des Datenschutzrechts mit dem Antidiskriminierungsrecht,[36] dem Lauterkeitsrecht[37] und, bereits am weitesten durch das Schrifttum erfasst, dem Kartellrecht[38] im Fokus.[39] Nur

[34] Siehe insbesondere §§ 4 B., 5 B., 6 C.

[35] Siehe zum Verhältnis von Datenschutzrecht und Erbrecht im Kontext des digitalen Nachlasses etwa BGH NJW 2018, 3178 Rn. 64 ff.; repräsentativ aus dem Schrifttum *Budzikiewicz*, AcP 218 (2018), 558 (577 ff.); zum Familienrecht, speziell zur Einwilligung in die Verarbeitung personenbezogener Daten durch Betreuungsbehörden, AG Altötting, Verfügung vom 9.9.2019 – 401 XVII 0178/92, BeckRS 2019, 30935; ferner allgemein die Beiträge in *Pertot* (Hrsg.), Rechte an Daten (im Erscheinen).

[36] Siehe dazu bereits *Hacker*, 55 Common Market Law Review 2018, 1143 (1172 ff.); *Zehlike/Hacker/Wiedemann*, 34 Data Mining and Knowledge Discovery 2020, 163 (186 ff.); *Wachter*, Affinity Profiling and Discrimination by Association in Online Behavioural Advertising, 35 Berkeley Technology Law Journal (im Erscheinen), https://ssrn.com/abstract=3388639, 17 ff.

[37] Siehe nur LG Stuttgart, ZD 2019, 366; *Uebele*, GRUR 2019, 694 (697 f.); *Köhler*, ZD 2019, 285 (285); *Ohly*, GRUR 2019, 686 (688 ff.); *de Franceschi*, in: Schmidt-Kessel/Kramme (Hrsg.), Geschäftsmodelle in der digitalen Welt, 2017, 113 (131 f.).

[38] Siehe dazu OLG Düsseldorf NZKart 2019, 495 (498): von Marktmacht unabhängiger Datenschutzverstoß als solcher für kartellrechtlichen Missbrauch marktbeherrschender Stellung nicht ausreichend; im internationalen Schrifttum zum EU-Recht überwiegt die Befürwortung der Berücksichtigung von Datenschutzbelangen in der kartellrechtlichen Analyse, siehe etwa *Costa-Cabral/Lynskey*, 54 Common Market Law Review 2017, 11 (besonders 33 ff., dort 35 zur Kausalität); *Graef/Clifford/Valcke*, 8 International Data Privacy Law 2018, 200 (210 f.); *Stucke*, 2 Georgetown Law Technology Review 2018, 275 (286–290); *Lianos*, Polycentric Competition Law, 71 Current Legal Problems 2018, 161 (185–189); *European Data Protection Supervisor*, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, Preliminary Opinion, 2014, besonders 29–32; ders., On the coherent enforcement of fundamental rights in the age of big data, Opinion 8/2016, 2016, besonders 5–7; *Autorité de la Concurrence/Bundeskartellamt*, Competition Law and Data, Joint Report (10.5.2016), 25; ferner auch *Monopolkommission*, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015, Rn. 522–527; *Kuner/Cate/Millard/Svantesson/Lynskey*, 4 International Data Privacy Law 2014, 247 (248); *Buchner*, WRP 2019, 1243 (1245); tendenziell auch *Kamann/Miller*, NZKart 2016, 405 (406); das deutsche Schrifttum sieht dies mehrheitlich kritisch, etwa *Körber*, NZKart 2016, 348 (351 ff.); *Franck*, ZWeR 2016, 137 (151 ff.) (mangels Kausalität der marktbeherrschenden Stellung für die Datenschutzverletzung); so auch *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (303 f.); *Körber*, NZKart 2019, 187 (192 f.); ferner *Colangelo/Maggiolino*, 42(3) World Competition Law and Economics Review 2019, 355; sowie die Nachweise unten in § 4, Fn. 550; insgesamt skeptisch jedoch hinsichtlich der Möglichkeit einer durch das Kartellrecht getragenen Regulierung digitaler Austauschprozesse *Grünberger*, AcP 218 (2018), 213 (245 f.).

[39] Auch darüber hinaus werden privatrechtliche Gebiete von der DS-GVO maßgeblich beeinflusst, siehe etwa zum Wechselspiel von DS-GVO und ZPO *Ory/Weth*, NJW 2018,

durch die Analyse dieser Querbeziehungen kann ein integriertes Marktordnungsrecht für die digitale Wirtschaft erarbeitet werden, das einerseits sachspezifische Risiken adressiert, andererseits aber auch die Bedingungen der Möglichkeit privatautonomer Gestaltung von Rechtsverhältnissen erhält bzw., wo notwendig, wiederherstellt.

Die vorliegende Untersuchung kann jedoch schon aus Gründen des Umfangs nur einen Ausschnitt dieses umfassenden Forschungsprojekts verwirklichen. Sie fokussiert sich daher innerhalb des Datenprivatrechts auf das Datenschutzprivatrecht im soeben beschriebenen Sinn. Dabei identifiziert sie drei spezifische regulatorische Herausforderungen, welche ein Daten(schutz)privatrecht nach hier vertretener Auffassung vorrangig meistern muss: die Multirelationalität von Daten; ihre Ambivalenz hinsichtlich Nutzen und Risiken; sowie die Heterogenität von Datenschutzpräferenzen.[40] Sachrechtlich kapriziert sich die Untersuchung dabei auf die Wechselwirkungen zwischen dem Datenschutzrecht einerseits und Kerngebieten des Zivilrechts andererseits, insbesondere der Rechtsgeschäftslehre und dem Schuldrecht. Dieser spezifische Querschnittsbereich erscheint gerade für die Frage des Stellenwerts und der Funktionsbedingungen der Privatautonomie zentral. Zudem werden rein rechtstatsächlich weite Bereiche der digitalen Austauschprozesse gegenwärtig auf vertraglichem Wege, zumal durch AGB, zwischen den Parteien geregelt,[41] was über die Rechtsgrundlage zur Verarbeitung vertragserforderlicher personenbezogener Daten in Art. 6 Abs. 1 lit. b. DS-GVO auch unmittelbar datenschutzrechtliche Relevanz gewinnt. Schließlich zeigt auch die zur Zeit der Niederschrift dieser Untersuchung gerade verabschiedete DIDD-Richtlinie,[42] dass die Wechselwirkungen zwischen Datenschutzrecht, Vertragsrecht und Rechtsgeschäftslehre gewissermaßen den Nukleus des Datenprivatrechts ausmachen.[43] Kartell- und lauterkeitsrechtliche Berührungspunkte werden im

2829; *Wiebe/Eichfeld*, NJW 2019, 2734; zur Rechtsdurchsetzung etwa *Fries*, NJW 2016, 2860 (2861 ff., besonders 2865).

[40] Siehe unten, § 3 A.–C.

[41] Siehe nur die Portale Terms of Service; Didn't Read (http://tosdr.org/), bei dem Online-Nutzungsbedingungen benotet werden, und TOSBack (https://tosback.org/), das Änderungen von Nutzungsbedingungen transparent macht. Alle in dieser Arbeit zitierten Webseiten wurden, sofern nichts anderes angegeben ist, zuletzt abgerufen am 30.4.2020.

[42] Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl. 2019 L 136/1; dazu, seit dem Erlass der Richtlinie, *Mischau*, ZEuP 2020, 335; *Metzger*, JZ 2019, 577; *Sein/Spindler*, 15 European Review of Contract Law 2019, 257; *Sein/Spindler*, 15 European Review of Contract Law 2019, 365; *Spindler/Sein*, MMR 2019, 415; *Spindler/Sein*, MMR 2019, 488; *Wendland*, ZvglRWiss 2019, 191; *Staudenmayer*, NJW 2019, 2497; *Bach*, NJW 2019, 1705; *Schulze*, ZEuP 2019, 695; *Morais Carvalho*, EuCML 2019, 194; bereits zuvor etwa, aus dem breiten Schrifttum, *Auer*, ZfPW 2019, 130 (132 ff.); *Grünberger*, AcP 218 (2018), 213 (218 ff.); *Gsell*, ZUM 2018, 75; *Grundmann/Hacker*, 13 European Review of Contract Law 2017, 255 (289 ff.); *Graf von Westphalen*, BB 2016, 1411.

[43] Vgl. *Staudenmayer*, NJW 2019, 2497 (2497).

Rahmen dieser Untersuchung an geeigneten Stellen aufgezeigt,[44] ohne dass jedoch eine umfassende Untersuchung der Interdependenzen dieser Rechtsgebiete mit dem Datenschutzrecht geleistet werden könnte. Den Verbindungen von Antidiskriminierungsrecht und Datenschutzrecht schließlich ist der Verfasser bereits an anderer Stelle nachgegangen.[45] In all diesen unterschiedlichen Querschnittsmaterien zeigt sich insbesondere, dass einmal mehr das europäische Mehrebenensystem[46] – im hier relevanten Bereich bestehend aus mitgliedstaatlichem und unionalem,[47] dabei teils durch Richtlinien geprägtem, teils unmittelbar durch Verordnungen gesetztem, teils durch Öffnungsklauseln konturiertem Recht – die methodische Komplexität der rechtswissenschaftlichen Erfassung neuer Technologien nicht unerheblich erhöht.[48]

C. Regulatorisches und ermöglichendes Privatrecht

Die systematische Erfassung des Datenprivatrechts muss sich nicht nur an der Dogmatik, sondern auch an den Funktionen des Privatrechts orientieren. Dieses wird bereits seit längerem,[49] besonders deutlich in der grundlegenden Untersuchung von *Hellgardt*,[50] als ein multifunktionales System betrachtet, das neben einem sachgerechten Interessenausgleich[51] (zumindest[52]) zwei weitere, einander partiell ausschließende Ziele verfolgt: einerseits die Ermöglichung der

[44] Siehe zum Kartellrecht etwa § 4 B.I.3.a)dd)(3)(b)(aa) zur Relevanz der Marktmacht des Anbieters bei der Bestimmung der Freiwilligkeit der datenschutzrechtlichen Einwilligung; Text bei § 4, Fn. 945 zur kartellrechtlichen Dimension von Zugangsrechten; zum Lauterkeitsrecht etwa Text bei § 5, Fn. 504 f. zum Unterlassungsanspruch von Mitbewerbern bei Datenschutzrechtsverstößen.

[45] Siehe die Nachweise oben in Fn. 36.

[46] Zu Begriff und Inhalt ausführlich *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, 115 ff.

[47] Die Ebene des internationalen Rechts (Völkerrecht, Einheitsrecht, *lex mercatoria*) wird hingegen in dieser Arbeit ausgeblendet; siehe zu dieser Ebene im Kontext des europäischen Privatrechts allgemein *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, 126 f., 469 ff.

[48] Siehe dazu unten, § 5 A.

[49] Siehe bereits *Böhm*, ORDO 17 (1966), 75 (91 f.); *Steindorff*, in: Festschrift für Ludwig Raiser, 1974, 621 (625); *Zöllner*, AcP 188 (1988), 85 (98–100), wenngleich mit kritischem Blick auf die regulatorische Seite des Privatrechts; zu einer funktionalen Vertragsperspektive grundlegend *Raiser*, in: von Caemmerer et al. (Hrsg.), Hundert Jahre deutsches Rechtsleben, 1960, 101 (109 ff.); siehe auch den Überblick bei *Grundmann*, in: Grundmann/Micklitz/Renner (Hrsg.), Privatrechtstheorie, Band I, 2015, 875 (877 ff.).

[50] *Hellgardt*, Regulierung und Privatrecht, 2016, 47 ff., besonders 58 f., der beide Funktionen auf das Recht als solches, über das Privatrecht hinaus, ausdehnt (ebd., 50 f., 58).

[51] Siehe repräsentativ *Hellgardt*, Regulierung und Privatrecht, 2016, 59 ff.; *Grundmann*, in: Festschrift Canaris, 2017, 907 (910 ff., 942); vgl. auch *Böhm*, ORDO 17 (1966), 75 (140 ff.); im Kontext des privaten Datenrechts auch *Denga*, NJW 2018, 1371 (1373 ff.).

[52] Zu weiteren Funktionen, *Hellgardt*, Regulierung und Privatrecht, 2016, 62 ff. (Organisations- und Begrenzungsfunktion); *Körber*, Grundfreiheiten und Privatrecht, 2004, 52 ff. (Integrationsfunktion im Binnenmarkt).

Ausübung von Privatautonomie (ermöglichendes Privatrecht)[53] und andererseits die Einhegung spezifischer Risiken (regulatorisches Privatrecht),[54] wobei sich letztere zumeist, wenngleich nicht notwendig,[55] als Folge eines Marktversagens darstellen.[56]

Regulierung, verstanden als bewusste, rechtsförmige, staatliche Beeinflussung, die einen über den Einzelfall hinausgehenden Ordnungszweck verfolgt,[57] ist schon begrifflich auf Ordnungsstrukturen bezogen.[58] In privatrechtlichen

[53] Siehe nur *Böhm*, ORDO 17 (1966), 75 (91); *Grundmann*, Europäisches Schuldvertragsrecht, 1999, 1. Teil, § 2 Rn. 52; *Collins*, Regulating Contracts, 1999, 7 f.; *Körber*, Grundfreiheiten und Privatrecht, 2004, 41 ff.; *Grundmann*, 6 European Review of Private Law 2010, 1055 (1063–1066); *Wagner*, in: Blaurock/Hager, Obligationenrecht im 21. Jahrhundert, 2010, 13 (14 f.); *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 36–38; diese Ermöglichungsfunktion wird auch als Infrastrukturfunktion des (Privat-)Rechts bezeichnet, siehe *Windbichler*, AcP 198 (1998), 261 (271); *Bachmann*, Private Ordnung, 2006, 73–76; *Ackermann*, Der Schutz des negativen Interesses, 2007, 136; *Möslein*, Dispositives Recht, 2011, 380 („staatliche Infrastrukturverantwortung"); *Hellgardt*, Regulierung und Privatrecht, 2016, 56–59; vgl. für das Gesellschaftsrecht auch *Fischel/Easterbrook*, The Economic Structure of Corporate Law, 1996, 34.

[54] Siehe dazu umfassend *Collins*, Regulating Contracts, 1999, 8 f. und 31 ff. (bezogen auf das Vertragsrecht); mit Blick auf das Privatrecht insgesamt *Hellgardt*, Regulierung und Privatrecht, 2016, 46 ff.; ferner *Windbichler*, AcP 198 (1998), 261 (272); *Körber*, Grundfreiheiten und Privatrecht, 2004, 47 ff.; *Wagner*, AcP 206 (2006), 352 (422 ff.) (Steuerungsfunktion); *Micklitz*, GPR 2009, 254 (255 ff.) (Europäisches Vertragsrecht als „Regulierungsprivatrecht"); *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 38–44; *Grundmann*, in: Festschrift Canaris, 2017, 907 (910); *Grundmann/Hacker*, 13 European Review of Contract Law 2017, 255 (256 f.); *Grünberger*, AcP 218 (2018), 213 (241); siehe auch die verwandte Unterscheidung zwischen marktkonstitutivem und marktkompensatorischem Vertragsrecht bei *Fornasier*, Freier Markt und zwingendes Vertragsrecht, 2013, 65 ff.). Unter denjenigen, welche die Regulierungsfunktion des Privatrechts anerkennen, ist freilich umstritten, ob sich diese auf den Erhalt bzw. die Wiederherstellung der Ermöglichungsfunktion beschränken muss (so etwa *Zöllner*, AcP 188 [1988], 85 [98 f.]; vgl. auch *Bydlinski*, AcP 204 [2004], 309 (344 f.) zum Strafschadensersatz) oder ob auch darüber hinausgehende Ziele verfolgt werden können (so *Collins*, Regulating Contracts, 1999, 8; *Wagner*, AcP 206 [2006], 352 [432 ff.]; *Micklitz*, GPR 2009, 254 [257]; *Collins*, 22 EBLR 2011, 425, 426; *Hellgardt*, Regulierung und Privatrecht, 2016, 81; *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 41 ff.; *Hacker*, Verhaltensökonomik und Normativität, 2017, § 6 und § 9).

[55] Siehe nur *Collins*, Regulating Contracts, 1999, 8.

[56] *Grundmann*, in: Grundmann (Hrsg.), Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts, 2000, 1 (29); siehe auch *Collins*, Regulating Contracts, 1999, 7.

[57] Vgl. *Eifert*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts – Band I, 2. Aufl. 2012, 1319, besonders Rn. 5; dort auch zum uneinheitlichen Begriff der Regulierung (ebd. Rn. 1 ff.); dazu auch, rechtsvergleichend, *Grundmann*, in: Festschrift Canaris, 2017, 907 (909 f.); *Hellgardt*, Regulierung und Privatrecht, 2016, 16 ff., besonders 50 ff., der zudem die Verfolgung von Zielen des Allgemeinwohls als notwendige Begriffsbedingung postuliert (ebd., 53–55, 81). Im hier betrachteten Schnittbereich von Datenschutz- und Privatrecht macht die (nicht unumstrittene, siehe nur *Collins*, Regulating Contracts, 1999, 7) Hinzunahme dieser Bedingung jedoch keinen Unterschied, da regelmäßig staatliche Eingriffe (zumindest auch) die Verwirklichung von Markt- oder Datenschutz zum Ziel haben; siehe im Einzelnen unten, § 4 C. und § 5 C.

[58] Vgl. auch den Überblick über Ordnungsdenken und die ordoliberale Schule bei

Kontexten interveniert Regulierung typischerweise durch die Verfolgung jeweils zu rechtfertigender Ordnungszwecke in den Marktmechanismus und begrenzt den Spielraum der Akteure.[59] Damit fungiert diese regulatorische Ebene als ein Rahmen für die Ausübung von Privatautonomie.[60] Demgegenüber lassen sich solche Normen identifizieren, die primär, zum Teil auch durch zwingendes Recht, eine Erweiterung dieses Spielraums bezwecken. Sie halten rechtliche Konstrukte bereit, welche privatautonome Gestaltung unterstützen oder überhaupt erst ermöglichen.[61] Beispiele für derartige Ermöglichungsstrukturen bieten die Anerkennung von (natürlichen oder juristischen) Personen als Rechtssubjekte,[62] rechtliche (z. B. vertragliche) Typisierungen[63] oder die Verfügbarmachung von staatlichen Rechtsdurchsetzungsmechanismen.[64]

Dabei ist zu konzedieren, dass gerade im Vertragsrecht viele Normen sowohl regulatorischen als auch ermöglichenden Charakter haben,[65] da sie einerseits bestimmte, (auch) der Allgemeinheit dienende Schutzzwecke verfolgen,

---

Grundmann, in: Grundmann/Micklitz/Renner (Hrsg.), Privatrechtstheorie, Band I, 2015, 405 (408 ff.); *Vanberg*, in: Newman (Hrsg.), The New Palgrave Dictionary of Law and Economics, Band 2, 1998, 172; zu Ordnungstrukturen im Privatrecht auch *Mestmäcker*, JZ 1964, 441 (443 ff.); grundlegend *Böhm*, ORDO 17 (1966), 75 (85 ff., 99 ff.).

[59] *Hellgardt*, Regulierung und Privatrecht, 2016, 59; vgl. auch *Eifert*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts – Band I, 2. Auf. 2012, 1319 Rn. 3; *Eisner/Worsham/Ringquist*, Contemporary Regulatory Policy, 2000, 6 ff.; für das Datenschutzrecht auch *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 62.

[60] *Kilian*, in: Grundmann (Hrsg.), Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts, 2000, 427 (431); *Grundmann*, in: Festschrift Canaris, 2017, 907 (911).

[61] Siehe die Nachweise oben in Fn. 53.

[62] *Körber*, Grundfreiheiten und Privatrecht, 2004, 41 f.; *Unberath*, Die Vertragsverletzung, 2007, 71 ff.; *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 36.

[63] *Körber*, Grundfreiheiten und Privatrecht, 2004, 42; *Hellgardt*, Regulierung und Privatrecht, 2016, 72.

[64] *Körber*, Grundfreiheiten und Privatrecht, 2004, 44; *Ackermann*, Der Schutz des negativen Interesses, 2007, 135 f.; *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 37; *Hacker*, Verhaltensökonomik und Normativität, 2017, 238; vgl. auch *Raiser*, in: von Caemmerer et al. (Hrsg.), Hundert Jahre deutsches Rechtsleben, 1960, 101 (115).

[65] *Körber*, Grundfreiheiten und Privatrecht, 2004, 41; *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 36; vgl. auch *Fornasier*, Freier Markt und zwingendes Vertragsrecht, 2013, 66 (Hybridqualität von Normen mit sowohl marktkonstitutiver als auch marktkompensatorischer Funktion, etwa § 138 BGB). Ob man Ermöglichung bzw. Erhalt und Wiederherstellung der Möglichkeit zur effektiven Wahrnehmung privater Gestaltungsmacht durch privatautonome Regelsetzung auch als Teil der Regulierung sieht, weil auch hier zielgerichtet Verhalten und Marktstruktur beeinflusst werden, ist eine rein begriffliche Frage, von der hier nichts weiter abhängt (ablehnend etwa *Hellgardt*, Regulierung und Privatrecht, 2016, 71 f.; *Ackermann*, Der Schutz des negativen Interesses, 2007, 136 [kein Eingriffscharakter]; bejahend *Grundmann*, in: Festschrift Canaris, 2017, 907 [911]; wohl auch schon *Grundmann*, 6 European Review of Private Law 2010, 1055 [1064 f.]). Für die Zwecke dieser Arbeit werden derartige Normen in terminologischer Hinsicht als Hybrid von Ermöglichungs- und Regulierungsfunktion betrachtet. Analytisch bleibt nichtsdestoweniger die Differenz zwischen Ermöglichung einerseits und restringierend ordnender Regulierung andererseits zentral.

die aber andererseits gerade die materiellen Grundlagen individueller Entscheidungsfreiheit und damit die Funktionsbedingungen der Privatautonomie an sich verbürgen sollen.[66] Informationspflichten etwa regulieren spezifisch und zwingend einen Teil des Informationsflusses im Markt; zugleich jedoch ermöglichen sie den Rezipienten der Pflichtinformationen (idealerweise), ihre privatautonomen Entscheidungen in informierter Weise zu tätigen.[67] Zivilrechtliche Normen können daher Hybrideigenschaften annehmen und zugleich unterschiedliche Grade sowohl hinsichtlich ihrer Regulierungs- als auch ihrer Ermöglichungsfunktion aufweisen. Nichtsdestoweniger lässt sich in den meisten Fällen ein Schwerpunkt bestimmen, der eine Zuordnung ermöglicht.[68]

Die Trennung von ermöglichendem und regulatorischem Privatrecht bildet daher ein analytisches Raster, durch das sich gerade im Schnittbereich von Datenschutzrecht und allgemeinem Privatrecht Wechselwirkungen und Funktionsverschiebungen zwischen den genannten Rechtsbereichen untersuchen lassen. Beide genannten Dimensionen des Privatrechts, die regulatorische und die ermöglichende, müssen jedoch auch dogmatisch rückgebunden und bewältigt werden; dies zeitigt die Notwendigkeit einer Rechtsdogmatik, welche die Realfolgen von bestimmten Auslegungs- und Rechtsfortbildungsalternativen und ihre Rückwirkungen auf die jeweils zugrundliegenden, auch technischen und ökonomischen, Herausforderungen mit in den Blick nimmt.[69] Dieser Verschränkung von funktionaler und dogmatischer Perspektive ist die Untersuchung verpflichtet.

---

[66] So etwa §§ 104 ff., 119 ff. BGB; vgl. nur *Reinhardt*, in: Festschrift Schmidt-Rimpler, 1957, 115 (125); *Zöllner*, AcP 188 (1988), 85 (99); *Canaris*, AcP 200 (2000), 273 (280 f.); *Grundmann*, 6 European Review of Private Law 2010, 1055 (1057); *Hellgardt*, Regulierung und Privatrecht, 2016, 78 f. Teilweise wird lediglich diese regulatorische Funktion der Verbürgung privatautonomer Entscheidungen überhaupt als privatrechtskonform angesehen, so etwa bei *Zöllner*; anders etwa explizit *Collins*, Regulating Contracts, 1999, 8.

[67] Siehe nur *Grundmann*, JZ 2000, 1133 (1137 f.); ausführlich *Hacker*, Verhaltensökonomik und Normativität, 2017, 404 ff.

[68] Siehe im Einzelnen unten, Text bei § 3, Fn. 166 sowie § 4 B.–C., § 5 B.–C.

[69] Umfassend insoweit zur regulatorischen Dimension und einer „regulatorischen Rechtsdogmatik" *Hellgardt*, Regulierung und Privatrecht, 2016, 403 ff.; kritisch aufgenommen für digitale Inhalte etwa bei *Grünberger*, AcP 218 (2018), 213 (241 ff.), der jedoch letztlich für eine gegenüber ökonomischen, technologischen und soziologischen Irritationen offene „responsive Rechtsdogmatik" wirbt (ebd., insbesondere 245); kritisch gegenüber dieser wiederum *Riesenhuber*, AcP 219 (2019), 892 (905 ff.); Duplik von *Grünberger*, AcP 219 (2019), 924; siehe allgemein zu einer Verbindung von rechtlicher Methodik und interdisziplinären Erkenntnissen nur *Grundmann/Micklitz/Renner*, in: Grundmann/Micklitz/Renner (Hrsg.), Privatrechtstheorie, Band I, 2015, 1 (8 ff.); *Grünberger/Jansen*, in: Grünberger/Jansen (Hrsg.), Privatrechtstheorie heute, 2017, 1; *Auer*, Zum Erkenntnisziel der Rechtstheorie, 2018, besonders 43 ff., mit Diskussion der Digitalisierung 60–63; *Grundmann*, Pluralistische Privatrechtstheorie, Working Paper, 2020, jeweils m. w. N.

D. Problemaufriss und Aufbau der Untersuchung

Die Differenzierung zwischen ermöglichender und regulatorischer Funktion des Privatrechts wurde bislang jedoch, soweit ersichtlich, im Schnittbereich von Datenschutzrecht und Privatrecht noch nicht systematisch fruchtbar gemacht.[70] *Buchner* hat zwar in seiner 2006 erschienenen Habilitationsschrift den Wert der Privatautonomie für das zivilrechtlich orientierte Datenschutzrecht stark gemacht,[71] konnte aber zum einen naturgemäß das neue Datenschutzrecht der DS-GVO und des Entwurfs der ePrivacy-Verordnung noch nicht rezipieren und sparte zum anderen wesentliche Teile des Privatrechts, etwa die Rechtsgeschäftslehre[72] und die AGB-Kontrolle,[73] fast gänzlich aus.[74] Ein Ziel dieser Arbeit ist daher die Untersuchung verschiedener Normkomplexe des Datenschutzrechts und der angrenzenden Kernbereiche des Privatrechts, um die dogmatischen und funktionalen Wechselwirkungen beider Rechtsgebiete auszumessen, aber auch Fehlgewichtungen offenzulegen und Anpassungsvorschläge zu unterbreiten.

I. Regulierende und ermöglichende Strukturen im Datenprivatrecht

Forschungsbedarf besteht dabei sowohl mit Blick auf die regulatorischen als auch die ermöglichenden Strukturen im Spannungsfeld von Datenschutzrecht und Privatrecht. Die regulatorische Komponente des Privatrechts lässt sich verstehen als ein legislatorisches Risikomanagementsystem, das spezifische Risiken für sachbereichsrelevante Zielsetzungen adressiert und es unternimmt, diese sachadäquat zuzuweisen. Bekannt ist dieses Verständnis zum Beispiel im Gesellschafts- und Kapitalmarktrecht, wo etwa Wertpapierprospekt und Anlageberatung auf die Investmentrisiken zugeschnitten werden müssen,[75] § 91 Abs. 2 AktG den Vorstand zur Einrichtung eines Risikoüber-

[70] Das Datenschutzrecht etwa wird vollständig ausgeblendet von *Hellgardt*, Regulierung und Privatrecht, 2016 (siehe ebd., 165 ff.).

[71] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 103 ff.

[72] Siehe den kurzen Überblick bei *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 236–239 und, zur fehlenden Überblendung von Einwilligung und Rechtsgeschäftslehre, *Riesenhuber*, RdA 2011, 257 (258).

[73] Siehe die sehr knappen Ausführungen bei *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 251–253.

[74] Siehe nunmehr aber, zur AGB-Kontrolle von Einwilligungen, allerdings auch unter weitgehender Ausblendung der DS-GVO, dafür jedoch rechtsvergleichend *Langhanke*, Daten als Leistung, 2018, 183–220; zum deutschen Recht, unter Berücksichtigung der DS-GVO, auch bereits *Hacker*, ZfPW 2019, 148 (183 ff.).

[75] Siehe etwa Art. 7 Abs. 1 der Verordnung (EU) 2017/1129 des Europäischen Parlaments und des Rates vom 14. Juni 2017 über den Prospekt, der beim öffentlichen Angebot von Wertpapieren oder bei deren Zulassung zum Handel an einem geregelten Markt zu veröffentlichen ist, ABl. 2017 L 168/12; dazu etwa *Grundmann*, in: Staub, HGB, Bd. 11/1, Bankvertragsrecht/Investment Banking I, 5. Aufl. 2017, 6. Teil Rn. 115 f.; zur Zentralität der

wachungssystems für die Gesellschaft anhält[76] und Risikomanagement gar zu einem Eckpfeiler der Bankenregulierung nach der Finanzkrise wurde.[77] Auch im BGB weisen jedoch – dispositive oder zwingende – Normen und Rechtsfiguren häufig transaktions- oder handlungsrelevante Risiken zu, was nicht nur dem Interessenausgleich dient, sondern zumeist auch einen handlungslenkenden bzw. marktkorrigierenden und insoweit regulatorischen Einschlag hat.[78] So adressieren bekanntermaßen etwa die Zugangsregeln das Risiko der inkorrekten, verzögerten oder fehlgeschlagenen Übermittlung einer Willenserklärung,[79] Normen der AGB-Kontrolle Risiken der rationalen Ignoranz von Vertragsklauseln[80] und Zurechnungsnormen wie § 278 BGB das Personalrisiko im Kontext von bestehenden Schuldverhältnissen.[81] Diese Normen sind auch für das Datenprivatrecht unmittelbar relevant, man denke nur an die Übermittlung und Inhaltskontrolle einer Einwilligungserklärung. Risikoregulierung ist jedoch zunehmend auch im Kernbereich des unionalen Datenschutzrechts selbst beheimatet: Dieses hat sich mit besonderem Nachdruck seit Erlass der DS-GVO einem risikobasierten Regulierungsprinzip verpflichtet,[82] das Be-

Risikoadressierung in der Anlageberatung etwa *Hacker*, Verhaltensökonomik und Normativität, 2017, 749 ff.

[76] Ob darin eine echte Rechtspflicht zur Einrichtung eines umfassenden Risikomanagementsystems liegt (ablehnend etwa *Kort*, ZGR 2010, 440 [470]; bejahend etwa *Spindler*, in: MüKo, AktG, 5. Aufl. 2019, § 91 Rn. 23 f.), spielt hier keine tragende Rolle; zum Compliance-Beauftragten etwa *Renz/Frankenberger*, ZD 2015, 158 (159 f.); siehe auch Ziff. 4.1.4 des Deutschen Corporate Governance Kodex (Fassung vom 7.2.2017).

[77] Siehe nur den 14.–16. Erwägungsgrund der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über Aufsichtsanforderungen an Kreditinstitute und Wertpapierfirmen und zur Änderung der Verordnung (EU) Nr. 646/2012 (EU-Bankenaufsichtsverordnung – CRR), ABl. 2013 L 176/1; ferner den 4., 43., 44. und 51.–54. Erwägungsgrund der Richtlinie 2013/36/EU des Europäischen Parlaments und des Rates vom 26. Juni 2013 über den Zugang zur Tätigkeit von Kreditinstituten und die Beaufsichtigung von Kreditinstituten und Wertpapierfirmen (CRD IV), ABl. 2013 L 176/338; dazu umfassend *Renner*, Bankkonzernrecht, 2019, 137 ff.

[78] Siehe etwa zum regulatorischen Gehalt des kaufrechtlichen Gewährleistungsrechts *Hellgardt*, Regulierung und Privatrecht, 2016, 99 sowie zu weiteren Normen des BGB (z. B. den in dieser Arbeit relevanten §§ 134, 138, 305 ff. BGB) ebd., 92 ff. sowie 155 ff.

[79] Siehe repräsentativ *Dörner*, AcP 202 (2002), 363 (366 f.); *Einsele*, in: MüKo, BGB, 8. Aufl. 2018, § 130 Rn. 11; *Medicus/Petersen*, BGB AT, 11. Aufl. 2016, Rn. 269, sowie unten, § 5 B.II.2.c)bb).

[80] Siehe unten, § 5 C.II.1.e).

[81] Siehe unten, Text bei § 5, Fn. 1044.

[82] *Article 29 Data Protection Working Party*, Statement on the role of a risk-based approach in data protection legal frameworks, WP 218, 2014, 2; *Hustinx*, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, Working Paper, 2014, 38; *Gellert*, 5 International Data Privacy Law 2015, 3; *Lynskey*, The Foundations of EU Data Protection Law, 2015, 81 ff.; *Veil*, ZD 2015, 347 (348 ff.); *Renz/Frankenberger*, ZD 2015, 158 (160 f.); *Buchner*, DuD 2016, 155 (157); *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (182 f.); *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (682); *Schröder*, ZD 2019, 503 (503 ff.); zum Gesetzgebungsprozess diesbezüglich *Böhning*, ZD 2013, 421 (422); *Thoma*, ZD 2013, 578 (580); zur begrenzten Reichweite des risikobasierten Ansatzes unter Geltung des BDSG aF siehe *Thoma*, ZD 2013, 578

stand und Intensität von rechtlichen Pflichten in weiten Bereichen an die Existenz und den Grad von datenschutzspezifischen Risiken[83] anknüpft.[84]

Daher liegt es nahe, den Verbindungen risikobasierter Regulierung zwischen Datenschutz- und Privatrecht im Kontext der rechtsbereichsübergreifend heranwachsenden digitalen Wirtschaft nachzugehen. Dabei ist danach zu fragen, inwieweit aus der Verschränkung von unionalem Datenschutzrecht und teilweise unionsrechtlich geprägtem, teilweise jedoch auch rein national determiniertem Zivilrecht ein integriertes Marktordnungsrecht für die typischen Risiken der digitalen Wirtschaft, die mit fortschreitender Vernetzung und Datenverarbeitung einhergehen, geschaffen werden kann. Dies impliziert dogmatische Grundlagenarbeit, die *de lege lata* insbesondere die Wechselwirkungen und Friktionen zwischen verschiedenen Rechtsbereichen des Datenprivatrechts im europäischen Mehrebenensystem systematisch untersucht und Kriterien für ihr effektives, arbeitsteiliges Zusammenwirken entwickelt. Eine derartige methodische Verhältnisbestimmung ist aus zwei Gründen entscheidend. Erstens gilt es zu verhindern, dass die zunehmende Erstreckung der Datenverarbeitung auf alle Rechts- und Austauschbereiche das nationale Privatrecht zugunsten eines allumfassenden Datenschutzrechts – gleichsam als eines *law of everything*[85] – aushöhlt. Zweitens muss umgekehrt Sorge getragen werden, dass das nationale Privatrecht den Regelungsanspruch und die Harmonisierungswirkung des unionalen Datenschutzregimes nicht unterminiert.

Mit Blick auf die ermöglichende Dimension des Privatrechts wiederum ist zu konstatieren, dass der Stellenwert von autonomieförderlichen Ermöglichungsstrukturen im Privatrecht unbestritten ist,[86] dies vom Datenschutzrecht jedoch nicht im selben Umfang behauptet werden kann.[87] Parallel zur Entwicklung einer rechtsbereichsübergreifenden digitalen Marktordnung unternimmt es die

(580); zur praktischen Implementierung instruktiv *Loomans/Matz/Wiedemann*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems. Ein risikobasierter Ansatz für alle Unternehmensgrößen, 2014.

[83] Zu diesen Risiken im Einzelnen unten, § 3 B.II.

[84] Siehe Art. 23 Abs. 2 lit. g (Maßgaben für Beschränkungen von Betroffenenrechten), Art. 24 Abs. 1 (allgemeine Reichweite der Veranwortung des Verantwortlichen), Art. 25 Abs. 1 (Anforderungen des Datenschutzes durch Technikgestaltung), Art. 32 Abs. 1 und 2 (Anforderungen an die IT-Sicherheit), Art. 33 Abs. 1 (Meldung an Aufsichtsbehörde bei DS-GVO-Verletzung), Art. 34 Abs. 1 (Benachrichtigung Betroffener bei DS-GVO-Verletzung), Art. 35 Abs. 1 und Art. 36 Abs. 1 (Datenschutz-Folgenabschätzung); Art. 39 Abs. 2 (Erfüllung der Aufgaben durch den Datenschutzbeauftragten); und Art. 49 Abs. 1 lit. a DS-GVO (Übermittlung von personenbezogenen Daten ins EU-Ausland); ferner den 9., 28., 38., 39., 51., 71., und besonders den 74.–77., 80.–86, 90.–91 sowie den 94. Erwägungsgrund der DS-GVO.

[85] Dazu oben, § 1, Fn. 1.

[86] Siehe unten, Text bei § 5, Fn. 178 sowie § 6 A.

[87] Vorschläge zur Stärkung der Privatautonomie im Datenschutzrecht auch bei *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 313 f.; *Sattler*, JZ 2017, 1036 (1042 ff.); *Sattler*, in: Ochs et al. (Hrsg.), Die Zukunft der Datenökonomie, 2019, 1 (17 ff.).

Arbeit daher, im Datenprivatrecht eine Ermöglichungsebene aufzuspannen, die signifikante Wahlfreiheit verbürgt und die Ausübung von materieller Privatautonomie unterstützt – ein effektives, aber zugleich grundrechtssensibles Datenermöglichungsrecht. Klassischerweise ist das Instrument für die Ausübung von Privatautonomie im technikgeprägten Umfeld die datenschutzrechtliche Einwilligung.[88] Diese kommt jedoch unter den Bedingungen einer zunehmend vernetzten Lebensumgebung, wie sie die Konvergenz von Tracking-Technologien, maschinellem Lernen und Internet der Dinge in Richtung eines *Internet of Everything* aufbaut, mehr denn je an ihre Grenzen.[89] Verschiedene Typen von Marktversagen, gespeist aus klassisch-ökonomischen wie auch verhaltensökonomischen Effekten, erschweren in diesem Kontext zunehmend die sachgerechte Wahrnehmung von Privatautonomie.[90] Aber auch aus rechtspraktischer Perspektive weckt die bevorstehende Quasi-Ubiquität der – nur teilweise transparenten – Datenerhebung und -analyse Zweifel an der Zweckmäßigkeit hochfrequenter Einwilligungen in immer neue Verarbeitungsszenarien im privaten und öffentlichen Raum.[91] Vor diesem Hintergrund bedarf es neuer Wege, sowohl in Form der Re-Interpretation bestehenden Rechts als auch des Erlasses neuer Gesetzgebung, um der Wahrnehmung materieller Privatautonomie – wenigstens in einer residualen Form – zur Durchsetzung zu verhelfen. Das Datenschutzrecht muss auch ein Stück weit ein Datenermöglichungsrecht werden. Diese Ermöglichungsstrukturen müssen jedoch so konfiguriert werden, dass sie auch in Alltagssituationen funktionale und präferenzkonforme Ergebnisse liefern.[92]

II. Kurzüberblick über die drei Hauptteile der Arbeit

Die vorliegende Studie nimmt sich der soeben dargestellten Forschungsfragen in drei Hauptteilen an. Ausführliche Zusammenfassungen am Ende der jeweiligen Abschnitte stellen die wesentlichen Ergebnisse regelmäßig thesenhaft zusammen. Ein vierter Teil am Ende der Arbeit ordnet diese Ergebnisse noch einmal den zentralen rechtlichen Herausforderungen, denen sich die Arbeit stellt, zu und formuliert abschließende Thesen. In der Folge wird daher lediglich ein Überblick über die verschiedenen in der Arbeit behandelten Fragestellungen und den Aufbau der Untersuchung geboten.

---

[88] Siehe nur *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 231, 314; *Sattler*, in: Ochs et al. (Hrsg.), Die Zukunft der Datenökonomie, 2019, 1 (18); ferner unten, § 4 B.I.

[89] Siehe unten, § 4 B.I.5.a).

[90] Siehe unten, § 3 B.II.1. und § 4 B.I.5.a)aa)–bb).

[91] Siehe unten, § 4 B.I.5.a)cc).

[92] Siehe insbesondere unten, § 6 C.

1. Technische und ökonomische Grundlagen (Teil 1)

Der erste Teil legt die technischen und ökonomischen Grundlagen der Untersuchung. Um einen technologieadäquaten Regulierungsrahmen für datenbasierte Austauschprozesse zu entwickeln, müssen zunächst die drei dafür zentralen Basistechnologien – Tracking-Technologien, künstliche Intelligenz und das Internet der Dinge – jedenfalls in den technischen Grundzügen erfasst werden (§ 2). Dabei zeigt sich, dass gerade diese drei Technologieformen zunehmend miteinander kombiniert werden und das *Internet of Everything* zwar noch keine Realität, jedoch theoretischer und zunehmend auch praktisch approximierter Konvergenzpunkt dieser Verknüpfungsprozesse ist.[93]

Diese technische Basis wiederum dient als Grundlage für die Erarbeitung der drei zentralen rechtsökonomischen Problemstellungen der Arbeit, mit denen drei regulatorische Herausforderungen korrespondieren (§ 3). Ausgeklammert bleiben dabei jedoch Fragestellungen, die sich aus der digitalen Natur der vom Anbieter zur Verfügung gestellten Leistungsobjekte (digitale Güter/Inhalte/Dienstleistungen) ergeben;[94] die Untersuchung fokussiert sich vielmehr auf die Überlassung von *personenbezogenen* Daten im Rahmen von marktbasierten Austauschverhältnissen.

Erstens führt in diesem Kontext die zunehmende Nutzung von personenbezogenen Daten als funktionales Geldäquivalent zu einer Multirelationalität, welche die ökonomische Zuordnung der genannten Daten erschwert: Ihr ökonomischer Wert weist typischerweise über das primäre Vertrags- bzw. Nutzungsverhältnis zwischen betroffener Person und Erstanbieter hinaus.[95] Unter den Rahmenbedingungen komplexer, arbeitsteiliger, datenbasierter Austauschprozesse der digitalen Wirtschaft ist ihnen ein Drittbezug einbeschrieben, der sich nicht nur durch automatisierten Datenaustausch mit Werbeplattformen (sog. *ad exchanges*[96]) oder das Tracking durch Drittanbieter (sog. *third-party tracking*),[97] sondern auch durch die zunehmende Erfassung unbeteiligter Dritter durch die Analyseraster des Internets der Dinge manifestiert.[98] Dieser Drittbezug stellt das zumindest als Regelfall auf bilateralen Austausch angelegte Datenschutz- und Vertragsrecht vor signifikante Herausforderungen.

Zweitens eignet der hier thematischen vernetzten Datenerhebung und -verarbeitung, wie letztlich jeder neuen Technologie, eine spezifische Ambivalenz hinsichtlich ihrer Kosten und ihres Nutzens. So ist nicht zu verkennen, dass

---

[93] Siehe unten, § 2 D.

[94] Dazu repräsentativ *Auer*, ZfPW 2019, 130 (137 ff.); *Kuschel*, Der Erwerb digitaler Werkexemplare zur privaten Nutzung, 2019; *Grünberger*, AcP 218 (2018), 213 (223 ff.); *Obergfell*, Verträge über digitale Inhalte als Lizenzverträge, in: Verhandlungen des 71. Deutschen Juristentages, Band II/1, 2017, K 53; siehe ferner auch die Nachweise in § 1, Fn. 42.

[95] Siehe unten, § 3 A.III.

[96] Siehe unten, § 3 D.I.1. und § 4 A.II.2.a)aa)(2)(b)(a)a.

[97] Siehe unten, § 3 D.I.2.

[98] Siehe unten, § 3 D.I.3.

diese Prozesse einerseits erhebliches Potenzial sowohl auf individueller als auch sozialer Ebene bereithalten,[99] zugleich jedoch erhebliche Risiken generieren, die sich nicht nur in unterschiedlichen Typen von Marktversagen,[100] sondern auch von weitergehenden sozialen Risiken äußern.[101] Diese Spannung muss ein Rechtssystem, das sich gerade im Rahmen eines risikobasierten Regulierungsansatzes gegenüber den tatsächlichen Folgen der eigenen Regeln nicht verschließt, bewältigen.

Die dritte regulatorische Herausforderung schließlich besteht in der ausgeprägten Heterogenität der Datenschutzpräferenzen der jeweiligen Akteure, die zumeist nicht normal-, sondern U-förmig zwischen den beiden Polen – der schwachen und starken subjektiven Gewichtung der Relevanz datenschutzrechtlicher Risiken – verteilt sind.[102] Recht und Regulierung müssen sich daher einem heterogenen Adressatenpool anpassen. Dies bedeutet insbesondere, dass zur Ermöglichung der effektiven Wahrnehmung von Privatautonomie, inklusive der Durchsetzung heterogener Datenschutzpräferenzen, womöglich auch regulatorische Eingriffe in die Marktstruktur notwendig sind.[103]

Als Konsequenz aus dieser dreifachen Herausforderung entwickelt der Schluss des ersten Teils zwei Leitfragen für die genuin rechtliche Analyse des zweiten Teils:[104] Erstens ist zu untersuchen, welche Ressourcen das Datenschutz- und das Zivilrecht *de lege lata* zur Bewältigung der genannten Risiken bereithalten. Zweitens muss danach gefragt werden, ob hinreichende entscheidungsunterstützende Normen bereitstehen, um dem jeweiligen Akteur die effektive Wahrnehmung materieller Privatautonomie zu ermöglichen. Diese Forschungsfragen werden konkretisiert durch drei Leitfälle,[105] die ihrerseits den Drittbezug personenbezogener Daten betonen (Datenweiterleitung *an* Dritte, besonders bei personalisierter Werbung; Datenerhebung *durch* Dritte, besonders bei *third-party tracking*; Datenerhebung *bei* Dritten, besonders bei Unbeteiligten im Internet der Dinge) und die im weiteren Verlauf der Analyse immer wieder aufgegriffen werden.

2. *Datenschutzrecht und allgemeines Privatrecht (Teil 2)*

Der zweite Teil der Arbeit nimmt die genannten Leitfragen unmittelbar auf. Dies setzt zunächst eine detaillierte Untersuchung der Regelung vernetzter Datenerhebung und -analyse im neuen unionalen Datenschutzrecht voraus, die vor allem anhand der drei Leitfälle vollzogen wird (§ 4). Die 2012 mit

[99] Siehe unten, § 3 B.I.
[100] Siehe unten, § 3 B.II.1.
[101] Siehe unten, § 3 B.II.2.
[102] Siehe unten, § 3 C.
[103] Siehe insbesondere dann unten, § 6 C.II.
[104] Siehe unten, § 3 D.II.
[105] Siehe unten, § 3 D.I.

dem Kommissionsentwurf der DS-GVO[106] angestoßene Datenschutzrechtsreform hat zwar eine Stärkung der individuellen Kontrolle durch verschiedene, zum Teil auch neue, Ermöglichungsstrukturen zum Ziel gehabt.[107] Eine Diskussion des Einwilligungsregimes,[108] der Datenverarbeitung auf Grundlage eines Vertrags[109] sowie des neuen Rechts auf Datenübertragung[110] offenbart jedoch, gerade bei Berücksichtigung der in § 3 der Arbeit untersuchten Formen von Marktversagen, erhebliche Defizite bei der Ermöglichung der Wahrnehmung materieller Privatautonomie mit Blick auf vernetzte Datenverarbeitung.[111] Deutlich stringenter und wirkmächtiger sind demgegenüber die regulatorischen Strukturen des neuen Datenschutzrechts ausgestaltet, etwa die Interessenabwägungsklausel,[112] Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen,[113] sowie verschiedene Formen der Co-Regulierung.[114] Bei konsequenter Anwendung führen diese Instrumente nach hier vertretener Auffassung zu signifikanten rechtlichen Grenzen für Geschäftsmodelle, bei denen Daten als Gegenleistung fungieren.[115] Eine bedeutsame Ausnahme besteht insoweit jedoch hinsichtlich der in der DS-GVO im Wesentlichen ausgesparten Regulierung der Datenverarbeitung auf vertraglicher Grundlage.[116] Bereits daraus erhellt die notwendige Verknüpfung von Datenschutz- und allgemeinem Vertragsrecht.

Das folgende Kapitel (§ 5) widmet sich in der Konsequenz der Frage, ob das allgemeine Privatrecht einerseits im Datenschutzrecht bestehende Schutzlücken schließen und andererseits dort fehlende Ermöglichungsstrukturen bereitstellen kann. Dies bedingt jedoch zunächst eine prinzipielle, methodische Bestimmung des Verhältnisses von unionalem Datenschutzrecht und grundsätzlich nationalem, partiell jedoch unionsrechtlich determiniertem Privatrecht.[117] Hier zeigt sich, dass sowohl im Geltungsbereich des Anwendungsvorrangs des Unionsrechts[118] als auch bei Entwicklung einer sachlichen Verzahnung von Normgruppen, die derselben (unionalen oder nationalen) Regelungsebene ent-

[106] *Europäische Kommission*, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig.

[107] Siehe nur den 2. Satz des 7. Erwägungsgrunds der DS-GVO; ausführlich *Lynskey*, The Foundations of EU Data Protection Law, 2015, 177 ff.; *Borgesius*, Improving Privacy Protection in the Area of Behavioural Targeting, 2015, 53 ff.

[108] Siehe unten, § 4 B.I.

[109] Siehe unten, § 4 B.II.

[110] Siehe unten, § 4 B.III.

[111] Siehe unten, § 4 B.IV.

[112] Siehe unten, § 4 C.I.

[113] Siehe unten, § 4 C.III.

[114] Siehe unten, § 4 C.IV.

[115] Siehe unten, § 4 C.V. Punkt 10.

[116] Siehe unten, § 4 B.II.3.

[117] Siehe unten, § 5 A.

[118] Siehe unten, § 5 A.I.

springen,[119] jeweils das Kriterium der Risikospezifizität entscheidend ist: Insbesondere dann, wenn nationale Rechtsnormen eigenständige Risiken adressieren, können sie die Regelungsprärogative des Unionsrechts überwinden.[120] Zugleich können anhand dieses aus der Rechtsprechung des EuGH entwickelten Kriteriums unterschiedliche, unionsrechtlich determinierte Regelungsmaterien in ein sachgerechtes Verhältnis zueinander gebracht werden.[121]

An diese methodischen Überlegungen schließt sich die Untersuchung zunächst von ermöglichenden sowie in der Folge von regulatorischen Strukturen im Zivilrecht an. Für die Ermöglichungsstrukturen ist es zunächst essenziell, die datenschutzrechtliche Einwilligung in die zivilrechtliche Rechtsgeschäftslehre einzuordnen und so zu klären, inwieweit diesbezüglich auf allgemeine Tatbestands- und Wirksamkeitsvoraussetzungen von Willenserklärungen zurückgegriffen werden kann und muss.[122] Ferner muss exploriert werden, inwiefern der angesprochene Drittbezug von personenbezogenen Daten im Rahmen digitaler Austauschprozesse durch Rechtsfiguren des allgemeinen Zivilrechts erfasst werden kann, die – wie z. B. der mehrseitige Vertrag oder der Vertrag mit Schutzwirkung zugunsten Dritter – über die bilaterale Vertragsordnung hinausgehen.[123] Insgesamt zeigt sich dabei, dass das bestehende Zivilrecht die durch die verschiedenen Typen von Marktversagen bedingten Defizite der effektiven Wahrnehmung materieller Privatautonomie nur partiell kompensieren kann.

Im Rahmen der regulatorischen Strukturen des Zivilrechts wiederum ist zu untersuchen, inwiefern sich einerseits regulatorische Wertungen des Datenschutzrechts auf das Zivilrecht erstrecken (lassen), andererseits aber auch Schutzlücken des Datenschutzrechts, gerade im Bereich der Datenverarbeitung auf Grundlage eines Vertrags, durch das BGB geschlossen werden können. Aufgeworfen ist damit zunächst die Frage des Durchschlagens der Datenschutzrechtswidrigkeit auf die Wirksamkeit eines Rechtsgeschäfts, das die datenschutzrechtswidrige Verarbeitung zum Inhalt hat oder ermöglicht (§ 134 BGB).[124] Entgegen der bislang herrschenden Meinung kann hier zumindest bei Verträgen mit betroffenen Personen das Vertragsrecht bei teleologischer Auslegung von der (zumeist höchst rechtsunsicheren) datenschutzrechtlichen Beurteilung entkoppelt werden.[125] Eine stärkere Konvergenz der beiden Rechtsgebiete findet sich hingegen im Bereich der Inhaltskontrolle, etwa im Rahmen der AGB-Kontrolle,[126] aber auch bei § 138 BGB[127] und § 242 BGB.[128] Nichts-

[119] Siehe unten, § 5 A.II.
[120] Genauer unten, § 5 A.I.2.b)aa).
[121] Siehe unten, § 5 A.II.2.b)bb).
[122] Siehe unten, § 5 B.II.
[123] Siehe unten, § 5 B.III.2.
[124] Siehe unten, § 5 C.I.
[125] Siehe unten, § 5 C.I.1.
[126] Siehe unten, § 5 C.II.1.
[127] Siehe unten, § 5 C.II.2.
[128] Siehe unten, § 5 C.II.3.

destoweniger besteht auch hier Spielraum für eigenständige, über den bloßen Nachvollzug des Datenschutzrechts hinausgehende Wertungen des bürgerlichen Rechts. Insoweit kann die restriktive Rechtsprechung des BGH, wonach das Datenschutzrecht für derartige Fälle den alleinigen Maßstab der AGB-Kontrolle bietet, unter Geltung der DS-GVO nicht aufrechterhalten werden.[129]

Neben § 134 BGB und der Inhaltskontrolle bildet das Haftungsrecht eine dritte zentrale Verschränkungsmaterie von Datenschutzrecht und Zivilrecht,[130] bei der insbesondere der neue unionsrechtliche Schadensersatzanspruch gemäß Art. 82 DS-GVO nach hier vertretener Auffassung signifikante Verschiebungen vom nationalen ins unionale Haftungsrecht, etwa im Bereich des allgemeinen Persönlichkeitsrechts,[131] mit sich bringt. Insgesamt zeigt der zweite Teil der Arbeit damit, dass einerseits ein integriertes Verständnis der regulatorischen Komponenten von Datenschutz- und Zivilrecht nicht nur notwendig, sondern auch möglich ist, andererseits jedoch gerade bei der Ermöglichung der effektiven Wahrnehmung materieller Privatautonomie in datengeprägten Umgebungen noch erhebliche Defizite bestehen.

3. Reformperspektiven (Teil 3)

Dieser Befund ist Grundlage für die im dritten Teil der Arbeit erarbeiteten Reformperspektiven, die sich jedoch nicht in rechtspolitischen Vorschlägen *de lege ferenda* erschöpfen, sondern auch konkrete Anregungen zur Neuinterpretation bestehenden Rechts *de lege lata* beinhalten. Zentrales Desiderat ist es dabei, durch bewusste Wahl der rechtlichen Rahmenbedingungen Technik so zu gestalten, dass heterogene Datenschutzpräferenzen möglichst effektiv zur Durchsetzung gebracht werden können. Dies setzt wiederum zunächst eine Klärung des begrifflichen Verhältnisses von Autonomie, Informiertheit und Datenschutzpräferenzen voraus.[132]

Auf dieser Grundlage wird dann entfaltet, inwieweit Technik von Nutzern selbst zur Minimierung von Datenschutzrisiken im Rahmen des Selbstdatenschutzes genutzt werden kann.[133] Hier zeigt sich jedoch sowohl bei der Diskussion von *privacy-enhancing technologies*[134] als auch von Formen der Rechtmäßigkeitskontrolle durch Applikationen maschinellen Lernens,[135] dass die Anreize zur Nutzung dieser Technologien bislang noch zu gering und die technischen Beschränkungen, trotz erheblicher Forschungsanstrengungen und Fortschritte in jüngerer Vergangenheit, gegenwärtig noch zu hoch sind. Auch die nunmehr in Art. 25 DS-GVO verankerte Rechtspflicht zu *data protection by*

[129] Siehe unten, § 5 C.II.1.a).
[130] Siehe unten, § 5 C.III.
[131] Siehe unten, § 5 C.III.4.a).
[132] Siehe unten, § 6 A.
[133] Siehe unten, § 6 B.
[134] Siehe unten, § 6 B.I.
[135] Siehe unten, § 6 B.II.

design and default hat insoweit noch keine durchschlagende Wirkung zeitigen können. Erhebliches Potenzial haben jedoch vor allem die Nutzung automatisierter Analyseinstrumente durch Aufsichtsbehörden und durch mit Klagebefugnis ausgestattete Verbraucher- oder Wettbewerbsverbände zur schnellen und skalierbaren Identifizierung von Rechtsverstößen.[136]

Code tritt damit zunehmend als weitere Kontrollinstanz neben Nutzer, Behörden und Gerichte. Auf die datenschutzrechtliche Einwilligung gewendet, bedeutet dies: Die informierte Einwilligung muss von der *technologischen Einwilligung* abgelöst werden. Der letzte Abschnitt der Arbeit zielt daher darauf, die notwendige rechtliche Infrastruktur für ein derartig maschinell mediiertes Einwilligungsregime zu beschreiben. Denn technische Ansätze können die Datensouveränität von Nutzern zwar stärken, aber nicht alleine garantieren. Sie müssen vielmehr präziser als bislang durch rechtliche Strukturen unterstützt werden, um signifikante Wirkung zu erzielen. Daher wird zunächst aufgezeigt, welche Möglichkeiten zur Verbesserung des bestehenden Einwilligungsregimes bestehen.[137] Hier lassen sich grundsätzlich transparenz-, verhaltens- und technologiebasierte Ansätze unterscheiden. Kernelement für eine Bewältigung der Anforderungen und Spannungslagen einer sich auf ein *Internet of Everything* zubewegenden Vernetzungsrealität ist dabei ein technologiebasierter Ansatz, bei dem Techniken maschinellen Lernens zur Modellierung von Datenschutzpräferenzen und zur darauf basierenden automatisierten oder gar autonomen Kommunikation dieser Präferenzen an datenverarbeitende Applikationen und Geräte im privaten und öffentlichen Raum eingesetzt werden.[138] Nach hier vertretener Auffassung können diese Präferenzen bereits auf Grundlage des bestehenden Rechts auch bei Einsatz von stark autonom agierenden Datenschutzassistenten rechtswirksam kommuniziert werden.[139]

Auch eine technologisch unterstützte, rechtswirksame Kommunikation von Datenschutzpräferenzen kann jedoch nur insoweit fruchten, wie tatsächlich Möglichkeiten zur Durchsetzung dieser Präferenzen am Markt angeboten werden. Dies ist gegenwärtig in zentralen Bereichen der digitalen Wirtschaft nicht oder nicht ausreichend der Fall. Daher endet die Untersuchung mit der Ausarbeitung eines sektorspezifischen Rechts der Nutzer auf eine datenschonende Option.[140] Dieses Recht muss jedoch, anders als bislang in der Literatur diskutiert, mit der verpflichtenden Angabe eines *privacy score* verbunden werden, um so Vergleichbarkeit zwischen den verschiedenen am Markt befindlichen Optionen – seien sie datenintensiver oder datenschonender Natur – herzustellen.[141] Nur so kann der marktwirtschaftliche Preismechanismus, der

[136] Siehe unten, § 6 B.II.3.
[137] Siehe unten, § 6 C.I.
[138] Siehe unten, § 6 C.I.3.
[139] Siehe unten, § 6 C.I.3.c)aa).
[140] Siehe unten, § 6 C.II.
[141] Siehe unten, § 6 C.II.1.b)bb).

im Zentrum der dezentralen Koordinierung des Wirtschaftsgeschehens steht, unter den Bedingungen der digitalen Wirtschaft seine Steuerungskraft wieder voll entfalten. Die Verquickung einer datenschonenden Pflichtoption mit einem derartigen Privatheitsindex verspricht daher, nicht nur heterogenen Datenschutzpräferenzen gerecht zu werden, sondern auch zentralen Formen des Marktversagens im Bereich der digitalen Wirtschaft wirksam entgegenzutreten.[142] Verbunden mit einer rechtlichen Förderung von digitalen Instrumenten der Präferenzkommunikation kann damit – so die Hoffnung – materielle Privatautonomie unter den Bedingungen unserer vernetzten Wirklichkeit zumindest in einer technologisch gestützten Residualform aufrechterhalten werden.

[142] Siehe unten, § 6 C.II.1.c)dd).

Teil 1

Technische und ökonomische Grundlagen

§ 2 Technische Grundlagen moderner Informationsverarbeitungssysteme

Die technischen Grundlagen moderner Informationsverarbeitungssysteme sind vielfältig. Für den im Zentrum dieser Arbeit stehenden Kern der verbraucherorientierten digitalen Wirtschaft können jedoch drei zentrale technologische Neuerungen identifiziert werden, die auf unterschiedliche Weise miteinander verbunden sind und das aus personenbezogenen Daten gespeiste wirtschaftliche Ökosystem grundieren. Zunächst müssen Daten überhaupt einmal erhoben werden, was vor allem durch verschiedene Tracking-Instrumente geschieht (A.). Die Analyse dieser Daten vollzieht sich dann zunehmend unter Einsatz von Techniken maschinellen Lernens (B.). Eine Rückkopplung an die Handlungssphäre des Nutzers erfolgt jedoch nicht nur über datenbasierte Angebote (etwa personalisierte Werbung), sondern auch unmittelbar technophysisch durch Aktuatoren, die in Geräte des Internets der Dinge eingebettet sind (C.). Diese „intelligenten" Geräte können allerdings nicht lediglich Signale in reale Handlungsimpulse umsetzen; sie erheben typischerweise auch selbst personenbezogene Daten. Damit schließt sich der Kreis. Zudem sind verstärkt Konvergenzen zwischen den drei genannten technologischen Typen zu gewärtigen (*Internet of Everything*, D.).

A. Tracking-Instrumente

Anbieter von datenbasierten Austauschverhältnissen können Daten über ihre Kunden auf verschiedenen Wegen gewinnen. Zunächst ist hier an die bewusste Überlassung von Daten durch die jeweiligen Nutzer zu denken, zum Beispiel beim Ausfüllen eines Registrierungsformulars oder einer Bestellung im Internet, beim Posten in einem sozialen Netzwerk oder der Eingabe eines Suchbegriffs.[1] Für die rechtliche Analyse besonders bedeutsam ist jedoch, dass auch darüber hinaus, für die Nutzer häufig in nur deutlich reduziertem Maße erkennbar, Nutzerdaten erhoben werden mithilfe einer Reihe von Tracking-Technologien.

[1] Siehe nur *Metzger*, AcP 216 (2016), 817 (821).

Diese Instrumente sind sowohl auf Webseiten als auch in Smartphone-Apps und IoT-Geräten weit verbreitet.[2] Daran hat auch die DS-GVO nichts geändert.[3] Sie bilden das technologische Rückgrat der werbefinanzierten digitalen Wirtschaft. Innerhalb der Tracking-Technologien unterscheidet man typischerweise zwischen *first-party tracking* und *third-party tracking*.[4] Bei ersterem findet die Datenerhebung durch ein Unternehmen statt, mit dem ein primäres Nutzungsverhältnis besteht, innerhalb dessen der Nutzer agiert (Betreiber der Webseite oder App, die man besucht/nutzt; Inhaber des Ladenlokals, in dem man einkauft). *Third-party tracking* erfolgt hingegen durch Drittunternehmen außerhalb des primären Nutzungsverhältnisses.

Unabhängig von ihrem Einsatz durch Erstanbieter[5] oder Drittanbieter lassen sich Tracking-Instrumente in drei unterschiedliche Gruppen einteilen:[6] Cookies, *fingerprinting* und sonstige geräteeigene eindeutige Kennungen (*unique strings*).[7] Gemeinsam können diese Tools als Geräte-Identifier bezeichnet werden.[8] Sie werden hier nur überblicksartig vorgestellt, weitere Einzelheiten werden jeweils dort beleuchtet, wo sie rechtlich relevant werden.

I. Cookies

Cookies sind kleine Textdateien, die mit einer eindeutige Kennung versehen sind, auf dem Computer, aber auch auf einem Smartphone, platziert werden können[9] und die typischerweise Informationen über den Besuch einzelner

---

[2] *Acar et al.*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security 2014, 674.

[3] *Sørensen/Van den Bulck/Kosta*, Privacy Policies Caught Between the Legal and the Ethical: European Media and Third Party Trackers Before and After GDPR, Working Paper, 2019, https://ssrn.com/abstract=3427207; *Degeling et al.*, 26th Annual Network and Distributed System Security Symposium (NDSS '19), 1; *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (1); *Aridor et al.*, The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR, NBER Working Paper No. w26900, 2020, https://www.nber.org/papers/w26900.

[4] Die Übergänge können insbesondere in einem durch eine Vielzahl an Spielern geprägten Angebots- und Marketingumfeld fließend sein; als grobe Kategorisierung hat die Unterscheidung jedoch weiterhin heuristischen Wert; siehe etwa *Mellet/Beauvisage*, Consumption Markets & Culture 2019, 1 (8).

[5] Als Erstanbieter werden diejenigen Anbieter bezeichnet, welche die primär vom Nutzer nachgefragte Leistung anbieten, also etwa den Inhalt einer Webseite bereitstellen; siehe auch unten, § 5, Fn. 338, zu IoT-Konstellationen.

[6] Dies gilt für die Online-Tracking-Tools. Hinzu kommen die Offline-Tracking-Tools über WLAN, Bluetooth o. Ä. (*beacons*), siehe unten, § 2, Fn. 25, die jedoch ebenfalls typischerweise eindeutige Kennungen vergeben.

[7] *Hanloser*, ZD 2018, 213 (213).

[8] *Hanloser*, ZD 2018, 213.

[9] *European Commission*, Cookies, in: The EU Internet Handbook, http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm; *Ryte Wiki*, Third Party Cookies, https://de.ryte.com/wiki/Third_Party_Cookies.

Webseiten oder die Nutzung einzelner Apps speichern oder übermitteln.[10] Diese Instrumente werden durch den Betreiber der Webseite oder der App eingebunden und übermitteln dann selbstständig Informationen unmittelbar an den Anbieter des Cookies. Ist dieser nicht mit dem Betreiber identisch, so spricht man von Drittanbietercookies. Typischerweise abgefragte Informationen umfassen die IP-Adresse, den Zeitpunkt des Zugriffs und Browserkonfigurationen, ferner verschiedene Maße des Nutzerverhaltens.[11] Ähnlich funktionieren Zählpixel, die ebenfalls in Webseiten eingebunden werden und Daten direkt an den Anbieter des Pixels übertragen.[12]

Ein praktisch und rechtlich äußerst relevantes Beispiel für die Nutzung von Cookies bilden Social Plug-Ins, die in Webseiten oder Apps von Drittanbietern integriert sind. Wenn etwa der Like Button von Facebook auf einer Zeitungwebseite erscheint, so sammelt Facebook über Drittanbietercookies, welche durch das Social Plug-In gesetzt werden,[13] Daten von den Besuchern der Zeitungswebseite, auch wenn das Plug-In gar nicht angeklickt wird.[14] Dies geschieht nicht nur bei Personen, die ein eigenes Facebook Konto unterhalten, sondern auch bei jenen, bei denen das nicht der Fall ist, auch wenn diese Nutzer auch sonst keinen Bezug zu Facebook haben.[15] Dabei wird die Datenerhebung automatisch gestartet, da ein Social Plug-In typischerweise über ein iframe, eine Art kleiner Webseite in der Hauptwebseite,[16] durch den Erstanbieter in die Hauptseite eingebettet wird und das iframe nicht nach Nutzergruppen differenziert.[17]

---

[10] BGH ZD 2017, 49 Rn. 15; *Hanloser*, ZD 2018, 213 (214); *Mellet/Beauvisage*, Consumption Markets & Culture 2019, 1 (7).

[11] *Acar et al.*, Facebook Tracking Through Social Plug-ins. Technical report prepared for the Belgian Privacy Commission, 2015, 14.

[12] Dies sind Objekte, die in Größe eines einzelnen Pixels in eine Webseite integriert und bei deren Aufruf automatisch geladen werden, so dass in einem Logfile verschiedene Daten über den Besucher festgehalten werden können; siehe *Kervizic*, Cookies, Tracking and pixels: Where does your Web data comes from?, Medium (22.10.2018), https://medium.com/analytics-and-data/cookies-tracking-and-pixels-where-does-your-web-data-comes-from-ff5d9b8bc8f7; *Steidle/Pordesch*, DuD 2008, 324 (325); *Ryte Wiki*, Tracking Pixel, https://de.ryte.com/wiki/Tracking_Pixel.

[13] Siehe dazu *Acar et al.*, Facebook Tracking Through Social Plug-ins, Technical report prepared for the Belgian Privacy Commission, 2015, 6, 14; *Schleipfer*, DuD 2014, 318 (319, 321); siehe auch GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 40; *Steidle/Pordesch*, DuD 2008, 324 (325); *Clifford*, 5 JIPITEC 2014, 194 (195).

[14] *Data Protection Commissioner*, Facebook Ireland Ltd, Report of Audit v. 21.12.2011, 52; *Acar et al.*, Facebook Tracking Through Social Plug-ins, Technical report prepared for the Belgian Privacy Commission, 2015, 5 ff.; Bundeskartellamt, Fallbericht v. 15.2.2019, Az. B6–22/16 (*Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung*), 3 f.

[15] *Schleipfer*, DuD 2014, 318 (319, 321); *Acar et al.*, Facebook Tracking Through Social Plug-ins, Technical report prepared for the Belgian Privacy Commission, 2015, 6.

[16] Siehe *Wikipedia*, Inlineframe, https://de.wikipedia.org/wiki/Inlineframe.

[17] *Data Protection Commissioner*, Facebook Ireland Ltd, Report of Audit v. 21.12.2011,

II. Fingerprinting-Techniken

Das Setzen von Cookies kann durch den Nutzer mit unterschiedlich großem Aufwand unterbunden werden. Dies ist deutlich schwerer[18] beim *fingerprinting*,[19] bei dem verschiedene Informationen über die Gerätekonfiguration (z. B. die Textdarstellung beim *canvas fingerprinting*[20]) durch einen Fingerprinting-Algorithmus abgefragt und noch im Endgerät durch den Prozessor zu einer Zeichenfolge (*hash*) verbunden werden.[21] Diese wird an den Anbieter gesendet und ermöglicht, bei konstanter Gerätekonfiguration, eine Identifikation des Nutzergeräts.[22] *Fingerprinting* ist auch bei IoT-Geräten möglich.[23]

III. Sonstige eindeutige Kennungen

Schließlich werden insbesondere bei Smartphones durch das Betriebssystem oder einzelne Apps eindeutige Zahlenkombinationen (*unique strings*) vergeben, die Werbetreibende zur Identifikation des Gerätes nutzen können.[24] Diese haben auch besondere Bedeutung, um Daten außerhalb des Onlineverhaltens zu erheben. So werden etwa sogenannte *bluetooth beacons* von stationären Anbietern (zum Beispiel ein Bekleidungsgeschäft) eingesetzt, um lokationsbasiert das Verhalten von Smartphonebesitzern nachzuvollziehen.[25]

All diesen Techniken ist gemein, dass sie einerseits durch den durchschnittlichen Nutzer nicht bemerkt werden, sie andererseits aber auf Informationen

81; *Schleipfer*, DuD 2014, 318 (319, 321); *mip Consult GmbH*, Social Plugins für Unternehmen, Blog Sofortdatenschutz (5.4.2018), https://blog.sofortdatenschutz.de/social-plug-ins/.

[18] *Acar et al.*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security 2014, 674 (684).

[19] Zu dieser Technik grundlegend *Kohno/Broido/Claffy*, 2 IEEE Transactions on Dependable and Secure Computing 2005, 93; *Nikiforakis et al.*, IEEE Symposium on Security and Privacy 2013, 541; *Mowery/Shacham*, Proceedings of W2SP 2012, 1.

[20] *Mowery/Shacham*, Proceedings of W2SP 2012, 1.

[21] *Mowery/Shacham*, Proceedings of W2SP 2012, 1 (2); *Acar et al.*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security 2014, 674 (675 f.).

[22] Siehe etwa *Cao et al.*, NDSS 2017, 1; *Hanloser*, ZD 2018, 213 (214); *Karg/Kühn*, ZD 2014, 285 (286 f.); *Schmidt/Babilon*, K&R 2016, 86 (86).

[23] *Yang*, 4 IEEE Internet of Things Journal 2017, 1250 (1254); *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 9.

[24] Werbe-ID bei Android, Ad-ID bei iOS, weitere persistente IDs durch Apps selbst, siehe *Reyes et al.*, Proceedings on Privacy Enhancing Technologies 2018 (3), 63 (73); *Hanloser*, ZD 2018, 213 (214).

[25] Siehe *Faragher/Harle*, 33 IEEE Journal on Selected Areas in Communications 2015, 2418; *Kwet*, In Stores, Secret Surveillance Tracks Your Every Move, New York Times (14.6.2019), https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html; *Yanofsky*, Google can still use Bluetooth to track your Android phone when Bluetooth is turned off, Quartz (24.1.2018), https://qz.com/1169760/phone-data/; zur Erfassung von *beacons* durch die ePrivacy-VO unten, Text bei § 4, Fn. 864.

aus dem jeweiligen Endgerät zugreifen, um dieses über eine gewisse Zeitspanne hinweg zu identifizieren. Dies kann für die Nutzung einer Webseite oder App notwendig sein, der Personalisierung des Produkts selbst oder aber Werbezwecken dienen. Diese Multifunktionalität von Tracking-Instrumenten wird uns im Rahmen der rechtlichen Bewertung noch beschäftigen. Sie sind jedenfalls essenziell für die breitflächige *Erhebung* von Daten in der digitalen Wirtschaft.

B. Künstliche Intelligenz: Techniken maschinellen Lernens

Demgegenüber werden für die *Datenanalyse* zunehmend Techniken maschinellen Lernens eingesetzt.[26] Dabei handelt es sich um die gegenwärtig bedeutendste Ausformung von Methoden, die der künstlichen Intelligenz zugerechnet werden.

I. Begriffe

Auf einen einheitlichen Begriff der künstlichen Intelligenz hat man sich bis heute nicht verständigen können.[27] Auch wenn die ersten der künstlichen Intelligenz zuzurechnenden Arbeiten bereits in den 1940er Jahren erfolgten (*cybernetics*),[28] wurde der Begriff „Artificial Intelligence" erst bei der Vorbereitung der im Jahr 1956 abgehaltenen „Dartmouth Conference" geprägt,[29] die den Grundstein für die systematische Erforschung computergetriebener Techniken legte, die verschiedene Aspekte typisch menschlicher Verhaltensweisen selbständig und adaptiv imitieren oder gar übertreffen können.[30]

---

[26] Die folgende Darstellung orientiert sich an der Primärliteratur aus dem Informatik. Für weitere Überblicke aus der rechtswissenschaftlichen Literatur siehe auch *Zech*, Risiken digitaler Systeme, Weizenbaum Series #2, 2020, 11 ff., 27 ff., 42 ff.; *Zech*, ZfPW 2019, 198 (199 ff.); *Ashley*, Artificial Intelligence and Legal Analytics, 2017, 107 ff.; speziell zu künstlichen neuronalen Netzen *Ehinger/Stiemerling*, CR 2018, 761 (762 ff.).

[27] *Rich/Knight/Nair*, Artificial Intelligence, 3. Aufl. 2009, 3; *Russell/Norvig*, Artificial Intelligence, 3. Aufl. 2010, 2.

[28] So etwa das sogenannten *McCulloch-Pitts*-Neuron, eine vom menschlichen Gehirn inspirierte künstliche neuronale Struktur, deren Entscheidungsgewichte händisch gesetzt und adaptiert werden konnten, *McCulloch/Pitts*, 5 Bulletin of Mathematical Biophysics 1943, 115; die Beschreibung der Grundarchitektur eines künstlichen neuronalen Netzes durch *Turing*, Intelligent Machinery, Report, 1948 („unorganized machines"), posthum abgedruckt in Copeland (Hrsg.), The Essential Turing, 2004, 410 (siehe besonders 416–418); siehe insgesamt *Russell/Norvig*, Artificial Intelligence, 3. Aufl. 2010, 16 f.; *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 12 ff.

[29] *McCarthy et al.*, A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, 1955.

[30] *Russell/Norvig*, Artificial Intelligence, 3. Aufl. 2010, 17.

Heutige Definitionen des Begriffs der künstlichen Intelligenz sind, bei allen Binnendifferenzen, regelmäßig anthropozentrisch konfiguriert.[31] Sie heben hervor, dass es um die Fähigkeit von Computern geht, menschlich zu denken[32] oder zu handeln[33] bzw. rational zu denken[34] oder intelligent zu handeln.[35] Messbar gemacht werden können diese Eigenschaften typischerweise durch verschiedene Formen eines sogenannten Turing-Tests.[36] Dessen ursprüngliche Konzeption durch *Alan Turing* sieht vor, dass ein Mensch im Verlauf einer fünfminütigen, schriftlichen Korrespondenz mit einem Computer anhand der Antworten nicht zuverlässig erkennen können darf, dass es sich nicht um einen menschlichen Dialogpartner handelt.[37]

Das Spektrum der Techniken, die zur künstlichen Intelligenz zählen, ist breit. Dazu werden auch Expertensysteme (*knowledge bases*) gerechnet, bei denen Personen mit spezifischem Fachwissen Datenbanken mit umfassenden, bereichsspezifischen Regeln befüllen, sodass auch komplexere Fragestellungen durch logische Inferenzregeln automatisiert bearbeitet werden können.[38] Für diese Anwendungen ist jedoch eine ganz erhebliche Menge an bereichsspezifischem Wissen notwendig, das in mühsamer Kleinarbeit in eine Datenbank eingepflegt und regelbasiert extrahiert werden muss.[39]

Auf dieses Erfordernis verzichten die heute dominierenden Techniken maschinellen Lernens, bei denen die relevanten Verknüpfungen vom algorithmischen Modell selbst auf der Grundlage von exemplarischem Anschauungsmaterial erstellt werden.[40] Die Erkenntnis dieser Möglichkeit sich zu einem hohen Grade selbst optimierender Prozesse setzte einen ganz erheblichen Innovations- und Performanceschub frei, der bis heute anhält.[41] Die Grundlagen für

---

[31] Überblick bei *Russell/Norvig*, Artificial Intelligence, 3. Aufl. 2010, 2 ff.

[32] *Haugeland*, Introduction, in: id. (Hrsg.), Artificial Intelligence. The Very Idea, 1985, 1 (2).

[33] *Rich/Knight/Nair*, Artificial Intelligence, 3. Aufl. 2009, 3.

[34] *Winston*, Artificial Intelligence, 3. Aufl. 1992, 5; vgl. auch *Charniak/McDermott*, Introduction to Artificial Intelligence, 1985, 6 („study of mental faculties").

[35] *Poole/Mackworth*, Artificial Intelligence, 2010, 3 f.; *Nilsson*, Artificial Intelligence, 1998, 1.

[36] Überblick bei *Shieber* (Hrsg.), The Turing Test, 2004; zu heutigen Adaptationen auch *Grosz*, 33(4) AI Magazine 2012, 73 (78 ff.).

[37] *Turing*, 59 Mind 1950, 433 (442). Der genaue Wortlaut ist: „I believe that in about fifty years' time it will be possible to programme computers with a storage capacity of about 10^9 to make them play the imitation game so well that an average interrogator will not have more than 70 per cent. chance of making the right identification after five minutes of questioning. The original question, ‚Can machines think?' I believe to be too meaningless to deserve discussion. Nevertheless I believe that at the end of the century the use of words and general educated opinion will have altered so much that one will be able to speak of machines thinking without expecting to be contradicted."

[38] *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 2, 9; *Russell/Norvig*, Artificial Intelligence, 3. Aufl. 2010, 22 f.

[39] *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 2.

[40] *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 2 f.

[41] Zu den spezifischen Bedingungen der gegenwärtigen, dritten Forschungswelle im Be-

Techniken maschinellen Lernens wurden allerdings bereits im 20. Jahrhundert, besonders während der konnektivistischen Welle der 1980er Jahre,[42] gelegt.[43] So stammt die klassische Definition maschinellen Lernens aus einem Lehrbuch von *Mitchell* aus dem Jahr 1997: „A computer program is said to learn from experience *E* with respect to some tasks *T* and performance measure *P*, if its performance at tasks in *T*, as measured by *P*, improves with experience *E*."[44]

II. Strategien und Modelle maschinellen Lernens

Das Lernergebnis wird bei Techniken maschinellen Lernens grundsätzlich so erzielt, dass das Modell eine Menge an Eingabedaten (*input*) analysiert und daraus nach einem bestimmten Lernalgorithmus ein Ergebnis (*output*) errechnet, das zum Beispiel eine bestimmte Größe, Wahrscheinlichkeit oder Handlungsstrategie darstellen kann.

1. Lernstrategien

Je nach Beschaffenheit des Lernalgorithmus und der Lernumgebung unterscheidet man dabei zwischen überwachtem (*supervised learning*), unüberwachtem (*unsupervised learning*) und Verstärkungslernen (*reinforcement learning*),[45] wobei auch Mischformen implementiert werden können.[46]

a) Überwachtes Lernen (*supervised learning*)

Beim überwachten Lernen errechnet das Modell zunächst aus den Eingabewerten der Trainingsdaten (*input*) für eine Reihe von Beispielen mögliche Ergebnis-

---

reich künstlicher Intelligenz, die etwa 2006 mit Entwicklungen im Bereich *deep learning* begann, siehe *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 18 ff.; ferner auch *Russell/Norvig*, Artificial Intelligence, 3. Aufl. 2010, 27 f.; knapp auch *LeCun/Bengio/Hinton*, 521 Nature 2015, 436 (438).

[42] Dazu *Russell/Norvig*, Artificial Intelligence, 3. Aufl. 2010, 24 f.

[43] Siehe etwa *Widrow/Hoff*, Adaptive Switching Circuits, Technical Report No. 1553–1, 1960 für eine Spezialform des Lernalgorithmus *stochastic gradient descent*; *Hinton*, Proceedings of the Eighth Annual Conference of the Cognitive Science Society 1986, 1 zu *distributed representations* von Analyseobjekten; *Rumelhart/Hinton/Williams*, 323 Nature 1986, 533 zum Lernalgorithmus *back-propagation*. All diese Techniken kommen bis heute beim Training von neuronalen Netzen als Standardverfahren zum Einsatz, siehe *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 147 ff., 197 ff., 536 ff.; *LeCun/Bengio/Hinton*, 521 Nature 2015, 436 (436 f., 440 f.).

[44] *Mitchell*, Machine Learning, 1997, 2.

[45] *Russell/Norvig*, Artificial Intelligence, 3. Aufl. 2010, 694 f.; *Shalev-Shwartz/Ben-David*, Understanding Machine Learning, 2014, 4 f.; *Jordan/Mitchell*, 349 Science 2015, 255 (257 f.); *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 102 f.; *Sutton/Barto*, Reinforcement Learning, 2. Aufl. 2018, 2.

[46] Dies ist etwa beim *semi supervised learning* der Fall, siehe *Dai/Le*, Advances in Neural Information Processing Systems 2015, 3079; *Rasmus et al.*, Advances in Neural Information Processing Systems 2015, 3546.

se (*output*).[47] Es bestimmt so zum Beispiel in erster Näherung einen Kreditwürdigkeits-Score[48] (*regression*: numerische Variable[49]) oder die Art von auf Bildern dargestellten Tieren (*classification*: kategoriale Variable[50]). Diese Ergebnisse des ersten Rechendurchlaufs werden nun mit den tatsächlich korrekten Ergebnissen verglichen, die – und das ist entscheidend – beim überwachten Lernen ebenfalls vorliegen, etwa in Form tatsächlicher Messungen oder menschlicher Annotationen.[51] Aus der Differenz von Vorhersage und tatsächlich korrektem Ergebnis wird mithilfe der Verlustfunktion (*loss function*) eine Fehlergröße errechnet.[52] Ein Lernalgorithmus sorgt nun dafür, dass die internen Gewichte (*weights*) des algorithmischen Modells, mit denen verschiedene Eigenschaften (*features*) der jeweiligen Beispiele als mehr oder weniger relevant ausgewiesen werden, so verändert werden, dass die Ergebnisse beim nächsten Trainingsdurchlauf näher an den korrekten Ergebnissen liegen.[53] Schrittweise wird so nach einem Minimum der Verlustfunktion gesucht.[54] Derart wird über viele Iterationen hinweg das Modell anhand der vorhandenen Beispiele (*training set*) trainiert.[55] Die korrekten Zielgrößen „überwachen" mithin das Training des Modells. Ob die so gefundene Anordnung der internen Gewichte des Modells auch belastbare Ergebnisse über den Trainingsdatensatz hinaus liefert, überprüfen die Entwickler sodann anhand für das Modell noch unbekannter Beispiele (*test set*).[56] Dies wird insgesamt so lange wiederholt (*cross-validation*),[57] bis die Performancemaße[58] ein gewünschtes Niveau erreicht haben. Beispiele für Anwendungen überwachten Lernens sind Modelle zur Gesichts-[59] und

---

[47] *Jordan/Mitchell*, 349 Science 2015, 255 (257); *Russell/Norvig*, Artificial Intelligence, 3. Aufl. 2010, 695.

[48] Siehe zu Algorithmen im Bereich *credit scoring* den Überblick bei *Lessmann et al.*, 247 European Journal of Operational Research 2015, 124.

[49] *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 98; ausführlich *James et al.*, An Introduction to Statistical Learning, 2013, 59 ff.

[50] *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 97; ausführlich *James et al.*, An Introduction to Statistical Learning, 2013, 127 ff.

[51] *Shalev-Shwartz/Ben-David*, Understanding Machine Learning, 2014, 4; *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 102.

[52] *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 79, 107.

[53] Siehe die Nachweise zu Lernalgorithmen in § 2, Fn. 43.

[54] *LeCun/Bengio/Hinton*, 521 Nature 2015, 436 (436 f.); *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 79 ff.

[55] *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 107.

[56] *LeCun/Bengio/Hinton*, 521 Nature 2015, 436 (437); *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 107.

[57] *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 118 f.

[58] Zu unterschiedlichen Performancemaßen (wie *accuracy*, *precision*, *recall*, *F1 score*) etwa *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 100 f., 410 ff.

[59] Grundlegend *Lawrence et al.*, 8 IEEE Transactions on Neural Networks 1997, 98; siehe auch *Y. Sun et al.*, Deepid3: Face recognition with very deep neural networks, Working Paper, 2015, https://arxiv.org/abs/1502.00873; *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 23 f.; *Ranjan et al.*, 35 IEEE Signal Processing Magazine 2018, 66.

Bilderkennung,[60] zur Spam-Klassifikation[61] und zur Prognose bestimmter Risiken oder Präferenzen.[62]

b) Verstärkungslernen (*reinforcement learning*)

Strukturell ist dem überwachten Lernen das Verstärkungslernen durchaus ähnlich,[63] die Lernsignale werden hier jedoch durch eine interaktive Lernumgebung generiert.[64] Dabei vollführt das Modell strategische Züge innerhalb dieser definierten Lernumgebung, wobei die einzelnen Züge jeweils durch ein Belohnungssignal (*reward signal*) mit Punktgewinnen oder -abzügen bewertet werden.[65] Ziel des Modells ist die langfristige Optimierung der Belohnung durch Maximierung einer Wertfunktion,[66] die einen langfristigen Zeithorizont abdeckt (*value function*).[67] Verstärkungslernen wird insbesondere bei Modellen angewandt, die in den vergangenen Jahren immer neue Formen strategischer Spiele, von Computerspielen[68] bis zu Go[69] und Poker,[70] mit supra-humaner Performanz gemeistert haben. *Reinforcement learning* kommt jedoch zunehmend auch bei der Modellierung von Nutzerpräferenzen im Onlinekontext und der Auswahl eines daran angepassten Werbe- oder Inhaltsangebots zum Einsatz.[71]

c) Unüberwachtes Lernen (*unsupervised learning*)

Unüberwachtes Lernen schließlich kommt ohne Vorgabe korrekter Ergebnisse und ohne ein vorab definiertes Belohnungssignal aus.[72] Vielmehr zerlegt der Algorithmus die zu analysierenden Daten in mathematische Einzelteile und unterteilt diese dann in unterschiedliche Gruppen, beispielsweise auf Grund-

[60] *Krizhevsky/Sutskever/Hinton*, Advances in Neural Information Processing Systems 2012, 1097; *Jordan/Mitchell*, 349 Science 2015, 255 (257); *Hu/Shen/G. Sun*, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2018, 7132.

[61] *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 3; *Jordan/Mitchell*, 349 Science 2015, 255 (257).

[62] *Baumann et al.*, Twenty-Third European Conference on Information Systems (ECIS) 2015, Article 15, 1; (2 ff.); *Witten et al.*, Data Mining, 4. Aufl. 2016, 27 f.

[63] *Littmann*, 521 Nature 2015, 445 (446).

[64] *Sutton/Barto*, Reinforcement Learning, 2. Aufl. 2018, 2.

[65] *Sutton/Barto*, Reinforcement Learning, 2. Aufl. 2018, 6; *Jordan/Mitchell*, 349 Science 2015, 255 (258).

[66] *Mnih et al.*, 518 Nature 2015, 529 (529); *Sutton/Barto*, Reinforcement Learning, 2. Aufl. 2018, 1.

[67] *Mnih et al.*, 518 Nature 2015, 529 (529); *Li*, Deep reinforcement learning: An overview, Working Paper, 2017, https://arxiv.org/abs/1701.07274, 9, 14 ff.; *Sutton/Barto*, Reinforcement Learning, 2. Aufl. 2018, 6.

[68] *Mnih et al.*, 518 Nature 2015, 529 (530 ff.).

[69] *Silver et al.*, 529 Nature 2016, 484.

[70] *Brown/Sandholm*, 359 Science 2018, 418; *Brown/Sandholm*, 365 Science 2019, 885.

[71] *Littmann*, 521 Nature 2015, 445 (446).

[72] *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 102; *Jordan/Mitchell*, 349 Science 2015, 255 (258).

lage der Ähnlichkeit der mathematischen Bestandteile.[73] So können etwa Textdokumente bestimmten *clustern* zugeordnet werden.[74] Eine Unterteilung nach Trainings- und Testdaten erfolgt jedoch nicht.[75]

2. *Maschinelles Lernen als Optimierungsproblem: Tiefe neuronale Netze*

Maschinelles Lernen kann insofern als mathematisches Optimierungsproblem aufgefasst werden, bei dem eine Funktion gesucht wird, welche den Eingabedaten ein nach Maßgabe der Performancemaße *P* möglichst korrektes Ergebnis zuordnet (*(un)supervised learning*) bzw. möglichst gute Handlungsstrategien entwickelt (*reinforcement learning*).[76] Je nach spezifischer Technik des maschinellen Lernens ist die Form dieser Funktion in gewissem Umfang vorgegeben oder auch nicht.[77] Die besondere Stärke unter anderem[78] der in der Öffentlichkeit viel diskutierten tiefen neuronalen Netze (*deep learning*), bei denen seit 2006 erhebliche Leistungsdurchbrüche erzielt wurden,[79] besteht nun darin, dass der Funktionstyp keinen apriorischen Einschränkungen unterliegt[80] und auch die relevanten *features* selbstständig gelernt werden.[81] Damit können sich diese Netze äußerst flexibel und mit im Vergleich zu anderen Techniken minimaler menschlicher Anleitung an unterschiedlichste Konstellationen von Eingabedaten anpassen. Auch beim *reinforcement learning* wird heute zumeist ein bereits trainiertes tiefes neuronales Netz als Agent verwendet, dessen Verhalten durch Verstärkung einzelner Strategien optimiert wird (*deep reinforcement learning*).[82] In vielen, wenngleich nicht allen,[83] Situationen liegt die Performanz von tiefen neuronalen Netzen daher über der von anderen Techniken

[73] *Russell/Norvig*, Artificial Intelligence, 3. Aufl. 2010, 817 ff.

[74] *Steinbach et al.*, KDD Workshop on Text Mining 2000, 525; *Shalev-Shwartz/Ben-David*, Understanding Machine Learning, 2014, 5; *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 102.

[75] *Shalev-Shwartz/Ben-David*, Understanding Machine Learning, 2014, 4.

[76] *Goodfellow/McDaniel/Papernot*, 61(7) Communications of the ACM 2018, 56 (56).

[77] Bei der linearen Regression ist der Funktionstyp etwa, wie der Name bereits sagt, auf lineare Funktionen festgelegt, siehe etwa *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 104 ff.; *LeCun/Bengio/Hinton*, 521 Nature 2015, 436 (437).

[78] Für weitere in der Funktionsform verhältnismäßig unbeschränkte Modelltypen, siehe *James et al.*, An Introduction to Statistical Learning, 2013, 265 ff.

[79] Grundlegend *Hinton/Osindero/The*, 18 Neural Computation 2006, 1527; Verallgemeinerung in *Bengio et al.*, Advances in Neural Information Processing Systems, 2006, 153.

[80] *Bengio et al.*, Advances in Neural Information Processing Systems, 2006, 153 (153 f.); *LeCun/Bengio/Hinton*, 521 Nature 2015, 436 (438); *Lin/Tegmark/Rolnick*, 168 Journal of Statistical Physics 2017, 1223 (1225); *Rolnick/Tegmark*, The power of deeper networks for expressing natural functions, Working Paper, 2017, https://arxiv.org/abs/1705.05502.

[81] *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 10; *LeCun/Bengio/Hinton*, 521 Nature 2015, 436 (438).

[82] *Silver et al.*, 529 Nature 2016, 484 (484 f.); *Mnih et al.*, 518 Nature 2015, 529 (529 f.); *Sutton/Barto*, Reinforcement Learning, 2. Aufl. 2018, 236, 475; *Li*, Deep reinforcement learning: An overview, Working Paper, 2017, https://arxiv.org/abs/1701.07274, 5.

[83] *Rudin*, 1 Nature Machine Intelligence, 2019, 206 (206 f.).

maschinellen Lernens.[84] Dass dies zugleich mit einer gegenüber anderen Techniken maschinellen Lernens verringerten Erklärbarkeit des Modells einhergeht, wurde in der informatischen[85] und datenschutzrechtlichen Literatur,[86] auch vom Verfasser,[87] bereits vielfach erörtert und muss hier nicht vertieft werden.

III. Technische Autonomie, Daten und Inferenzen

Entscheidend für die Zwecke dieser Arbeit sind vielmehr drei Aspekte maschinellen Lernens. Allen Techniken ist erstens gemein, dass sie (nach einem bestimmten, vorab definierten Lernalgorithmus) über viele Iterationen so trainiert werden, dass sie fortan auf Grundlage ihrer internen Parameter Ergebnisse adaptiv und grundsätzlich ohne intensive menschliche Eingriffe auch für solche Situationen mit hinreichender Performanz errechnen können, mit denen sie zuvor noch nicht konfrontiert wurden. Diese Fähigkeit zur Bewältigung neuer Entscheidungsszenarien (i) in weitgehender Unabhängigkeit von menschlichen Korrektureingriffen[88] und (ii) auf Grundlage adaptiver, eigenständiger Wissenserweiterung[89] wird in der technischen Literatur als Autonomie der informationstechnischen Systeme bezeichnet.[90] Während der Begriff der Auto-

[84] *LeCun/Bengio/Hinton*, 521 Nature 2015, 436 (438); *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 21 ff.; *Topol*, 25 Nature Medicine 2019, 44 (44 f.); siehe ferner die Nachweise in § 2, Fn. 59 f. und 68–70.

[85] Siehe nur *Rudin*, 1 Nature Machine Intelligence, 2019, 206; *Lipton*, 61(10) Communications of the ACM 2018, 36; *Ribeiro/Singh/Guestrin*, Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining 2016, 1135; *Burrell*, 3(1) Big Data & Society 2016, 1.

[86] Repräsentativ *Wachter/Mittelstadt/Floridi*, 7 International Data Privacy Law 2017, 76; *Wachter/Mittelstadt/Russell*, 31 Harvard Journal of Law and Technology 2017, 841; *Selbst/Barocas*, 87 Fordham Law Review 2018, 1085; *Wischmeyer*, AöR 143 (2018), 1 (42 ff.); *Information Commissioner's Office/Alan Turing Institute*, Explaining decisions made with AI, Draft Guidance, 2019.

[87] *Hacker/Krestel/Grundmann/Naumann*, 28 Artificial Intelligence and the Law 2020, DOI: https://doi.org/10.1007/s10506-020-09260-6.

[88] *Department of Defense*, Defense Science Board, The Role of Autonomy in DoD Systems, 2012, 1; *Bekey*, in: Lin et al. (Hrsg.), Robot Ethics, 2012, 17 (18); *Tessier*, in: Lawless et al. (Hrsg.), Autonomy and Artificial Intelligence, 2017, 179 (180); *Sartor*, in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, 263 (267 f.).

[89] *Russell/Norvig*, Artificial Intelligence, 3. Aufl. 2010, 39; *Department of Defense*, Defense Science Board, Summer Study on Autonomy, 2016, 4; *Alonso/Mondragón*, Agency, Learning and Animal-Based Reinforcement Learning, in: Nickles (Hrsg.), Agents and Computational Autonomy, 2005, 1 (2 f.); *Sartor*, in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, 263 (269).

[90] Überblick etwa bei *McFarland*, in: Steels/Brooks (Hrsg.), The Artificial Life Route to Artificial Intelligence, 2018, 187; Lawless et al. (Hrsg.), Autonomy and Artificial Intelligence, 2017; Nickles (Hrsg.), Agents and Computational Autonomy, 2005; *Zeigler*, Proceedings of AI, Simulation and Planning in High Autonomy Systems 1990, 2; kritisch hinsichtlich der Verwendung des Terminus „autonomy" in dieser Hinsicht *Bradshaw et al.*, 28

matisierung lediglich die determinierte Abfolge bestimmter Rechenschritte ohne konkreten menschlichen Eingriff designiert,[91] muss für technische Autonomie eine Adaptationsfähigkeit des Systems hinzukommen.[92] Diese wird typischerweise in unterschiedlichen Graden gemessen,[93] die jeweils angeben, wie stark die Abhängigkeit des Systems von menschlichen Korrektureingriffen bei der Bewältigung neuer Aufgaben ist. Stark autonome Systeme können, wie der letzte Teil der Arbeit zeigen wird,[94] Menschen in verschiedenen Situationen, so auch bei der Durchsetzung ihrer Datenschutzpräferenzen in vernetzten Umgebungen, erheblich entlasten.[95] Zugleich löst sich jedoch der Bezug der maschinellen Handlung zu einer spezifischen menschlichen Willensentscheidung mit steigendem Grad der Autonomie zunehmend auf, was die Zurechnung adaptiven maschinellen Verhaltens zu menschlichen Nutzern zivilrechtlich problematisch werden lässt.[96]

Zweitens kann die für adaptive Prognosen notwendige Übertragung der Leistungen aus dem Testdatensatz auf neue Konfigurationen nur gelingen, wenn das Modell mit einer hinreichenden Menge von Trainingsdaten kalibriert wurde.[97] Diese Angewiesenheit auf erhebliche Mengen an Trainingsdaten macht Tracking-Werkzeuge zur idealen Partnertechnologie von Techniken maschinellen Lernens. Erstere können genau jene Rohdaten bereitstellen, die zweitere benötigen, um daraus Prognosen ableiten zu können.[98] Insofern verstärken Techniken maschinellen Lernens die Nachfrage nach (qualitativ hochwertigen) nutzerbezogenen Daten signifikant.

Drittens sind durch die in den letzten Jahren gestiegenen Performancewerte der verschiedenen Modelle maschinellen Lernens immer weiter reichende Inferenzen hinsichtlich des Verhaltens und der Präferenzen menschlicher Ak-

IEEE Intelligent Systems 2013, 54 (58 f.); zum Begriff menschlicher Autonomie unten, § 6 A.

[91] *Department of Defense*, Defense Science Board, Summer Study on Autonomy, 2016, 4.

[92] Siehe die Nachweise in § 2, Fn. 89.

[93] Siehe aus dem Bereich des autonomen Fahrens *National Highway Traffic Safety Administration*, Preliminary Statement of Policy Concerning Automated Vehicles, 2013, 4 f. (mit 5 Stufen); SAE International, Standard J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, 2014 (mit 6 Stufen); kritisch gegenüber einer Einteilung auf einer eindimensionalen Skala jedoch *Bradshaw et al.*, 28 IEEE Intelligent Systems 2013, 54 (57 f.).

[94] Siehe dazu unten, § 6 C.I.3.

[95] Vgl. *Castelfranchi/Falcone*, in: Nickles (Hrsg.), Agents and Computational Autonomy, 2005, 40 (44); zur Notwendigkeit von *human-machine-teaming* jedoch, auch im Fall stark autonomer Agenten, *Department of Defense*, Defense Science Board, The Role of Autonomy in DoD Systems, 2012, 24; *Bradshaw et al.*, 28 IEEE Intelligent Systems 2013, 54 (58); *Topol*, 25 Nature Medicine 2019, 44 (52); *University of Maryland*, The Buddy System: Human-Computer Teams, IEEE Spectrum (16.4.2019), https://spectrum.ieee.org/robotics/robotics-hardware/the-buddy-system-human-computer-teams.

[96] Siehe dazu unten, § 6 C.I.3. sowie *Hacker*, RW 9 (2018), 243.

[97] *C. Sun et al.*, Proceedings of the IEEE International Conference on Computer Vision 2017, 843 (844); *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 18 ff.

[98] *Jordan/Mitchell*, 349 Science 2015, 255 (256 f.).

teure möglich (*consumer preference modeling*).[99] Zwar sind auch Modelle maschinellen Lernens vor Fehlern keineswegs gefeit.[100] Insgesamt lässt sich jedoch menschliches Verhalten damit in vielen Bereichen besser modellieren als mit herkömmlichen Werkzeugen. Dies kann auf der einen Seite genutzt werden für die automatisierte Anpassung von Produkten an inferierte Präferenzen des Nutzers, wie der Überblick über das Internet der Dinge sogleich zeigen wird. Auf der anderen Seite zeitigen präzise maschinelle Prognosen jedoch auch manifeste Probleme im Bereich des Datenschutzes und, sofern dadurch Handlungen der Nutzer unterschwellig gelenkt werden, auch der Autonomie.[101] Insbesondere die datenschutzrechtlichen Konfliktlagen werden im weiteren Verlauf der Arbeit noch mehrfach thematisch werden.[102]

C. Das Internet der Dinge

Neben Verfahren der künstlichen Intelligenz stellt das Internet der Dinge (*Internet of Things*, IoT) eine weitere zentrale technologische Entwicklung dar, welche den Austausch, die Analyse, aber auch die Erhebung von personenbezogenen Daten aller Voraussicht nach spezifisch verändern wird[103] und dies

[99] *Kokol/Verlic/Krizmaric*, 3 WSEAS Transactions on Information Science and Applications 2006, 2054; *Christidis/Apostolou/Mentzas*, European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases 2010, 12; *Netzer et al.*, 31 Marketing Science 2012, 521; *Baumann et al.*, Twenty-Third European Conference on Information Systems (ECIS) 2015, Article 15, 1; (2 ff.); *Wedel/Kannan*, 80 Journal of Marketing 2016, 97 (101 ff.); *Baumann et al.*, 61 Business & Information Systems Engineering 2019, 413 (426 ff.); *Gabel/Guhl/Klapper*, 56 Journal of Marketing Research 2019, 557 (566 ff.); *Guo et al.*, An interpretable machine learning framework for modelling human decision behavior, Working Paper, 2019, https://arxiv.org/abs/1906.01233; vgl. auch *Littmann*, 521 Nature 2015, 445 (446); *Witten et al.*, Data Mining, 4. Aufl. 2016, 27 f.; *Polania/Woodford/Ruff*, 22 Nature Neuroscience 2019, 134; *Roberts/Hutcherson*, 23 Trends in Cognitive Sciences 2019, 602 (602 f.); *Rosoff*, IBM and Salesforce Shake Hands on Artificial Intelligence, CNBC (6.3.2017), https://www.cnbc.com/2017/03/06/ibm-and-salesforce-shake-hands-on-artificial-intelligence.html; *Forbes Technology Council*, Looking Ahead: The Industries that Will Change the most as Machine Learning Grows, Forbes (8.3.2017), https://www.forbes.com/sites/forbestechcouncil/2017/03/08/looking-ahead-the-industries-that-will-change-the-most-as-machine-learning-grows/; McKinsey Global Institute, The Age of Analytics, Report, London u. a. 2016, 83–86 (basierend auf Interviews mit 50 Entscheidungsträgern aus der Wirtschaft); hinsichtlich der Qualität der algorithmischen Prognose von Konsumpräferenzen durch real verwendete Modelle liegen jedoch nur wenige belastbare empirischen Studien vor, da diese Modelle von den Entwicklern typischerweise nicht für Forschungszwecke offengelegt werden, siehe nochmals *Baumann et al.*, 61 Business & Information Systems Engineering 2019, 413 (427); siehe aber unten, § 3, Fn. 53.

[100] *Dressel/Farid*, 4 Science Advances 2018, Article eaao5580, 1 (1 f.).; *Topol*, 25 Nature Medicine 2019, 44 (51 f.).

[101] Siehe unten, § 6 A.

[102] Siehe unten, § 4.

[103] Statt vieler *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, 2014, 580 f.

zum Teil auch bereits tut.[104] Datenaustausch zwischen Alltagsgegenständen wird damit ubiquitär, die Erfassung von Lebensgewohnheiten zur notwendigen Funktionsvoraussetzung vernetzter Geräte. Das *Internet of Things* vereint dabei Elemente der Datenerhebung (mittels Sensoren) mit jenen der Datenanalyse (teilweise mithilfe maschinellen Lernens) und schließlich der Umsetzung in der Realität (mithilfe von Aktuatoren).[105]

Auf einer technischen Ebene beschreibt das Internet der Dinge zunächst jedoch lediglich eine besondere Form der techno-physischen Vernetzung, die vor allem durch Sensordaten getrieben ist. Unter einem Netzwerk versteht man in der Informatik die Verbindung von zwei autonomen Rechnern, die Informationen austauschen können.[106] Das Paradigma stellt das Internet selbst dar, das ein übergreifendes Netzwerk von lokalen Netzwerken bildet.[107] Das Internet der Dinge verbindet nun reale Objekte mit dem Internet oder anderen Netzwerken und macht so einen Datenaustausch zwischen den Geräten oder hin zu einer zentralen Kontrollinstanz möglich.[108] Werden über reale Objekte auch Menschen und Prozesse verstärkt in die Vernetzung einbezogen (z. B. über *wearables*), so spricht man auch, über das *Internet of Things* hinausgehend, vom *Internet of Everything*.[109]

Stammt der Begriff des *Internet of Things* auch aus dem Jahr 1999,[110] so steht seine Realisierung nach wie vor doch vor erheblichen technischen, aber auch rechtlichen Herausforderungen. Datenschutz und IT-Sicherheit werden durch das Internet der Dinge in besonderer Weise auf die Probe gestellt.[111] Diese Ansicht teilt auch die Europäische Kommission.[112] Während Fragen der IT-Si-

[104] Repräsentativ *DeNardis*, The Internet in Everything, 2020, 59 ff.

[105] Siehe etwa *Zech*, Risiken digitaler Systeme, Weizenbaum Series #2, 2020, 48–50.

[106] *Tanenbaum/Wetherall*, Computer Networks, 2014, 2: „We will use the term ‚computer network' to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information." In der Mathematik wird der Netzwerkbegriff verallgemeinert auf die Möglichkeit der Wechselwirkung zwischen Elementen einer Menge, die durch (gerichtete) Graphen verbunden sind, siehe etwa *Nitzsche*, Graphen für Einsteiger, 2009, 154; *Brand*, Ökonomische Fragestellungen mit vielen Einflussgrößen als Netzwerke, 2006, 9.

[107] *Tanenbaum/Wetherall*, Computer Networks, 2014, 2.

[108] *Tanenbaum/Wetherall*, Computer Networks, 2014, 332; *Gershenfeld/Krikorian/Cohen*, 291 Scientific American 2004, 76.

[109] *Di Martino et al.*, in: Di Martino et al. (Hrsg.), Internet of Everything, 2018, 1 (2); *Velasquez et al.*, 9 Journal of Internet Services and Applications 2018, 14; siehe dazu genauer unten, § 2 D.

[110] Der Begriff wurde wohl von Kevin Ashton vom MIT Auto-ID Center im Jahr 1999 in einer Präsentation zum ersten Mal gebraucht, siehe *Ashton*, That ‚Internet of Things' Thing, RFID Journal (22.6.2009), https://www.rfidjournal.com/articles/view?4986.

[111] *Ziegler et al.*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 9; früh bereits *Weber*, 26 Computer Law & Security Review 2010, 23; *Peppet*, 93 Texas Law Review 2014, 85 (129 ff.).

[112] *European Commission*, Advancing the Internet of Things in Europe, Commission Staff Working Document, COM(2016) 180 final, 27–31.

cherheit hier nicht behandelt werden können,[113] ist der zweite Teil dieser Arbeit unter anderem den datenschutzrechtlichen Fragen der Vernetzung gewidmet. Zunächst aber sollen noch weitere technische Grundlagen gelegt werden, um die rechtliche Beurteilung auf ein sicheres Fundament zu stellen.

I. Vier Charakteristika von IoT-Geräten

Vier Aspekte sind charakteristisch für IoT-Geräte: Sensorfähigkeit; Konnektivität; Aktuation; und Automatisierung.[114] Grundlage des Internets der Dinge ist die Fähigkeit von IoT-Produkten, Umweltdaten mithilfe von Sensoren zu messen (Sensorfähigkeit). Dabei kann es sich z. B. um Geodaten, Interaktionsdaten oder andere physikalische Zustandsgrößen handeln. Sensoren sind spezifische Energiewandler (*transducer*), da sie eine Energieform in eine andere umwandeln: Sie konvertieren physikalische Phänomene in elektrische Impulse, sodass diese messbar werden.[115] Mikrophone beispielsweise wandeln Schallwellen in elektrische Impulse um. Diese Daten verbleiben jedoch typischerweise nicht in dem Gerät selbst, sondern werden mittels des Internets oder einer anderen Kommunikationstechnologie[116] zu einer geeigneten Verarbeitungseinheit übertragen (Konnektivität),[117] wo sie analysiert und mit anderen Messdaten zusammengeführt werden (können).[118] Dieser aus der Konnektivität erwachsende Netzwerkcharakter bildet die Grundlage für die Skalierbarkeit des IoT-Systems: Es können jederzeit weitere Geräte hinzugefügt werden, die von den Daten der anderen Geräte profitieren und selbst Daten einspeisen,

[113] Siehe dazu etwa *Ziegler*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 1; *Ziegler et al.*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 9 (19–31); *Ning*, Unit and Ubiquitous Internet of Things, 2013, 140 ff.

[114] *Madaan/Nurse/de Roure/O'Hara/Hall/Creese*, A Storm in an IoT Cup: The Emergence of Cyber-Physical Social Machines, Working Paper, 2018, https://ssrn.com/abstract=3250383, 6; siehe auch *Aher*, A Look at IoT Architecture, DZone (18.8.2018), https://dzone.com/articles/iot-architecture-2; ferner *Ning*, Unit and Ubiquitous Internet of Things, 2013, 5 f., der allerdings Aktuation und Sensorfähigkeit zu einem Charakteristikum verbindet.

[115] *Little*, IoT Systems: Sensors and Actuators, DZone (30.6.2017), https://dzone.com/articles/iot-systems-sensors-and-actuators; *Ning*, Unit and Ubiquitous Internet of Things, 2013, 37.

[116] Ursprünglich sollte RFID Technologie dafür Verwendung finden, siehe z. B. *Welbourne et al.*, Building the internet of things using RFID: the RFID ecosystem experience, 13(3) IEEE Internet Computing 2009, 48; RFID hat sich jedoch nicht durchgesetzt, weshalb heute zumeist andere drahtlose Techniken (Bluetooth, WLAN etc.) Verwendung finden, siehe *Madakam/Ramaswamy/Tripathi*, 3 Journal of Computer and Communications 2015, 164 (169–171).

[117] *Shi/Cao/Zhang/Li/Xu*, 3 IEEE Internet of Things Journal 2016, 637 (640); *Ning*, Unit and Ubiquitous Internet of Things, 2013, 6; *Ziegler*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 1 (1).

[118] Diese Zusammenführung der Messdaten verschiedener IoT-Geräte wird auch *ubiquitous Internet of Things* genannt, im Unterschied zum *unit Internet of Things*, siehe *Ning*, Unit and Ubiquitous Internet of Things, 2013, 15.

sodass ein positiver direkter Netzwerkeffekt entsteht.[119] Häufig finden Aggregation und Analyse der Daten auf einer Cloud[120] oder in einem abgelegenen Datencenter statt.[121] Aufgrund der Übertragungsverzögerung und der limitierten Bandbreite der Übertragungswege, sowie aus Sicherheits- und Datenschutzgründen,[122] wird jedoch zunehmend auch versucht, bereits innerhalb des Heimnetzwerks, in das die IoT-Geräte eingebettet sind, oder in deren unmittelbarer Nähe eine Analyse vorzunehmen (*edge computing*[123]), z. B. in einer Recheneinheit innerhalb eines Smart Home.[124] Sind die Daten einmal analysiert, kann je nach Inhalt der Daten und Programmierung des Geräts eine Reaktion des Geräts erfolgen, die sich auf die physische Außenwelt auswirkt (Aktuation). Dafür wandelt ein Aktuator elektrische Impulse in Bewegungen oder die Veränderung anderer physikalischer Zustandsgrößen um.[125] Das Wirkprinzip der Aktuatoren ist daher dem der Sensoren gerade entgegengesetzt. Die Ana-

[119] Zu direkten Netzwerkeffekten, bei denen der Nutzen jedes Teilnehmers des Netzwerks mit jedem weiteren Teilnehmer steigt, siehe aus der umfangreichen Literatur *Katz/Shapiro*, 75 American Economic Review 1985, 424; *Belleflamme/Peitz*, Industrial Organization, 2010, 549; *Shy*, 38 Review of Industrial Organization 2011, 119 (120); *Engert*, AcP 213 (2013), 321 (325); *Haucap/Heimeshoff*, 11 International Economics and Economic Policy 2014, 49 (51); *Monopolkommission*, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015, Rn. 300.

[120] Eine Cloud bezeichnet ein Netzwerk, das technische Infrastruktur, Speicherplatz und/oder Softwarekapazitäten als Service (*as a service*) durch Verwendung eines oder mehrerer Fernserver über eine Internetverbindung anbietet, siehe die Definition des National Institute of Standards and Technology in *Mell/Grance*, The NIST Definition of Cloud Computing, Special Publication (NIST SP) – 800–145, 2011, 2: „Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e. g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."; siehe auch *Bolognini/Balboni*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 71 (72); *Ning*, Unit and Ubiquitous Internet of Things, 2013, 4; *V*, Demystifying Edge vs. Cloud Computing, DZone (15.3.2019), https://dzone.com/articles/demystifying-the-edge-vs-cloud-computing.

[121] *Abdelwahab et al.*, 1 IEEE Internet of Things Journal 2014, 276 (276); *Aher*, A Look at IoT Architecture, DZone (18.8.2018), https://dzone.com/articles/iot-architecture-2.

[122] *Satyanarayanan*, 50 Computer 2017, 30 (32); *V*, Demystifying Edge vs. Cloud Computing, DZone (15.3.2019), https://dzone.com/articles/demystifying-the-edge-vs-cloud-computing.

[123] *Shi/Cao/Zhang/Li/Xu*, 3 IEEE Internet of Things Journal 2016, 637 (638): „Edge computing refers to the enabling technologies allowing computation to be performed at the edge of the network, on downstream data on behalf of cloud services and upstream data on behalf of IoT services. Here we define ‚edge' as any computing and network resources along the path between data sources and cloud data centers."; siehe auch *Satyanarayanan*, 50 Computer 2017, 30 (30); *Velasquez et al.*, 9 Journal of Internet Services and Applications 2018, 14; *Alexandrova*, The Impact of Edge Computing on IoT: The Main Benefits and Real-Life Use Cases, DZone (6.2.2019), https://dzone.com/articles/the-impact-of-edge-computing-on-iot-the-main-benef.

[124] *Shi/Cao/Zhang/Li/Xu*, 3 IEEE Internet of Things Journal 2016, 637 (637 f.).

[125] *Little*, IoT Systems: Sensors and Actuators, DZone (30.6.2017), https://dzone.com/articles/iot-systems-sensors-and-actuators; *Ning*, Unit and Ubiquitous Internet of Things, 2013, 38.

lyse der gesammelten Daten und die Reaktion darauf können in unterschiedlichem Maße automatisiert werden,[126] bis hin zu einem Einsatz von Formen maschinellen Lernens,[127] die dem IoT-Gerät einen gewissen Grad von Autonomie verleihen (Automatisierung).[128]

II. Vier Schichten des IoT

Technisch gesehen ruht das Internet der Dinge auf (mindestens[129]) vier unterschiedlichen Schichten und korrespondierenden Protokollen der Verarbeitung von Information, die den vier Charakteristika von IoT-Geräten weitestgehend entsprechen.[130] Die unterste Ebene wird durch die Wahrnehmungsschicht (*perception layer*) aufgespannt, die im Wesentlichen durch die Sensoren, aber auch die Aktuatoren konstituiert wird.[131] Darüber liegt die Netzwerkschicht (*network layer*), durch die IoT-Geräte mit Netzwerkgeräten verbunden werden, welche die Daten weiterleiten. Die Verarbeitungsschicht (*processing layer*) speichert und analysiert die dergestalt übermittelten Daten.[132] Dies kann, wie erwähnt, sowohl am *edge* des Heimnetzwerks als auch in einem Datencenter oder auf der Cloud geschehen. Zumeist werden die Daten am *edge* zumindest grob voranalysiert und selektiert, um bei der weiteren Übermittlung keine unnötigen Engpässe zu kreieren und die Rechen- und Verarbeitungskapazität der Cloud nicht zu überfordern. Big Data-Technologien und Methoden maschinellen Lernens werden hingegen bislang noch vorzugsweise auf der, mit größerer Rechenkapazität gesegneten, Cloud angewandt. Die vierte und letzte Schicht,

[126] *Ning*, Unit and Ubiquitous Internet of Things, 2013, 6.

[127] *Ning*, Unit and Ubiquitous Internet of Things, 2013, 52 f.

[128] *Hacker*, 7 International Data Privacy Law 2017, 266 (267).

[129] Weitere Schichten, etwa für Monitoring, Service Management, Data Abstraction, Speicherung und IT-Sicherheit, können hinzutreten, siehe *Aher*, A Look at IoT Architecture, DZone (18.8.2018), https://dzone.com/articles/iot-architecture-2; *Shi/Cao/Zhang/Li/Xu*, 3 IEEE Internet of Things Journal 2016, 637 (640, 642 f.); *Ning*, Unit and Ubiquitous Internet of Things, 2013, 18. Insgesamt wurden eine Reihe von Schichtenmodellen vorgeschlagen (insbesondere das 3-, 4- und 8-Schichtenmodell), deren technische Unterschiede hier jedoch nicht weiterführen; siehe dazu *Ning*, Unit and Ubiquitous Internet of Things, 2013, 17–20.

[130] *Aher*, A Look at IoT Architecture, DZone (18.8.2018), https://dzone.com/articles/iot-architecture-2; vgl. auch *European Commission*, Advancing the Internet of Things in Europe, Commission Staff Working Document, COM(2016) 180 final, 13; siehe allerdings auch § 2, Fn. 131.

[131] *Ning*, Unit and Ubiquitous Internet of Things, 2013, 17.

[132] Im 3-Schichtenmodell wird die Verarbeitungsschicht nicht eigens spezifiziert, sondern in die Netzwerkschicht integriert, *Ning*, Unit and Ubiquitous Internet of Things, 2013, 17; *Pagallo/Durante/Monteleone*, in: Leenes et al. (Hrsg.), Data Protection and Privacy: (In)visibilities and Infrastructures, 2017, 59 (65). Für die datenschutzrechtliche Diskussion ist sie jedoch von erheblicher Wichtigkeit, so dass sie hier, entsprechend *Aher*, A Look at IoT Architecture, DZone (18.8.2018), https://dzone.com/articles/iot-architecture-2, aufgenommen wurde.

die Anwendungsschicht (*application layer*) wendet den Informationsfluss wieder zurück zum Nutzer, indem für diesen anwendungsspezifische Dienstleistungen zur Verfügung gestellt werden und die Interaktion mit dem Nutzer über ein Interface ermöglicht wird.[133]

Zwar ist das Internet der Dinge bislang nicht vollständig implementiert[134] und der Grad der Durchsetzung von Gebrauchsgegenständen mit internetfähiger Kommunikationstechnologie lässt sich nur schwer prognostizieren. Der Markt für IoT-Geräte verzeichnet jedoch seit 2014 Wachstumsraten von zwischen knapp 20 und 40 %, mit steigender Tendenz.[135] Bereits jetzt ist jedoch absehbar, dass es zumindest in einzelnen Bereichen zu einem erheblich verstärkten Datenaustausch infolge der fortschreitenden Vernetzung von Gegenständen, aber auch ganzen Architekturen und Umgebungen kommen wird.[136] Einige dieser Geräte sind bereits jetzt Realität. Fahrzeuge werden zunehmend vernetzt, was nicht zuletzt mit der fortschreitenden Autonomisierung der Transportmittel Hand in Hand geht.[137] *Wearables* vernetzen Menschen und liefern Datenströme zur Selbstvermessung.[138] Energieunternehmen messen den Energieverbrauch und adaptieren die Netzauslastung durch IoT-Technologie im Rahmen von Smart Grids.[139] Vernetzte Lautsprecher wie Amazons Echo werden mittels Spracherkennung und -Assistenz zu Dienstleistungsplattformen im eigenen Wohnzimmer[140] und Smart Homes mit Sensordaten ausgestattet, sodass die Eigentümer Licht, Temperatur, Durchlüftung, Strom- und Wasserverbrauch sowie andere relevante Parameter integriert messen und steuern (lassen) können.[141] Auf die Spitze getrieben wird das Vernetzungskon-

---

[133] *Ning*, Unit and Ubiquitous Internet of Things, 2013, 17. Diese Schicht stellt kein Charakteristikum des IoT dar und findet daher keine Entsprechung in den oben genannten vier Charakteristika.

[134] *Pagallo/Durante/Monteleone*, in: Leenes et al. (Hrsg.), Data Protection and Privacy: (In)visibilities and Infrastructures, 2017, 59 (61).

[135] *Columbus*, 2018 Roundup of Internet of Things Forecasts and Market Estimates, Forbes (13.12.2018), https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/; siehe auch *Hoofnagle/Kesari/Perzanowski*, 87 George Washington Law Review 2019, 783 (788 ff.).

[136] *Pagallo/Durante/Monteleone*, in: Leenes et al. (Hrsg.), Data Protection and Privacy: (In)visibilities and Infrastructures, 2017, 59 (60).

[137] *Becker*, Die 100-Milliarden-Euro-Frage. Digitale Angebote im Auto, SZ vom 13.3.2019, https://www.sueddeutsche.de/auto/auto-vernetzung-digital-1.4358303; *Hacker*, 7 International Data Privacy Law 2017, 266.

[138] *Di Martino et al.*, in: Di Martino et al. (Hrsg.), Internet of Everything, 2018, 1 (3 f.). Allerdings fehlt den Wearables häufig eine genuine Aktuationskomponente, die über eine Speicherung und Anzeige von Daten hinausginge.

[139] *Kumar*, Cloud and Edge Computing for an IoT-Based Smart Grid, DZone (19.3.2017), https://dzone.com/articles/cloud-computing-and-edge-computing-for-an-iot-base.

Aher, A Look at IoT Architecture, DZone (18.8.2018), https://dzone.com/articles/iot-architecture-2.

[140] https://www.amazon.de/Amazon-Echo-Intelligenter-Lautsprecher-Alexa/dp/B06ZXQV6P8.

[141] *Shi/Cao/Zhang/Li/Xu*, 3 IEEE Internet of Things Journal 2016, 637 (639 f.); *Schaper/Teubert*, ZfV 2016, 613 (613).

zept in Smart Cities,[142] in denen auch die Außenumgebung durch eine Reihe von Sensoren und anderen Messgeräten durchsetzt ist, sodass eine möglichst weitreichende Vermessung und Steuerung der urbanen Lebenswirklichkeit erzielt werden kann. Dies erfasst die Steuerung des Verkehrs, des Wassersystems, aber auch potenziell den Zutritt zu Gebäuden und die Kriminalitätsbekämpfung. In der EU wird dieses Konzept in einer groß angelegten Machbarkeitsstudie (SynchroniCity), die durch das Horizon 2020 Programm gefördert wird, erprobt.[143] Auch die Stadt Toronto experimentiert in einer Partnerschaft mit einer Alphabet-Tochter mit Möglichkeiten der Realisierung einer datengetriebenen Stadtumgebung.[144] In China schließlich nimmt die ubiquitäre Erfassung von Handlungen im öffentlichen Raum, gepaart mit dem Sozialkreditsystem, eine kategorial neue Dimension an.[145]

Bereits unabhängig von diesen potenziellen Auswirkungen werden auf allen vier Schichten des Internets der Dinge Datenverarbeitungsprozesse angestoßen, die sowohl im Datenschutzrecht als auch im allgemeinen Zivilrecht Fragen nach (Selbst-)Verantwortung, Kontrollpotenzialen und der Zukunft der Privatsphäre aufwerfen. Nimmt man die weitreichenden Analyse- und Steuerungsmöglichkeiten eines ausgereiften Internets der Dinge mit in den Blick, so erlangen diese Fragen eine unausweichliche Dringlichkeit. Ihnen wird im zweiten und dritten Teil der Arbeit nachgegangen.

D. Konvergenzprozesse: Auf dem Weg zum *Internet of Everything*

Wie bereits mehrfach erwähnt, werden die drei verschiedenen, soeben vorgestellten Technologieformen zunehmend miteinander kombiniert. Nicht nur dienen Daten aus Tracking-Technologien und dem Internet der Dinge als Eingangs- oder Trainingsdaten für Modelle maschinellen Lernens;[146] auch auf der Ebene der Geräte und Applikationen selbst wird zunehmend das Internet der Dinge mit Techniken maschinellen Lernens verschränkt.[147] Komponenten maschinellen Lernens werden in IoT-Geräte implantiert, um diesen über die

---

[142] Dazu etwa *Madaan/Ahad/Sastry*, 34 Computer Law & Security Review 2018, 125 (128 ff.); *Cobbe/Morison*, in: Slautsky (Hrsg.), The Conclusions of the Chaire Mutations de l'Action Publique et du Droit Public, 2019.

[143] Dazu *Ziegler/Menon/Annichino*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 149 (150 f.).

[144] *Goodman/Powles*, Urbanism under Google: Lessons from Sidewalk Toronto, Fordham Law Review (im Erscheinen), https://www.ssrn.com/abstract=3390610.

[145] Siehe etwa *Liang et al.*, 10 Policy & Internet 2018, 415; *Genzsch*, in: Loitsch (Hrsg.), China im Blickpunkt des 21. Jahrhunderts, 2019, 129.

[146] Siehe oben, Text bei § 2, Fn. 98 f.

[147] Fraunhofer-Allianz Big Data, Zukunftsmarkt Künstliche Intelligenz. Potenziale und Anwendungen, 2017, 28 ff.

Vernetzungsdimension hinaus eine gewisse technische Autonomie (inklusive Lernfähigkeit) zu verleihen,[148] die nicht nur in Privathaushalten, sondern auch in Industrie und Dienstleistungssektoren erhebliche Fortschritte verspricht.[149] Elemente künstlicher Intelligenz übernehmen dabei sowohl Analyse- als auch Steuerungsfunktionen.[150] Paradigmatisches Beispiel sind vernetzte Transportmittel wie etwa autonome Fahrzeuge,[151] bei denen Verfahren aus dem Bereich *deep learning* die Bilderkennung liefern[152] und über Vernetzung zugleich die Interaktion mit anderen Fahrzeugen ermöglicht wird (*autonomous connected vehicles*).[153] Bei persönlichen Assistenten wie Siri, Alexa oder Cortana sowie Smart Home-IoT-Geräten wie Echo stellt maschinelles Lernen aus dem Bereich des *natural language processing*[154] die Spracherkennung bereit.[155] Auch die Schnittstellen zwischen Mensch und Maschine, zum Beispiel für das in Zukunft immer bedeutendere *human-machine-teaming*,[156] werden häufig durch Applikationen maschinellen Lernens bereitgestellt.[157]

Das *Internet of Everything*[158] bildet dabei den Zielpunkt einer Verschränkung aller drei genannten Basistechnologien in einer auf ununterbrochenen Datenfluss, ineinandergreifende Abläufe und personalisierte Prozesse ausgelegten Umgebung der Zukunft.[159] Auch wenn die Implementierung noch im Anfangsstadium steckt,[160] so zeichnet sich eine zunehmend vernetzte Lebensumgebung mit einer nahtlosen Integration von Messung, maschineller Analyse und autonomer Aktuation, „from recording a child's first steps to maintai-

[148] *Breiner/Sriram/Subrahmanian*, AAAI Spring Symposium Series 2018, 107 (108).

[149] *Wang et al.*, Industrial Big Data Analytics: Challenges, Methodologies, and Applications, Working Paper, 2018, https://arxiv.org/abs/1807.01016, 8; Fraunhofer-Allianz Big Data, Zukunftsmarkt Künstliche Intelligenz. Potenziale und Anwendungen, 2017, 28 f., 32.

[150] *Denga*, in: Bräutigam/Kraul (Hrsg.), Internet of Things. Rechtshandbuch, 2020, Teil A.I.3.; *Schatsky/Kumar/Bumb*, Intelligent IoT. Bringing the power of AI to the Internet of Things, Deloitte Insights, 2017, 2 f.

[151] Siehe dazu *Hacker*, 7 International Data Privacy Law 2017, 266 (267); Fraunhofer-Allianz Big Data, Zukunftsmarkt Künstliche Intelligenz. Potenziale und Anwendungen, 2017, 29; *Becker*, Die 100-Milliarden-Euro-Frage, SZ (13.3.2019), https://www.sueddeutsche.de/auto/auto-vernetzung-digital-1.4358303.

[152] *Zhang et al.*, Dive into Deep Learning, Open Source Manuskript, Release 0.7.1., 2019, https://d2l.ai/, 40.

[153] *Abeck et al.*, INFORMATIK 2019, 125 (125 ff.); *Crane/Logue/Pilz*, 23 Michigan Telecommunications and Technology Law Review, 2016, 191 (199 f.).

[154] Siehe dazu etwa *Manning et al.*, Proceedings of 52nd Annual Meeting of the Association for Computational Linguistics: System Demonstrations 2014, 55 sowie unten, § 6, Fn. 126.

[155] *Xiong*, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2018, 5934; *Zhang et al.*, Dive into Deep Learning, Open Source Manuskript, Release 0.7.1., 2019, https://d2l.ai/, 40.

[156] Siehe oben, § 2, Fn. 95.

[157] Fraunhofer-Allianz Big Data, Zukunftsmarkt Künstliche Intelligenz. Potenziale und Anwendungen, 2017, 28.

[158] Siehe oben, § 2, Fn. 109.

[159] *Breiner/Sriram/Subrahmanian*, AAAI Spring Symposium Series 2018, 107 (107 f.).

[160] *Breiner/Sriram/Subrahmanian*, AAAI Spring Symposium Series 2018, 107 (107 f.).

ning an elderly heartbeat",[161] bereits jetzt klar am Horizont ab.[162] Durch diese Konvergenzprozesse werden jedoch nicht nur das Potenzial, sondern auch die spezifischen Risiken der einzelnen Technologien (super-)additiv verknüpft.[163] Diesen spezifischen Möglichkeiten und Risiken, die jeweils eigene regulatorische Herausforderungen mit sich bringen, ist das folgende Kapitel gewidmet.

[161] *Breiner/Sriram/Subrahmanian*, AAAI Spring Symposium Series 2018, 107 (107).

[162] *Shojafar/Sookhak*, International Journal of Computers and Applications 2019, DOI: 10.1080/1206212X.2019.1575621, 1 (1); *Miraz et al.*, 10 Future Internet 2018, Article 68, 1 (5); *Botta et al.*, 56 Future Generation Computer Systems 2016, 684 (688); *Miraz et al.*, IEEE Internet Technologies and Applications (ITA) 2015, 219 (220 f.); *Sriram*, 17(3) IT Professional 2015, 60; *Abdelwahab et al.*, 1 IEEE Internet of Things Journal 2014, 276 (276); *Jara/Ladid/Gómez-Skarmeta*, 4 Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 2013, 97 (98); *Evans*, The Internet of Everything, Cisco Internet Business Solutions Group (IBSG), Report, 2012, 3 ff.

[163] Dazu etwa *Hacker*, 7 International Data Privacy Law 2017, 266 (268 ff.).

§ 3 Technisch-ökonomische Problemstellungen und rechtliche Herausforderungen

Bei technischer und ökonomischer Analyse der zunehmend vernetzten Datenverarbeitung im Internet der Dinge und im Bereich des maschinellen Lernens stellen sich drei zentrale rechtliche Herausforderungen, die in den folgenden Abschnitten entfaltet werden. Zunächst bedingt die vernetzte Datenerhebung und -weiterleitung eine technisch und ökonomisch gespeiste Multirelationalität von Daten, die ihnen einen Drittbezug einbeschreibt, der die Komplexität der rechtlichen Analyse erhöht (A.). Ein zweites regulatorisches Problem ergibt sich aus der Ambivalenz der Verarbeitung personenbezogener Daten, die einerseits erhebliches individuelles und soziales Potenzial offenbart, aber auch mit signifikanten Risiken einhergeht (B.). Drittens muss eine rechtliche Bewältigung datenschutzrechtlicher Risiken die Heterogenität von Datenschutzpräferenzen im Blick behalten, wenn sie (zumindest auch) privatautonome Gestaltung ermöglichen will (C.). Diese Herausforderungen sind jedoch notwendig stark abstrakt. Daher werden drei Leitfälle entwickelt, welche die regulatorischen Probleme konkret zuspitzen und Leitfragen für die weiteren Teile dieser Arbeit suggerieren (D.).

A. Erste rechtliche Herausforderung: Multirelationalität vernetzter Datenanalyse

Die großflächige Erhebung und Weiterleitung von Daten im Rahmen von privatrechtlichen Austauschverhältnissen birgt zwei Dimensionen einer fortschreitenden Vernetzung: eine techno-physische durch das Internet der Dinge (I.) und eine ökonomische durch die Verknüpfung des Angebots der Leistung mit der Datenüberlassung als Gegenleistung (II.). Daraus ergibt sich eine erste regulatorische Herausforderung, die in einer den Daten und ihrer Analyse typischerweise inhärenten Multirelationalität besteht (III.).

I. Techno-physische Vernetzung: Internet der Dinge

Anders als andere Technologien ist das Internet der Dinge funktional auf eine Erfassung von Lebensgewohnheiten der Gerätenutzer angelegt: Dies ist Struk-

turmerkmal der IoT-Technologie.[1] Über die eigentliche Vernetzung hinaus ist es Signum des IoT-Geräts, auf Messwerte in spezifischer Weise reagieren und damit die Umwelt, und die Interaktion mit den darin befindlichen Menschen, beeinflussen oder steuern zu können.[2] Ein in gewissem Umfang vernetztes Auto oder ein selbst Lebensmittel ordernder Kühlschrank bieten nur dann überhaupt einen signifikanten Vorteil gegenüber nicht vernetzten Geräten, wenn sie sich auf die Präferenzen der Nutzer einstellen oder zumindest auch über Fernkommunikation Anweisungen von diesen empfangen können.[3] Autonome Steuerung und die Erfassung von Präferenzen oder zumindest Gewohnheiten machen, wie in § 2 diskutiert, eine Verbindung mit Techniken des maschinellen Lernens notwendig. Ihren besonderen Wettbewerbsvorteil erlangen IoT-Produkte jedoch gerade durch die Zusammenführung von unterschiedlichen Datenquellen in einem Gerät oder an einer zentralen Verarbeitungsinstanz. Einen erheblichen Beitrag zur gehobenen Datenqualität, welche IoT-Geräte liefern, leisten dabei die hier besonders gut bestimmbaren Geodaten. Da IoT-Geräte typischerweise mit dem Internet oder anderen, drahtlosen Netzwerken verbunden sind, lässt sich (vereinfacht) über die Netzwerkkennung der Standort des Geräts, und damit auch des Verwenders, häufig sehr genau ermitteln, ohne dass auf ressourcenaufwändige GPS-Daten zurückgegriffen werden müsste.[4]

Dies hat zweierlei zur Folge: Erstens wird die physische Realität dadurch in einer bisher unbekannten Reichweite durch Sensordaten erfasst; dies impliziert eine deutlich umfassendere Nachvollziehbarkeit von personenbezogenen Handlungsabläufen als die reine Analyse von Onlineaktivitäten. Zweitens können in den Austausch und die Analyse der Daten durch die Abfolge der verschiedenen Schichten der IoT-Architektur eine Reihe von Unternehmen einbezogen sein, sodass sich Fragen nach der Zuweisung der datenschutzrechtlichen und zivilrechtlichen Verantwortung stellen.

Wie soeben angemerkt, ist das Internet der Dinge noch längst nicht vollständig ausgebaut und in vielen Bereichen in einem Versuchsstadium befangen. Dies weist jedoch zugleich auf das Potenzial hin, durch rechtliche Gestaltung der Technik deren Entwicklung in sozial wünschenswerte Bahnen zu lenken.

---

[1] *Pagallo/Durante/Monteleone*, in: Leenes et al. (Hrsg.), Data Protection and Privacy: (In)visibilities and Infrastructures, 2017, 59 (60); *Metzger*, GRUR 2019, 129 (129).

[2] *Madaan/Nurse/de Roure/O'Hara/Hall/Creese*, A Storm in an IoT Cup: The Emergence of Cyber-Physical Social Machines, Working Paper, 2018, https://ssrn.com/abstract=3250383, 2.

[3] Vgl. *Di Martino et al.*, in: Di Martino et al. (Hrsg.), Internet of Everything, 2018, 1 (9 f.), die mit dem Begriff des *Internet of People* operieren: „The ultimate objective of interconnected sensors and devices in this context [of the Internet of People] is to *anticipate the owner's needs* […]." [Hervorhebung im Original].

[4] Genauer *Ziegler et al.*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 9 (33).

II. Ökonomische Folgerungen: Daten als Gegenleistung

Leistungen sowie ihre Neben- und Folgeprozesse vollziehen sich infolge der techno-physischen Vernetzung zunehmend digital. Dies impliziert zugleich, dass der Begriff der „digitalen Leistungen" überaus weit ist.[5] Die folgende Untersuchung klammert daher Fragestellungen, die sich mit der digitalen Natur des durch den Anbieter zur Verfügung gestellten Leistungsobjekts (digitale Güter/Inhalte/Dienstleistungen, z. B. E-Books[6]) verbinden, weitgehend aus[7] und beschränkt sich auf das, was im Folgenden ein „datenbasiertes Austauschverhältnis" genannt wird. Dieses wird verstanden als Beziehung, in der personenbezogene Daten einen Teil des Leistungspakets zumindest einer Partei darstellen.

Es ist kein Geheimnis, dass die weitreichende technische Vernetzung und Übertragung von Daten zwischen verschiedenen Akteuren zur Folge hat, dass diese Daten selbst in ökonomischer Perspektive in zunehmendem Maße als werthaltige Produkte betrachtet werden. Dies ist an sich keine neue Entwicklung: Schon immer konnten Daten, und daraus gewonnene Informationen und Erkenntnisse, einen ökonomischen Wert haben.

1. Daten als funktionales Geldäquivalent

Neu ist hingegen zweierlei: Erstens werden Daten im IoT und in der digitalen Wirtschaft nicht nur irgendwie ökonomisch monetarisiert; vielmehr haben sie dabei teilweise auch den Charakter einer Gegenleistung, die funktional an die Stelle einer monetären Transaktion tritt.[8] Zweitens steht mit dem maschinellen Lernen eine Technologie zur Verfügung, die es ermöglicht, zwischen personenbezogenen Daten und ökonomisch relevanten Präferenzen neue Korrelationen aufzuzeigen.[9] Dies beeinflusst die Wertschöpfungskette, die Daten durchlaufen, erheblich.

Auch hier offenbart sich ein Vernetzungscharakter: Häufig erfolgt eine Nutzung der Daten durch verschiedene, netzartig verbundene Unternehmen und

[5] *Auer*, ZfPW 2019, 130 (130): „Versteht man den Begriff [der digitalen Leistung] im weitesten Sinne, umfasst er sämtliche Leistungsbeziehungen, deren Leistungsgegenstand oder Leistungsmodalitäten in digitalen Gütern oder Dienstleistungen bestehen oder die durch digitale Verfahren durchgeführt oder vermittelt werden – und damit fast alles, was das Arsenal der Gesellschaft 4.0 an Gütern, Dienstleistungen und Vertragsschlussmodalitäten bereithält.".

[6] Dazu etwa *Grünberger*, AcP 218 (2018), 213 (247 ff., 270 ff.); *Kuschel*, Der Erwerb digitaler Werkexemplare zur privaten Nutzung, 2019, 31 ff., 53 ff.; *Wendehorst*, in: Schulze/Staudenmayer (Hrsg.), Digital Revolution. Challenges for Contract Law in Practice, 2016, 189 (197 f.).

[7] Siehe zu diesen Fragestellungen die Nachweise in § 1, Fn. 94 und 42.

[8] Siehe statt vieler *de Franceschi*, in: Schmidt-Kessel/Kramme (Hrsg.), Geschäftsmodelle in der digitalen Welt, 2017, 113 (115) m. w. N.; Sattler, JZ 2017, 1036 (1036); *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (272 f.).

[9] Siehe die Nachweise oben, § 2, Fn. 99.

Plattformen,[10] ohne dass dies Nutzern hinreichend bewusst wäre. Der ökonomische Wert von Daten wird typischerweise in mehreren, miteinander verbundenen Austauschbeziehungen überhaupt erst geschöpft.

a) Austausch ohne monetäre Gegenleistung

Dass Daten in vielfältigen Transaktionen an die Stelle von monetärem Austausch treten, gehört mittlerweile zum festen Bestand der digitalen Wirtschaft.[11] Dies zeigt sich ganz deutlich an Vergütungsmodellen, die nach dem Grad differenzieren, mit dem die Nutzer Daten überlassen bzw. in Trackingmethoden einwilligen: Hier wird ein unternehmensseitiger Verzicht auf eine bestimmte Form der Datenauswertung durch einen monetären Preisaufschlag abgegolten.[12] Aber auch Geschäftsmodelle, die keine unmittelbare Gegenüberstellung von monetärer Differenz und unterschiedlicher Datenverarbeitung ermöglichen, bauen in nachvollziehbarer Weise auf der Werthaltigkeit der Überlassung von Daten auf, wenn sie keinen monetären Preis verlangen.[13] Wer beispielsweise die Kommunikationssoftware Skype herunterladen möchte, wird darauf aufmerksam gemacht, dass durch den Download der Software die Nutzungsbedingungen und die Richtlinien für Datenschutz und Cookies akzeptiert werden.[14] Diese wiederum beschreiben die Art und Weise, in der Skype personenbezogene Daten nutzt und verwertet. Die Marktpraxis, nach der Daten eine Gegenleistung darstellen, wurde im Jahr 2015 prominent von dem Kommissionsentwurf für eine Richtlinie über die Bereitstellung digitaler Inhalte aufgegriffen.[15]

Zwar liegt in der Vereinbarung einer nicht-monetären Gegenleistung wiederum kein Novum der digitalen Wirtschaft. Schon seit Urzeiten wurde durch

---

[10] Siehe etwa, für Android Apps, *Gamba et al.*, An Analysis of Pre-installed Android Software, Working Paper, 2019, https://arxiv.org/abs/1905.02713, 5 ff.

[11] Siehe nur *Whittington/Hoofnagle*, 90 North Carolina Law Review 2011, 1327 (1346); *Hoofnagle/Whittington*, 61 UCLA Law Review 2014, 606 (626); *Metzger*, AcP 216 (2016), 817 (826); *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (275).

[12] Siehe etwa die Optionen der Washington Post, https://www.washingtonpost.com/gdpr-consent/: 30 $ Aufschlag auf das Jahresabonnement, dafür „No on-site advertising or third-party ad tracking"; von https://futurezone.at/ (zuletzt abgerufen am 27.9.2019): Verzicht auf Werbung für 3,60 € im Monat; sowie des Standard, https://abo.derstandard.at/purfaq/: werbe- und trackingfreies Abo für 6 € im Monat, als Alternative zur Nutzung des Onlineangebots gegen Einwilligung in die Datenverarbeitung; siehe auch Text bei § 4, Fn. 1121; ferner auch *Sattler*, in: Schmidt-Kessel/Grimm (Hrsg.), Telematiktarife & Co. – Versichertendaten als Prämienersatz, 2018, 1 (4 mit Fn. 2).

[13] Vgl. die empirischen Studien bei *Baumann et al.*, 61 Business & Information Systems Engineering 2019, 413 (426 ff.); *Gabel/Guhl/Klapper*, 56 Journal of Marketing Research 2019, 557 (566 ff.); ferner die weiteren Nachweise in § 2, Fn. 99.

[14] Siehe https://www.skype.com/de/ (zuletzt abgerufen am 2.5.2019).

[15] *Europäische Kommission*, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM(2015) 634 final, Art. 3 Abs. 1.

Tauschverträge eine Form von außer-monetärem Austausch gepflegt.[16] Die moderne Wirtschaft hat jedoch diese Form der ökonomischen Integration weitestgehend marginalisiert, da sich die Vorteile von Geld als einem universell einsetzbaren Austauschmittel langfristig durchgesetzt haben.[17] Die Abkehr von diesem Modell im Rahmen der „Kostenlos-Kultur" des Internets ist demgegenüber dem Umstand geschuldet, dass einerseits Daten selbst in immer größerem Umfang als Austauschmittel in verschiedensten Beziehungen wirtschaftlicher Art eingesetzt werden können und andererseits die auf Daten basierende Wertschöpfung erhebliches ökonomisches Potenzial birgt.

b) Wertschöpfung an Daten

Wichtig ist dabei zu erkennen, dass Daten selbst zumeist keinen unmittelbaren intrinsischen Wert haben, sondern vielmehr Grundlage einer Wertschöpfungskette sind, in deren Rahmen aus Daten Informationen gewonnen und daraus wiederum Erkenntnisse generiert werden.[18] Auch wenn die Möglichkeiten der Wertschöpfung aus Daten vielgestaltig sind, so lassen sich doch drei zentrale Typen identifizieren.

aa) Optimierung von Modellen

Im Rahmen der technischen Einführung im zweiten Kapitel dieser Arbeit wurde darauf hingewiesen, dass Techniken maschinellen Lernens typischerweise auf große Datenmengen angewiesen sind, um adäquat trainiert werden zu können.[19] Genau diese Trainingsdaten können die im Rahmen einer digitalen Austauschbeziehung gewonnenen personenbezogenen Daten darstellen.[20] Die überlassenen Daten werden dann dazu genutzt, maschinelle Prognosemodelle zu kalibrieren.

bb) Daten als Input für Modelle

Zweitens fungieren die im Rahmen von Austauschbeziehungen gewonnenen Daten als Input, mithin als zu analysierendes Datum, für eben diese (oder auch andere, nicht ML-basierte) Modelle. Sind letztere erst einmal entsprechend kalibriert, können sie, wie bereits bemerkt, genutzt werden, um anhand der über eine Zielperson gesammelten Daten bestimmte, ökonomisch relevante Para-

[16] *Dalton*, 16 Journal of Economic Issues 1982, 181 (182 f.).
[17] *Mankiw*, Macroeconomics, 9. Aufl. 2015, 82.
[18] *Zech*, GRUR 2015, 1151 (1152); *Bundesverband der digitalen Wirtschaft*, Data Economy, 2018, 10; *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf, ZEW Discussion Paper No. 17–043, 2017, http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf, 15–18; *Hacker*, ZfPW 148 (151–153).
[19] Siehe oben, § 2, Fn. 97.
[20] *Tufekci*, Machines Shouldn't Have to Spy On Us to Learn, Wired (25.3.2019), https://www.wired.com/story/machines-shouldnt-have-to-spy-on-us-to-learn/.

meter vorherzusagen.[21] Dabei lässt sich danach differenzieren, welches Unternehmen jeweils das Modell einsetzt: Dies kann das erhebende Unternehmen selbst sein, etwa wenn ein Modeunternehmen aus Nutzerdaten mögliche Fashiontrends für die kommende Modesaison abzuleiten versucht, oder Netflix personalisierte Empfehlungen für Filme ausspricht.[22] Ferner kann das Modell bei einem Unternehmen eingesetzt werden, das mit dem erhebenden konzernrechtlich verbunden ist, wie dies zum Beispiel beim Datenaustausch zwischen Facebook und WhatsApp der Fall ist.[23] Schließlich können auch die Modelle gänzlich anderer, mit dem erhebenden Unternehmen unverbundener Unternehmen von den Daten profitieren, etwa wenn diese über Werbeplattformen (*ad exchanges*) für personalisierte Werbung von Drittunternehmen genutzt werden.[24]

cc) Datenhandel

Eine dritte Form der Wertschöpfung an Daten besteht im schlichten Datenhandel, bei dem die Daten selbst das Objekt der primären Leistungspflicht darstellen.[25] Der Datenhandel kann sich im legalen wie auch im illegalen Bereich abspielen; in beiden Bereichen erfolgt eine nicht unerhebliche Wertschöpfung.[26]

Die Nicht-Rivalität von digitalen Datenbeständen sorgt dafür, dass sich diese unterschiedlichen Formen der Wertschöpfung nicht gegenseitig ausschließen.[27] Dies legt nahe, dass eine möglichst extensive, die Anzahl der digitalen Verarbeitungspartner maximierende Wertschöpfung, innerhalb gewisser Grenzen, typischerweise auch profitmaximierend sein wird. Es offenbart sich damit eine Parallele zwischen der technischen Architektur des IoT und der ökonomischen Architektur von Austauschprozessen, bei denen Daten als Gegenleistung fungieren: Beide sind strukturell auf eine Weiterleitung und Mehrfachverarbeitung von Daten angelegt.

---

[21] Siehe die Nachweise in § 2, Fn. 99; ferner *Bundesverband der digitalen Wirtschaft*, Data Economy, 2018, 13–15.

[22] Vgl. *Sorescu*, 34 Journal of Product Innovation Management 2017, 691 (694).

[23] Siehe dazu Bundeskartellamt, Fallbericht v. 15.2.2019, Az. B6–22/16 (*Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung*), 3 f.

[24] Siehe etwa *Lewis/Rao/Reiley*, in: Goldfarb/Greenstein/Tucker (Hrsg.), Economic Analysis of the Digital Economy, 2015, 191; *Urbach*, in Schmidt-Kessel/Kramme, Geschäftsmodelle in der digitalen Welt, 2017, 39 (55 f.); *Mellet/Beauvisage*, Consumption Markets & Culture 2019, 1 (10); siehe auch unten, § 4, Fn. 155 ff.

[25] Zu den USA, siehe etwa *Federal Trade Commission*, Data Brokers. A Call for Transparency and Accountability, 2014, 16 f.; *Kuempel*, 36 Northwestern Journal of International Law & Business 2016, 207; zu Deutschland, siehe *Goldhammer/Wiegand*, Ökonomischer Wert von Verbraucherdaten für Adress- und Datenhändler, 2017, 21 ff.

[26] *OECD*, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, 2013, 25–29; *Symantec*, Internet Security Threat Report, Volume 24, 2019, 56, 58.

[27] Vgl. *Goldhammer/Wiegand*, Ökonomischer Wert von Verbraucherdaten für Adress- und Datenhändler, 2017, 6 zur Mehrfachnutzung von Daten.

2. Systematisierung: Kategorien von Daten als Gegenleistung

In systematischer Hinsicht müssen jedoch verschiedene Kategorien von Geschäftsmodellen, bei denen Daten als Gegenleistung fungieren, unterschieden werden.[28] Der Hauptdifferenzierungsgesichtspunkt besteht darin, dass einige Modelle primär an eine datenbasierte Gegenleistung gekoppelt sind, während andere primär ein monetäres Entlohnungsmodell verfolgen. Dies ist für die rechtliche Bewertung durchaus relevant, wie sich im Einzelnen noch zeigen wird. In der Praxis treten zwar häufig Mischformen zwischen den einzelnen Modellen auf; dies macht ihre grundsätzliche Unterscheidung für die rechtliche Analyse jedoch nur umso wichtiger.

a) Datenbasiertes Grundmodell

Im Rahmen des datenbasierten Grundmodells wiederum können zwei Unterformen unterschieden werden: das vollkommen datenfinanzierte Modell und das Freemium-Modell.

aa) Vollkommen datenfinanzierte Modelle

Vollkommen datenfinanzierte Geschäftsmodelle zeichnen sich dadurch aus, dass die Endkunden bzw. Nutzer keinerlei monetäre Gegenleistung erbringen. Bei mehrseitigen Plattformen ist diese Bedingung erfüllt, sobald sie auf nur eine von der Plattform abgedeckte Marktseite zutrifft. Natürlich werden die Daten auf anderen Marktseiten durch die Plattform monetarisiert, etwa auf dem Werbemarkt.[29] Entscheidend ist jedoch, dass das Verhältnis zum Nutzer des primären Plattformangebots frei von einer monetären Komponente ist. Vollkommen datenfinanzierte Geschäftsmodelle kennzeichnen einen Großteil der „kostenlosen" Internetangebote, von Facebook über Google bis hin zu kleineren Smartphone-Applikationen wie Taschenlampen-Apps.

bb) Freemium-Modelle

Freemium-Modelle hingegen stellen eine Basisversion bereit, die kostenlos verfügbar ist, bieten jedoch zugleich Anreize für ein Upgrade auf eine monetär kostenpflichtige Premium-Version.[30] Im Gegensatz zu vollkommen datenfinanzierten Modellen ist hier also eine monetäre Entlohnung durch die Endkunden durchaus möglich. Das von den meisten Kunden genutzte Basismodell jedoch bleibt monetär kostenfrei, weshalb auch hier ein grundsätzlich

---

[28] Siehe dazu eingehend *Hacker*, ZfPW 2019, 148 (153 ff.).

[29] *Engert*, AcP 218 (2018) 304 (305 f., 310 f.); Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 214 f.

[30] *Kumar*, 92(5) Harvard Business Review 2014, 27; *Elvy*, 117 Columbia Law Review 2017, 1369 (1383 f., 1386).

datenbasiertes Geschäftsmodell vorliegt. Beispiele bieten etwa Dropbox[31] oder LinkedIn.[32]

b) Monetäres Grundmodell

Demgegenüber stellt in monetären Grundmodellen die geldförmige Entlohnung den Basistatbestand dar. Auch hier können zwei Untertypen unterschieden werden: Rabattmodelle und data on top-Modelle.

aa) Rabattmodelle

Rabattmodelle funktionieren dergestalt, dass zwischen den Parteien ein monetärer Preis als Gegenleistung vereinbart wird, der in Abhängigkeit von den überlassenen Daten um einen Rabattbetrag reduziert wird. Diese Modelle sind bereits seit langem in Form von Kundenbindungsprogrammen wie etwa *Payback* in Anwendung.[33] Darüber hinaus erfreuen sie sich seit längerer Zeit in der Versicherungswirtschaft einer gewissen Beliebtheit, wo die Höhe der Rabattierung von Versicherungsprämien oder bestimmte Rückzahlungen an Verhaltensweisen gekoppelt werden, auf die wiederum die Auswertung personenbezogener Daten Rückschlüsse geben (sog. Telematikversicherungen).[34] So haben etwa einige Kfz-Versicherungen sogenannte *pay as you drive*-Versicherungen im Angebot, bei denen der monetäre Aufwand des Versicherten unter anderem von der Güte des Fahrstils abhängig ist, der über verschiedene Sensoren im Auto erfasst werden kann.[35] Bei Rabattmodellen besteht daher ein rechtlicher Konnex typischerweise nicht zwischen der primären Leistung des Anbieters, etwa dem Versicherungsschutz, und der Überlassung von Daten, sondern zwischen letzterer und der Rabattierungskomponente.[36]

bb) Data on top-Modelle

Noch einmal anders stellen sich data on top-Modelle dar.[37] Hier wird ebenfalls die maßgebliche ökonomische Gegenleistung in monetärer Form erbracht,

[31] *Dropbox*, Wieviel kostet Dropbox, https://www.dropbox.com/de/help/billing/cost.

[32] *LinkedIn*, Kostenlose LinkedIn Konten und kostenpflichtige Premium-Mitgliedschaften, https://www.linkedin.com/help/linkedin/answer/1412/kostenlose-linkedin-konten-und-kostenpflichtige-premium-mitgliedschaften?lang=de.

[33] *Unabhängiges Landeszentrums für Datenschutz Schleswig-Holstein*, Kundenbindungssysteme und Datenschutz, Gutachten, 2003, 23 ff.; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 268 ff.

[34] Dazu etwa *Rudkowski*, ZVersWiss 2017, 453; *Kraft/Hering*, ZVersWiss 2017, 503; *Brömmelmeyer*, r + s 2017, 225; *Lüttringhaus*, in: Festschrift Basedow, 2018, 55; ferner die Beiträge in *Schmidt-Kessel/Grimm* (Hrsg.), Telematiktarife & Co. – Versichertendaten als Prämienersatz, 2018; *Hacker*, ZfPW 2019, 148 (154 ff.).

[35] Siehe etwa *Grimm*, in: Schmidt-Kessel/Grimm (Hrsg.), Telematiktarife & Co. – Versichertendaten als Prämienersatz, 2018, 47; *Schumann*, Pay As You Drive, 2017.

[36] *Rudkowski*, ZVersWiss 2017, 453 (486).

[37] Begriff und weitere Nachweise bei *Hacker*, ZfPW 2019, 148 (156 f.).

die überlassenen Daten sind jedoch nicht Grundlage für einen Rabatt. Vielmehr kommen sie zu der monetären Gegenleistung schlicht hinzu. Dieses Format bestimmt nicht nur das Internet der Dinge,[38] es wird auch von vielen Onlinehändlern gewählt, etwa Amazon,[39] oder Vermittlern, etwa Airbnb.[40] Bestellt der Kunde zum Beispiel Schuhe im Wert von 50 € bei einem Onlinehändler, so bezahlt er damit (typischerweise) auch die Händlermarge. Zugleich jedoch werden personenbezogene Daten erhoben, analysiert und in wertschöpfender Art und Weise verarbeitet. Die daraus entstehenden Umsätze und Gewinne treten mithin aus Sicht des Anbieters neben die aus der monetären Transaktion gezogenen. Es bestehen Anzeichen dafür, dass gerade bei Onlinehändlern wie Amazon die datenbasierte Entlohnungskomponente, die typischerweise auch personalisierte Werbung umfasst, zunehmend gegenüber der monetären an Bedeutung gewinnt.[41] Auch in anderen Bereichen fungieren Daten als eine weitere Entlohnungskomponente: Monetär billigere Smartphones[42] oder Apps[43] z. B. sammeln tendenziell mehr personenbezogene Daten.

III. Die Multirelationalität von personenbezogenen Daten

Die technische und ökonomische Analyse der fortschreitenden Vernetzung der Datenerhebung und -Verarbeitung impliziert eine erste regulatorische Herausforderung, die das Recht bewältigen muss. Personenbezogene Daten sind in verschiedener Hinsicht multirelational: Sie sagen nicht nur in semantischer Hinsicht häufig etwas über die kommunikative oder die Handlungsumgebung der betroffenen Person, insbesondere ihre Interaktionspartner, aus,[44] sondern

---

[38] *Wendehorst*, in: Schulze/Staudenmayer (Hrsg.), Digital Revolution. Challenges for Contract Law in Practice, 2016, 189 (193 f.).

[39] *Amazon Europe*, Cookies, https://www.amazon.de/gp/help/customer/display.html/?nodeId=201890250 (zuletzt abgerufen am 9.5.2019).

[40] *Airbnb*, Cookie-Richtlinie, https://www.airbnb.de/terms/cookie_policy (zuletzt abgerufen am 9.5.2019), unter „Warum Airbnb diese Technologien einsetzt".

[41] *Lindner*, Für Amazon wird Werbung wichtiger, FAZ (20. September 2018), http://www.faz.net/aktuell/wirtschaft/diginomics/unternehmen-investieren-werbebudget-vermehrt-bei-amazon-15796306.html.

[42] *Privacy International*, Buying a smart phone on the cheap? Privacy might be the price you have to pay, Privacy International (20.9.2019), https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay.

[43] *Kummer/Schulte* 65 Management Science 2019, 3470 (3480).

[44] Dies betont das klassische Verständnis von Multirelationalität, siehe *Zöllner*, Informationsordnung und Recht, 1990, 22 f.; *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, 2001, 37 f.; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 221 ff.; *Roßnagel*, SVR 2014, 281 (283); *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 258 f.; siehe auch *Zech*, Information als Schutzgegenstand, 2012, 37 f., 53 f.; ferner BVerfG NJW 1984, 419 (422) – Volkszählung: „Der einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‚seine' Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information,

auch ihre technische Verarbeitung und ihr ökonomischer Wert weisen über das primäre Vertrags- bzw. Nutzungsverhältnis zwischen betroffener Person und Erstanbieter hinaus. Ihnen ist damit typischerweise ein Drittbezug eingeschrieben: zu Monetarisierungszwecken werden Daten *an* Dritte, etwa *ad exchanges*, weitergeleitet;[45] Daten werden unmittelbar *durch* Drittanbieter im Rahmen des *third-party tracking* erhoben;[46] und im Internet der Dinge erheben Erstanbieter Daten – gewollt oder ungewollt – *bei* Dritten, mit denen kein primäres Nutzungsverhältnis besteht.[47] Dies gilt im Übrigen grundsätzlich auch für solche Daten, die Nutzer aktiv und bewusst, etwa im Verlauf eines Registrierungsprozesses,[48] überlassen: Auch solche zunächst lediglich für das bilaterale Verhältnis relevanten Informationen werden häufig, wenn auch zum Teil in pseudonymisierter Form, an Drittanbieter zu Werbezwecken weitergeleitet.[49] Signum der digitalen Wirtschaft ist daher, dass das aus dem bürgerlichen Recht bekannte Modell des Zweipersonenverhältnisses jedenfalls in technisch-ökonomischer Hinsicht regelmäßig auf ein Mehrpersonenverhältnis erweitert werden muss. Aus diesen multirelationalen Konstellationen werden in der Folge drei Leitfälle entwickelt, welche die weitere Analyse dieser Arbeit prägen werden.[50] Dieser Drittbezug erhöht die Komplexität des autonomen Umgangs mit personenbezogenen Daten und stellt das Recht vor besondere Herausforderungen.

B. Zweite rechtliche Herausforderung: Ambivalenz vernetzter Datenerhebung und -verarbeitung

Sowohl in technischer als auch ökonomischer Hinsicht sind die Strukturen der digitalen Wirtschaft mithin auf die Vernetzung von Akteuren und den Austausch von Daten zwischen diesen angelegt. Regulatorisch stellt dies insbesondere deshalb eine Herausforderung dar, weil diese Formen datenbasierter Austauschprozesse, wie letztlich praktisch jede neue Technologie, einerseits ein erhebliches Potenzial für individuelle und kollektive Gewinne bereithalten, andererseits jedoch zugleich mit signifikanten Risiken auf individueller und kollektiver Ebene einhergehen.[51] Ziel eines rechtlichen Rahmens muss es daher

---

auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann"; aufgenommen von BGH NJW 2009, 2888 (2891 f.).

[45] Siehe oben, § 3, Fn. 24 sowie unten, § 4, Fn. 155 ff. und § 3 D.I.1.

[46] Siehe unten, § 3 D.I.2.

[47] Siehe unten, § 3 D.I.3.

[48] Siehe oben, Text bei § 2, Fn. 1.

[49] Siehe nur die von der Rechtsprechung für unwirksam erklärte Klausel in den AGB von Facebook: LG Berlin, MMR 2018, 328 Rn. 66; KG MMR 2020, 239 Rn. 50.

[50] Siehe unten, § 3 D.

[51] *DeNardis*, The Internet in Everything, 2020, 3 f.; siehe auch Picard, *Affective Computing*, 1997, 136.

sein, Möglichkeiten für die Ausschöpfung des Potenzials bereitzustellen und gleichzeitig die relevanten Risiken zu minimieren.

I. Potenzial

Erhebliches Potenzial bieten die Vernetzung von Geräten und der Einsatz von Daten als Gegenleistung sowohl auf individueller als auch sozialer Ebene.

1. Individuelle Ebene

Auf individueller Ebene sind im Wesentlichen drei Phänomene zu berücksichtigen: eine präzisere Präferenzerfüllung, die Möglichkeit einer Zeitersparnis und eine Kaufkraftsteigerung.

a) Präferenzerfüllung

Wenn im Rahmen des IoT oder bei sonstigen Onlineaktivitäten Daten über Lebensgewohnheiten gesammelt werden, so lassen sich daraus Rückschlüsse auf die Präferenzen und Restriktionen der Nutzer ziehen.[52] Dies ist typischerweise gerade das Ziel der von den Verarbeitern angestellten Datenanalyse, die darauf aufbauend maßgeschneiderte Produkte anbieten.[53] Was manche Nutzer als Belästigung empfinden, kann für andere jedoch eine Bereicherung darstellen: Jedenfalls potenziell können so präferenzkonformere Angebote gemacht werden als ohne Datenanalyse.[54] Dies gilt nicht nur für personalisierte Werbung. Im Rahmen des IoT kann das Lebensumfeld durch die Aktuatoren in den Geräten an ermittelte Präferenzen automatisiert angepasst werden.[55] Temperatur, Lichtstärke oder Belüftung eines Smart Home können so die Bedürfnisse und Wünsche der Bewohner widerspiegeln.

b) Zeitersparnis

Diese Automatisierung bedingt zugleich eine Zeitersparnis, die sich bei der werbebasierten Produktsuche in geringeren Suchkosten und bei der Regelung des Lebensumfelds in der Vermeidung von Opportunitätskosten niederschlägt. Mit der Präferenzerfüllung hängt auch dieser Punkt eng zusammen, da hierdurch weitere Präferenzen für eine anderweitige Zeitgestaltung, sei es durch Freizeitaktivitäten, sei es durch berufliche Aktivitäten, besser erfüllt werden können.

---

[52] Siehe die Nachweise oben, § 2, Fn. 99.

[53] Siehe etwa *United States Government Accountability Office*, Internet of Things, 2017, 16–19 sowie die Industrieberichte von *Cognizant*, The Rise of the Smart Product Economy, 2015; *Accenture Strategy*, Satisfy the Craving for Insurance Personalization, 2017, 5.

[54] *Hoofnagle/Kesari/Perzanowski*, 87 George Washington Law Review 2019, 783 (804).

[55] *United States Government Accountability Office*, Internet of Things, 2017, 16–18 sowie oben, § 2 D.

c) Kaufkraftsteigerung

Speziell der Einsatz von Daten als Gegenleistung bedingt ferner, dass die Kaufkraft der Nutzer, im weitesten Sinne, gesteigert wird.[56] Ihr Budget besteht nicht nur aus der für sie verfügbaren Menge an Geld, sondern ist zusätzlich durch die übertragbaren Daten angereichert, die sie typischerweise selbst und zu sehr geringen Grenzkosten produzieren. Gerade Geringverdiener könnten sich womöglich nicht alle Onlinedienste, die sie nutzen, mit monetärer Zahlung erkaufen. Die Möglichkeit, Daten als Gegenleistung einzusetzen, erhöht mithin ihr Budget und damit ihre Konsummöglichkeiten.

2. Sozialer Nutzen

Neben diesen individuellen Effekten können durch vernetzte Geräte und Datenerhebung im Rahmen von Onlineaktivitäten auch soziale Gewinne erwirtschaftet werden. Datenaustausch und -handel kann zur Betrugsvermeidung beitragen, wie die US-amerikanische FTC betont.[57] Verfechter der personalisierten Medizin weisen etwa auf effektivere und neue Therapiemethoden durch extensive Datenanalyse hin.[58] Die Aggregation von Lokalisierungsdaten aus vernetzten Fahrzeugen kann zu Stauvermeidung und damit zum Betrieb des Allmendeguts des öffentlichen Straßenverkehrs beitragen. Durch Vernetzung im Bereich der Industrie (Industrie 4.0) lassen sich in der Produktion und Distribution Effizienzgewinne erzielen.[59] Die Liste ließe sich beliebig erweitern.

II. Datenschutzrechtliche Risiken

Diesem substantiellen Potenzial der Vernetzung und des Einsatzes von Daten als Gegenleistung stehen, wie bei fast allen technischen Entwicklungen, jedoch

---

[56] Siehe *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter III.1.

[57] *Federal Trade Commission*, Data Brokers. A Call for Transparency and Accountability, 2014, 47.

[58] Siehe etwa *Nationale Akademie der Wissenschaften Leopoldina/acatech – Deutsche Akademie der Technikwissenschaften/Union der deutschen Akademien der Wissenschaften*, Individualisierte Medizin – Voraussetzungen und Konsequenzen, 2014, 30–33; *Benson*, 279 Journal of Internal Medicine 2016, 229; *Poland/Ovsyannikova/Kennedy*, 36 Vaccine 2018, 5350; empirische Studie zur wechselseitigen Ausschließlichkeit von positiven Netzwerkeffekten aus der Adoption von elektronischen Patientenakten einerseits und strengeren Datenschutzregimen andererseits bei *Miller/Tucker*, 55 Management Science 2009, 1077 (besonders 1091).

[59] *European Commission*, A Digital Single Market Strategy for Europe – Analysis and Evidence, Commission Staff Working Document, SWD (2015) 100 final, 57; *Zech*, GRUR 2015, 1151 (1151 f.); *United States Government Accountability Office*, Internet of Things, 2017, 19 f.

auch erhebliche Risiken entgegen.[60] Nicht umsonst wird das Datenschutzrecht auch als Recht des Managements von Risiken bezeichnet, die sich aus spezifischen technologischen Prozessen ergeben.[61]

Diese Risiken lassen sich grob in zwei Klassen einteilen. Besonders wichtig sind unter dem Gesichtspunkt der Marktregulierung, der für diese Arbeit entscheidend ist, bestimmte Formen von Marktversagen, die sich aus den genannten technischen Phänomenen ergeben können (1.). Ferner soll jedoch nicht unterschlagen werden, dass auch weitere, im weitesten Sinne soziale Risiken bestehen, die sich zum Teil aus dem Marktversagen ergeben, durch eine rein ökonomische Perspektive jedoch nur unzureichend erfasst werden können (2.).

1. Vier Typen von Marktversagen

Insgesamt lassen sich verschiedene Typen von Marktversagen beschreiben, die an den Vernetzungscharakter oder den Einsatz von Daten als Gegenleistung anknüpfen. Vier Typen sind für die hiesige Analyse entscheidend: Informationsasymmetrie; verhaltensökonomische Effekte; Externalitäten; und die Unschärfe des Datenpreissignals. Sie erklären zugleich unterschiedliche Aspekte des Paradoxes der Privatheit (*privacy paradox*), der Differenz von erklärten und gelebten Datenschutzpräferenzen.[62]

Gerade die Vernetzungseffekte können freilich eine weitere Form von Marktversagen bedingen: Marktmacht von datenverarbeitenden Unternehmen. Eine stetig wachsende Literaturströmung widmet sich diesem Problem,[63] das auch der spezifischen Kostenstruktur von digitalen Angeboten (teilweise hohe *sunk costs*, gegen null tendierende Grenzkosten in Produktion und Distribu-

---

[60] Siehe nur *Thoma*, ZD 2013, 578 (579), die Nachweise oben in § 1, Fn. 82 sowie den 75. Erwägungsgrund der DS-GVO.

[61] Siehe insbesondere *Gellert*, 5 International Data Privacy Law 2015, 3 (4); ferner bereits oben, Text bei § 1, Fn. 82 f.

[62] Siehe aus der umfangreichen Literatur etwa *Barnes*, 11(9) First Monday, 2006, http://firstmonday.org/issues/issue11_9/barnes/index.html; *Norberg/Horne/Horne*, 41 Journal of Consumer Affairs 2007, 100; *Acquisti/Taylor/Wagman*, 54 Journal of Economic Literature 2016, 442 (476–478); *Kokolakis*, 64 Computers & Security 2017, 122.

[63] Grundlegend *Katz/Shapiro*, 75 American Economic Review 1985, 424 (426 ff.); siehe ferner *Evans/Schmalensee*, 3 Competition Policy International 2007, 151; *Argenton/Prüfer*, 8 Journal of Competition Law and Economics 2012, 73; *Lianos/Motchenkova*, 9 Journal of Competition Law & Economics 2013, 419; *Rubinstein/Gal*, 59 Arizona Law Review 2017, 339 (349 ff.); *Schweitzer et al.*, Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, Gutachten für das Bundesministerium für Wirtschaft und Energie, 2018; *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269; *Burri*, in: Mathis/Tor, New Developments in Competition Law and Economics, 2019, 241; *Botta/Wiedemann*, The Antitrust Bulletin 2019, 428 (432 f.); zum IoT auch *Hoofnagle/Kesari/Perzanowski*, 87 George Washington Law Review 2019, 783 (836 ff.); ferner *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter III.2.

tion[64]) geschuldet sein kann. Daraus resultieren jedoch im wesentlichen kartellrechtliche Probleme, die hier allenfalls am Rande beleuchtet werden. Für eine ausführliche Darstellung dieses Wettbewerbsproblems sei auf die genannte Literatur verwiesen.

a) Informationsasymmetrie: Mangelnde Kenntnis der Datenverarbeitung

Hinlänglich bekannt ist aus der ökonomischen Analyse von Märkten, dass imperfekte Informationsverteilung zu Marktversagen führen kann.[65] Informationsasymmetrien zwischen Marktteilnehmern können dabei entweder daraus resultieren, dass eine Information gar nicht erst offengelegt wird, dass Unsicherheit über die Korrektheit einer offengelegten Information besteht, oder aber daraus, dass die Information von der Marktgegenseite nicht zur Kenntnis genommen wird.[66] Im Rahmen der hier betrachteten Phänomene spielt insbesondere der zuletzt genannte Aspekt eine erhebliche Rolle.

Das Datenschutzrecht verpflichtet Verarbeiter, alle für eine informierte Entscheidung relevanten Informationen über geplante Datenverarbeitungsvorgänge offenzulegen, Art. 4 Nr. 11, 12–14 DS-GVO. Es ist jedoch kein Geheimnis, dass diese Informationen, selbst wenn sie zur Verfügung gestellt werden, zumeist nicht zur Kenntnis genommen werden. Dafür lassen sich zwei Gründe anführen: kognitive Informationsüberlastung und rationale Ignoranz.

aa) Informationsüberlastung

Die Offenlegung erfolgt typischerweise in drei verschiedenen Dokumenten, den Nutzungsbedingungen, der Richtlinie zum Datenschutz und der Richtlinie über Cookies. Diese Komplexität wird noch gesteigert durch die typische Vielzahl von Verarbeitungsvorgängen, die bereits bei der Datenverarbeitung durch lediglich ein Unternehmen anfallen. Verstärkt wird die Informationslast dabei durch die mangelnde Lesbarkeit von Datenschutzerklärungen (*readability*)[67] sowie die oben geschilderte Drittdimension: die Erfassung von Daten durch Dritte (z. B. Social Plug-Ins) und von Dritten (z. B. Ehepartner); sowie die Weiterleitung von Daten an Dritte, einerseits zu Werbezwecken oder andererseits zur Verarbeitung in der Cloud.[68]

---

[64] Vgl. *Goldfarb/Greenstein/Tucker*, in: Goldfarb/Greenstein/Tucker (Hrsg.), Economic Analysis of the Digital Economy, 2015, 1 (2).

[65] Grundlegend *Akerlof*, 84 The Quarterly Journal of Economics 1970, 488; siehe auch *Veljanovski*, in: Baldwin/Cave/Lodge (Hrsg.), The Oxford Handbook of Regulation, 2010, 18 (21 f.); spezifisch zu Datenmärkten *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter III.2.; knapp ferner *Metzger*, in: Festschrift Basedow, 2018, 131 (151 f.); *Drexl*, NZKart 2017, 415 (418).

[66] Vgl. *Hacker*, Verhaltensökonomik und Normativität, 2017, 414–417.

[67] *Fabian/Ermakova/Lentz*, Proceedings of the International Conference on Web Intelligence 2017, 18; *Becher/Benoliel*, in: Mathis/Tor (Hrsg.), Consumer Law & Economics, 2020, (im Escheinen).

[68] Zum Kontrollverlust beim Cloud Computing, siehe *Artikel-29-Datenschutzgruppe*,

Bekannt ist jedoch aus der empirischen Verhaltensforschung, dass die Menge der kognitiv sinnvoll verarbeitbaren Informationen beim Menschen deutlich beschränkt ist.[69] Die Grenze der Simultanverarbeitungsfähigkeit liegt typischerweise bei zwischen vier und zehn Informationseinheiten.[70] Dies deutet bereits darauf hin, dass Informationen über komplexe digitale Verarbeitungsprozesse aufgrund von kognitiven Engpässen nicht vollständig rezipiert werden.[71] Zwar können strukturierte Formate der Informationsvermittlung die kognitive Verarbeitung unterstützen;[72] die Verteilung der bei der Datenverarbeitung relevanten Informationen über die genannten Dokumente, mit häufig komplexen Querverweisen, wirkt jedoch tendenziell genau in die entgegengesetzte Richtung.[73]

bb) Rationale Ignoranz

Doch nicht nur die beschränkte menschliche Verarbeitungskapazität führt zu geringer Rezeption von Informationen über Datenverarbeitungsvorgänge. Nutzer bleiben, auch wenn sie vollkommen rational handeln, typischerweise uninformiert aufgrund von rationaler Ignoranz.[74] Die erwarteten Suchkosten (Zeit, kognitive Verarbeitung) liegen über dem erwarteten Gewinn, der aus der Lektüre der Nutzungsbedingungen, der Datenschutzerklärung und der Cookie-Richtlinie gezogen werden kann.[75] Daher lässt sich vorhersagen, dass ein Großteil der Nutzer die genannten Dokumente einfach ignorieren wird.

Dies wird durch die empirische Forschungslage bestätigt. Eine Studie zeigte auf, dass lediglich ein bis zwei von 1000 Nutzern die Endnutzerlizenzvereinbarung vor dem Download kostenloser Software zur Kenntnis nehmen.[76] Bei Datenschutzerklärungen sieht es nicht anders aus: In einer empirischen Studie

---

Stellungnahme 05/2012 zum Cloud Computing, WP 196, 2012, 6 f.; *Bolognini/Balboni*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 71 (74 f.).

[69] Grundlegend *Miller*, 63 The Psychological Review 1956, 81; aus der jüngeren Literatur *Cowan*, 24 Behavioral and Brain Sciences 2000, 87; *Eppler/Mengis*, 20 Information Society 2004, 325; siehe auch *Hacker*, Verhaltensökonomik und Normativität, 2017, 117 ff.

[70] *Hacker*, Verhaltensökonomik und Normativität, 2017, 118 f.

[71] *Calo*, 87 Notre Dame Law Review 2012, 1027 (1054).

[72] *Bettman/Payne/Staelis*, 5 Journal of Public Policy & Marketing 1986, 1 (9, 15, 21); zu Datenschutzerklärungen *McDonald et al.*, Proceedings of the 9th Symposium on Usable Privacy and Security 2009, 37.

[73] Siehe etwa die Untersuchung der norwegischen Verbraucherbehörde *Forbrukerrådet*, Deceived by Design, Bericht, 2018; ferner *Conti/Sobiesk*, Proceedings of the 19th International Conference on World Wide Web 2010, 271; *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (4).

[74] *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 236; siehe auch, zum strukturell identischen Problem bei AGBs, *Eisenberg*, 47 Stanford Law Review 1995, 211 (241–243).

[75] Vgl. *McDonald/Cranor*, 4 I/O Journal of Law and Policy for the Information Society 2008, 543.

[76] *Bakos/Marotta-Wurgler/Trossen*, 43 The Journal of Legal Studies 2014, 1; ähnliche Ergebnisse *Obar/Oehldorf-Hilsch*, 21 Information, Communication & Society 2018, 1 (14): 86 % der Teilnehmer beschäftigten sich weniger als eine Minute mit AGB, deren Lektüre 15 Minuten dauern würde, 98 % weniger als 5 Minuten.

ignorierten 74 % der Teilnehmer die Datenschutzerklärung vollkommen und die übrigen 26 % verwandten so wenig Zeit auf die Informationen, dass sie kaum sinnvolle Erkenntnisse gewonnen haben können.[77] In einer weiteren Feldstudie klickten gar nur 0,2 % der Teilnehmer während eines Bestellvorgangs auf die Datenschutzerklärung.[78] Das qualitativ gleiche Muster zeigte sich selbst bei Datenschutzerklärungen, die nach den *best practices* von Verbraucherschutzbehörden auf ihre Lesbarkeit hin optimiert worden waren.[79] Auch hier waren kaum Teilnehmer bereit, trotz eines im Sexualbereich angesiedelten Versuchsaufbaus die Datenschutzerklärung hinreichend zur Kenntnis zu nehmen.

Problematisch ist hierbei insbesondere, dass *praktisch niemand* die Datenschutzerklärungen und verwandte Materialien zur Kenntnis nimmt.[80] Dies führt dazu, dass keine sogenannte informierte Minderheit entsteht, welche durch ihre Marktentscheidungen die Anbieter disziplinieren könnte.[81] Zudem setzt der positive Effekt der informierten Minderheit für die uniformierte Mehrheit voraus, dass die Anbieter nicht effektiv zwischen beiden Gruppen unterscheiden können.[82] Auch dies ist im Zeitalter der fortgeschrittenen Datenanalyse jedoch zunehmend unwahrscheinlich. Damit lässt sich, im Einklang mit der einschlägigen Literatur,[83] festhalten, dass tatsächlich ein marktrelevantes Informationsproblem hinsichtlich der Datenverarbeitungsvorgänge besteht.

b) Verhaltensökonomische Effekte bei der Datenbewertung

Selbst wenn die Nutzer, aus den Datenschutzerklärungen oder sonstigen Quellen, hinreichend über die Datenverarbeitungspraktiken informiert sind, kön-

---

[77] *Obar/Oehldorf-Hilsch*, 21 Information, Communication & Society 2018, 1 (13).

[78] *ConPolicy*, Wege zur besseren Informiertheit im Datenschutz, 2018, 42 (n = 91).

[79] *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S41.

[80] Siehe nochmals *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S41 (S52 f.); *Obar/Oehldorf-Hilsch*, 21 Information, Communication & Society 2018, 1; *Rothmann/Buchner*, DuD 2018, 342 (344 f.); siehe auch *Becher/Benoliel*, in: Mathis/Tor (Hrsg.), Consumer Law & Economics, 2020, (im Escheinen).

[81] Zur Verhinderung von informationellem Marktversagen durch eine informierte Minderheit grundlegend aus theoretischer Perspektive *Schwartz/Wilde*, 127 University of Pennsylvania Law Review 1979, 630; siehe auch *Gottschalk*, AcP 206 (2006), 555 (564); *Beimowski*, Zur ökonomischen Analyse Allgemeiner Geschäftsbedingungen, 1989, 108 f.; *Adams*, in: Neumann (Hrsg.), Ansprüche, Eigentums- und Verfügungsrechte, 1983, 655 (670 ff.); zur empirischen Unhaltbarkeit dieser These jedenfalls für AGB von Endnutzerverträgen *Bakos/Marotta-Wurgler/Trossen*, 43 The Journal of Legal Studies 2014, 1; ferner allgemeiner *Wagner/Eidenmüller*, 86 University of Chicago Law Review 2019, 581 (607); *Hacker*, Verhaltensökonomik und Normativität, 2017, 657.

[82] *Schwartz/Wilde*, 127 University of Pennsylvania Law Review 1979, 630 (638).

[83] Siehe nur *Acquisti/Brandimarte/Loewenstein*, 347 Science 2015, 509 (509); *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 236–238; *Blume*, 2 International Data Privacy Law 2012, 26 (29); *Zuiderveen Borgesius*, Improving Privacy Protection in the Area of Behavioural Targeting, 2015, Kapitel 7; *Boerman/Kruikemeier/Zuiderveen Borgesius*, 46 Journal of Advertising 2017, 363 (367).

nen bei der Entscheidung über die Preisgabe von Daten im Gegenzug zur Erlangung von Diensten oder sonstigen Vorteilen eine Reihe von kognitiven Verzerrungen auftreten, welche die Rationalität dieser Entscheidung infrage stellen können. Auch dies wurde bereits in der Literatur ausführlich aufgearbeitet,[84] sodass hier ein kurzer Überblick genügt.

Neuere Experimente legen nahe, dass derartige verhaltensbasierte Effekte besonders bei realen (im Gegensatz zu hypothetischen) Datenschutzentscheidungen eine Rolle spielen.[85] Bekannt ist etwa, dass Menschen dazu neigen, sie selbst betreffende Risiken zu unterschätzen (*optimism bias*).[86] Dieser in bestimmten Situationen durchaus nützliche Effekt kann jedoch im Kontext der Datenverarbeitung dazu führen, dass die Nutzer die Risiken, die sie durch ihre Datenpreisgabe eingehen, für zu gering veranschlagen.[87] Gerade zeitlich ferner liegende Risiken wie die mögliche Verwendung von Daten durch Dritte, etwa potenzielle Arbeitgeber oder Versicherungsunternehmen im Rahmen zum Zeitpunkt der Datenüberlassung noch nicht absehbarer Vertragsverhandlungen, können so kognitiv heruntergespielt werden. Ähnliche Effekte lassen sich durch gezieltes *framing* der Risiken erzielen.[88]

Ferner folgt gerade aus der zeitlichen Struktur des Tausches von Daten gegen Dienste ein weiteres Hindernis für eine rationale Entscheidung. Viele Menschen diskontieren die Zukunft nicht, wie es die rationale ökonomische Theorie nahelegt, mit einem über die Zeit konstanten Diskontfaktor (exponentielle Diskontierung), sondern diskontieren den Übergang von der unmittelbaren Zukunft zur Gegenwart besonders stark (β-δ-Diskontierung).[89] Dieser *present bias* führt dazu, dass der gegenwärtige, unmittelbar zur Verfügung stehende Gewinn überproportional stärker gewichtet wird als zeitlich fernliegende Einbußen. Genau diese Struktur haben aber typischerweise die genannten Konstellationen: Dem unmittelbaren Erwerb eines Zugangs zu einer Dienstleistung oder einem Inhalt stehen lediglich zeitlich in die Zukunft verschobene, mögliche Einbußen aufgrund der Datenverarbeitung gegenüber.[90] Menschen

[84] Siehe vor allem *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 233 ff.; *Acquisti/Taylor/Wagman*, 54 Journal of Economic Literature 2016, 442; *Zuiderveen Borgesius*, Improving Privacy Protection in the Area of Behavioural Targeting, 2015, Kapitel 2 und 7; *Solove*, 126 Harvard Law Review 2012, 1880 (1883 ff.).

[85] *Adjerid/Peer/Acquisti*, 42 MIS Quarterly 2018, 465.

[86] Siehe nur *Weinstein/Klein*, 15 Journal of Social and Clinical Psychology 1996, 1; ausführlich *Hacker*, Verhaltensökonomik und Normativität, 2017, 87–89.

[87] *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 385.

[88] *Adjerid/Acquisti/Brandimarte/Loewenstein*, Proceedings of the Ninth Symposium on Usable Privacy and Security 2013, 1; *John/Acquisti/Loewenstein*, 37 Journal of Consumer Research 2011, 858; *Braunstein/Granka/Staddon*, Proceedings of the Seventh Symposium on Usable Privacy and Security 2011, Article 15, 1; *Brandimarte/Acquisti/Loewenstein*, 4 Social Psychological and Personality Science, 2013, 340; *Adjerid/Samat/Acquisti*, 45 The Journal of Legal Studies 2016, S97 (S99 f.).

[89] Grundlegend *Laibson*, 112 Quarterly Journal of Economics 1997, 443.

[90] Siehe nur *Acquisti*, Proceedings of the 5th ACM Conference on Electronic Commerce 2004, 21 (25); *Acquisti/Brandimarte/Loewenstein*, 347 Science 2015, 509 (510); *Hermstrüwer*,

mit β-δ-Diskontierung können daher Verträge eingehen, die sie bei rationaler exponentieller Diskontierung nicht abgeschlossen hätten.

Schließlich spielt auch noch der Sicherheitseffekt (*certainty effect*) eine Rolle:[91] Experimente wie das *Allais*-Paradox zeigen, dass schon die Entscheidung zwischen einer riskanten und einer sicheren Option mit gleichem Erwartungsgewinn typischerweise zugunsten der sicheren Option ausfällt.[92] Bei den hier betrachteten Verträgen steht nun häufig ein sicherer Gewinn mit lediglich probabilistischen Risiken einem sicheren Verlust mit probabilistischen Gewinnen gegenüber. Der Sicherheitseffekt lässt daher die erste Option, mit sicherem Gewinn und lediglich möglichen Verlust, als deutlich attraktiver erscheinen.

Zwar ist unklar, welcher Anteil der Nutzer diesen verhaltensökonomischen Effekten tatsächlich unterliegt. Die genannten empirischen Untersuchungen legen jedoch nahe, dass dies zumindest ein erheblicher Teil derjenigen ist, die Daten als Zahlungsmittel verwenden.[93]

c) Negative Externalitäten durch Kollektiveffekte

Eine weitere, klassische Kategorie von Marktversagen sind negative Externalitäten,[94] also nachteilige Auswirkungen von Verhaltensweisen auf Dritte, deren Kosten die Verursacher nicht vollständig internalisieren. Infolge von zwei gleich noch näher zu beschreibenden Kollektiveffekten kann die Datenpreisgabe durch eine hinreichende Anzahl von Personen durchaus auch negative Folgen für die Privatheit anderer Personen haben, die ihre Daten nicht preisgegeben haben.[95] Dies ist insbesondere deshalb misslich, weil die Preisgabe von persönlich vorteilhaften Daten typischerweise, unabhängig von der Aktion anderer Nutzer, die dominante Strategie ist, auch wenn kollektiv die Zurückhaltung von Informationen besser wäre (Gefangenendilemma).[96]

Durch negative Externalitäten kann es zu einer mittelbaren Beeinträchtigung der Datenschutzgrundrechte Dritter kommen. Zwar ist umstritten, ob

---

Informationelle Selbstgefährdung, 2016, 258 f.; *Acquisti/Taylor/Wagman*, 54 Journal of Economic Literature 2016, 442 (447 f.).

[91] *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 242.

[92] *Allais*, 21 Econometrica 1953, 503; dazu etwa *Hacker*, Verhaltensökonomik und Normativität, 2017, 48 f.

[93] Vgl. *Acquisti/Brandimarte/Loewenstein*, 347 Science 2015, 509 (514).

[94] Zum Begriff *Fritsch/Wein/Ewers*, Marktversagen und Wirtschaftspolitik, 7. Aufl., 2007, 90 ff.

[95] *McCarthy*, 6 I/S: A Journal of Law and Policy 2011, 425 (445 ff.); *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 12; *Ben-Shahar*, 11 Journal of Legal Analysis, 2019, 104 (112 ff.); *Barocas/Levy*, Washington Law Review (im Erscheinen), https://ssrn.com/abstract=3447384, Part II.B. („negative externalities"); siehe auch *Regan*, Legislating Privacy: Technology, Social Values, and Public Policy, 1995, 213; *Nissenbaum*, Privacy in Context: Technology, Policy and the Integrity of Social Life, 2010, 88; siehe auch noch unten zur Re-Identifizierung mithilfe von bekannten Zusatzdaten, Text bei § 4, Fn. 121.

[96] *Fairfield/Engel*, 65 Duke Law Journal 2015, 385 (411 f.); *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 13 f.

einzelne Privatsubjekte selbst an Grundrechte gebunden sind.[97] Nach der neueren Rechtsprechung des EuGH ist es jedoch nicht ausgeschlossen, dass derartige Drittwirkungen auch unter Grundrechtsgesichtspunkten rechtlich relevant sind.[98] Jedenfalls führen sie zu einem präferenzinkonformen Absinken des Schutzes der Privatsphäre bei den genannten Dritten.

aa) Adverse Inferenz

Ein erster Mechanismus, der derartige Kollektiveffekte zeitigt, ist die sogenannte adverse Inferenz:[99] In bestimmten Situationen kann auf private, nicht geoffenbarte Informationen schon allein deshalb korrekt geschlossen werden, weil die betreffende Person die Information *nicht* offenlegt. Dies ist immer dann der Fall, wenn eine Offenlegung bei für den Entscheider positivem Inhalt der privaten Informationen zu erwarten wäre.[100] Ein im Bereich der Kollektiveffekte der Privatheit besonders häufig diskutiertes Phänomen der adversen Inferenz ist das *unraveling*.[101] Voraussetzung ist, dass ein relevantes, personenbezogenes Merkmal zwischen verschiedenen Merkmalsträgern ungleich verteilt ist (zum Beispiel die Ausprägung eines zu versichernden Risikos). Deckt niemand aus der Gruppe der Merkmalsträger dieses Merkmal gegenüber einem Entscheider, für den das Merkmal von Belang ist, auf, so muss der Entscheider alle Merkmalsträger rationalerweise hinsichtlich des Merkmals gleichbehandeln. Er wird also für alle Betroffenen von einem Durchschnittsniveau bezüglich des Merkmals ausgehen. Dies erzeugt jedoch für denjenigen Teil der Gruppe, dessen Merkmal überdurchschnittlich gut ausgeprägt ist, einen signifikanten Anreiz, das Merkmal offenzulegen, um sich so eine bessere Position zu verschaffen. Ist dies einmal erfolgt, muss der Entscheider das Durchschnittsniveau anpassen, da ihm bewusst ist, dass jetzt nur noch solche Merkmalsträger ihr Merkmal nicht aufgedeckt haben, bei denen das Merkmal unter dem initialen Durchschnittsniveau lag. Dadurch entsteht wiederum für all diejenigen Merkmalsträger ein Anreiz zur Aufdeckung, deren Merkmal positiv von dem neuen Durchschnittsniveau abweicht. Dies führt zu einer neuerlichen Anpassung des Durchschnittsniveaus, neuen Anreizen zur Aufdeckung usw., bis nur noch diejenigen Merkmalsträger nicht offengelegt haben, deren Merkmal maximal negativ ist. Bei Unterstellung vollständiger Rationalität aller beteiligten

---

[97] Siehe unten, § 5 C.III.4.a)aa).

[98] Siehe unten, § 5, Fn. 1074.

[99] *Barocas/Levy*, Washington Law Review (im Erscheinen), https://ssrn.com/abstract=3447384, Part II.B.3.

[100] *Barocas/Levy*, Washington Law Review (im Erscheinen), https://ssrn.com/abstract=3447384, Part II.B.3. („were it to be common for the Alices to protect their own privacy").

[101] Dazu *Posner*, in: Newman (Hrsg.), The New Palgrave Dictionary of Economics and the Law, Band 3, 1998, 103 (107); *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 193 ff.; *Peppet*, 105 Northwestern University Law Review 2011, 1153; *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 21 ff.

Parteien kann daher mit Sicherheit geschlossen werden, dass die Merkmale der verbliebenen Merkmalsträger maximal negativ sind, auch wenn sie ihr Merkmal nicht aufgedeckt haben.

Trotz der nicht ganz trivialen Struktur des *unraveling*-Effekts konnte dieser in einer empirischen Studie jedenfalls mit hinreichender Annäherung nachgewiesen werden.[102] Allerdings gibt es neben einer Reihe von anderen Limitationen des *unraveling*-Effekts[103] auch eine datenschutzspezifische Beschränkung, die sich ebenfalls in der Studie zeigte:[104] Der Schluss von der Nicht-Aufdeckung auf das Merkmal ist, selbst bei Unterstellung von vollständiger Rationalität,[105] dann nicht mehr zwingend, wenn das Zurückhalten sowohl darauf zurückzuführen sein kann, dass das verborgene Datum für den Betroffenen negativ ist, als auch darauf, dass er hohe Datenschutzpräferenzen hat und das Merkmal daher, trotz möglicherweise für ihn vorteilhaften Wertes, nicht offenlegt.[106] Insofern ist bei realistischer Annahme von jedenfalls bei einigen Merkmalsträgern hohen Datenschutzpräferenzen grundsätzlich hinsichtlich der Beurteilung der Leistungsfähigkeit von Analysen, die auf *unraveling* gestützt werden, Zurückhaltung geboten. Denn tatsächlich legen empirische Studien nahe, dass ein signifikanter Anteil der Bevölkerung hohe Datenschutzpräferenzen hat.[107] Nichtsdestoweniger ist nicht von der Hand zu weisen, dass jedenfalls tendenziell z. B. die Krankenversicherung für traditionell versicherte Personen teurer werden könnte, wenn sich immer mehr besonders gesunde Menschen freiwillig in Vitalitätstarifen versichern, in denen ihre Gesundheitsparameter digital überwacht werden.[108]

bb) Ähnlichkeitsbasierte Inferenz

Neben der adversen Inferenz gibt es jedoch noch eine zweite Möglichkeit, aus Informationen, die andere Personen preisgeben, auf zurückgehaltene Merkmale zu schließen: die ähnlichkeitsbasierte Inferenz (*similarity-based dependency*[109]), auch Triangulation genannt.[110] Im Rahmen dieses Verfahrens kann der

---

[102] *Benndorf/Kübler/Normann*, 75 European Economic Review 2015, 43 (48 f.).

[103] Dazu *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 193 ff.

[104] *Benndorf/Kübler/Normann*, 75 European Economic Review 2015, 43 (50).

[105] Zu deren Lockerung im Rahmen von *level-k reasoning* ebenfalls *Benndorf/Kübler/Normann*, 75 European Economic Review 2015, 43 (51); ferner *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 24.

[106] Vgl. *Benndorf/Kübler/Normann*, 75 European Economic Review 2015, 43 (50); *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 24.

[107] Siehe unten, § 3, Fn. 163.

[108] Vgl. Sachverständigenrat für Verbraucherfragen, Verbrauchergerechtes Scoring, 2018, 143.

[109] *Barocas/Levy*, Washington Law Review (im Erscheinen), https://ssrn.com/abstract=3447384, Part II.B.; siehe auch *Zarsky*, 56 Maine Law Review 2004, 13 (43 f.); *McCarthy*, 6 I/S: A Journal of Law and Policy 2011, 425 (455); *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 12.

[110] *Fuster et al.*, Predictably Unequal? The Effects of Machine Learning on Credit Markets, Working Paper, 2018, https://ssrn.com/abstract=3072038, 11 f.

zurückgehaltene Zielparameter korrelativ errechnet werden aus anderen Parametern der betreffenden Person, sofern genügend andere Personen diese Parameter und den Zielparameter zur Verfügung stellen.[111] Ein einfaches Beispiel zeigt die Wirkweise: Viele Menschen offenbaren nicht gerne in sozialen Netzwerken, welcher politischen Partei sie zuneigen. Andere wiederum tun dies bereitwillig. Mitglieder beider Gruppen jedoch veröffentlichen, das sei unterstellt, bereitwillig Informationen zu den Autos, die ihnen besonders gefallen. Aus diesen Informationen kann man nun Korrelationen errechnen zwischen Autotypen und politischer Orientierung,[112] die auch auf jene angewandt werden können, die zwar nur ihre Autopräferenzen, nicht jedoch ihre politische Orientierung offenbaren. Dies ist jedoch nur deshalb der Fall, weil andere die Zielvariable, die politische Orientierung, bereitgestellt haben.

Diese Kollektiveffekte sind insbesondere deshalb relevant, weil gerade das Datenschutzrecht von einem Mantra individueller Kontrolle durchzogen ist, das es erschwert, derartige Kollektivdimensionen in der rechtlichen Analyse zu berücksichtigen. Sie zeigen jedoch, dass die Privatsphäre selbst dann leiden kann, wenn Betroffene Informationen sorgsam zurückhalten. Dies gilt es rechtlich einzufangen.

d) Unschärfe des Datenpreissignals

Der vierte hier relevante Typus von Marktversagen besteht in der Unschärfe des Preissignals, wenn Daten als Zahlungsmittel verwendet werden. In der ökonomischen Theorie, gerade auch der rationalitätsbasierten, neoklassischen Theorie der Chicago School, wird der Preis, basierend auf den Überlegungen *Hayeks*,[113] als *das* zentrale Steuerungssignal des Marktes identifiziert.[114] *Stigler* hat Preisdispersion – das gleichzeitige Angebot von homogenen Gütern zu unterschiedlichen Preisen – gar als den entscheidenden Gradmesser für Unkenntnis im Markt angesehen.[115] Voraussetzung für die Propagation von Information durch Preise ist jedoch, dass man den Preis eines konkreten Angebots, inklusive kleiner Abweichungen, jeweils klar und ohne Umschweife erkennen kann, wie *Hayek* eingehend dargelegt hat.[116]

---

[111] *Patka*, 68 Buffalo Law Review 2020, https://ssrn.com/abstract=3435608.

[112] Siehe etwa *Peterson*, Car Owners Select Trump Over Other Candidates, Forbes (19.2.2016), https://www.forbes.com/sites/georgepeterson1/2016/02/19/car-owners-select-trump/.

[113] *Hayek*, 35 American Economic Review 1945, 519 (525–527).

[114] Aus der ökonomischen Literatur repräsentativ *Stigler*, The Theory of Price, 4. Aufl. 1987, 11–16; *Stigler*, 69 Journal of Political Economy 1961, 213 (214 ff.); *Samuelson/Nordhaus*, Economics, 19. Aufl., 2009, 46 ff.; *Varian*, Intermediate Micro-Economics, 8. Aufl., 2010, 3, 78; aus der juristischen Literatur *Böhm*, ORDO 17 (1966), 75 (92 f.); *Grundmann*, in: Grundmann/Micklitz/Renner (Hrsg.), Privatrechtstheorie, Band I, 2015, 968 (972 f.).

[115] *Stigler*, 69 Journal of Political Economy 1961, 213 (214); diese Aussage dürfte sogar unter den Bedingungen von algorithmischer Preisdifferenzierung ihre Gültigkeit behalten.

[116] *Hayek*, 35 American Economic Review 1945, 519 (525–527).

Dies ist zugleich elementare Voraussetzung für das effiziente Funktionieren des Marktmechanismus überhaupt. Nur so können die Kräfte von Nachfrage und Angebot ihre dezentral steuernde Wirkung entfalten.[117] Preise haben dabei zwei unterschiedliche Funktionen:[118] Einerseits registrieren und veröffentlichen sie Informationen über Präferenzen, spezifischer: über das Verhältnis von Angebot und Nachfrage.[119] Andererseits setzen sie Anreize zu einer ressourcenschonenden Produktions- und Konsumtionsentscheidung.[120] Weiß man, dass frische Früchte außerhalb der Saison teurer sind als innerhalb, setzt dies Anreize, saisonal zu konsumieren.

Das Internet verringert Suchkosten für in Geld ausgezeichnete Waren und kann damit einen Beitrag zu geringerer Preisdispersion und geringeren (monetären) Preisen leisten.[121] Zugleich jedoch führen Geschäftsmodelle, die Daten als Gegenleistung verwenden, in die entgegengesetzte Richtung. Der „Datenpreis" wird durch die Menge und Art der im Gegenzug für die Nutzung eines Geräts, eines Dienstes oder einer Applikation erhobenen und verarbeiteten Daten sowie ihre Verarbeitungsform bestimmt.[122] Daten vermitteln im Gegensatz zu monetären Kosten jedoch gerade kein präzises Preissignal:[123] Erstens kann ein intrinsischer Wert von Daten schon aufgrund der Vielfältigkeit der Wertschöpfungsmöglichkeiten nicht angegeben werden.[124] Hinzu kommt, dass der Wert von Daten auf verschiedene Arten gemessen werden kann (z. B. Reservationspreis für die Preisgabe von Daten, *valuation of personal data*, vs. Zahlungsbereitschaft für den Schutz von Daten, *valuation of privacy*), die typischerweise zu unterschiedlichen Ergebnissen führen[125] und hochgradig

---

[117] *Stigler*, The Theory of Price, 4. Aufl. 1987, 12.

[118] Siehe nochmals *Hayek*, 35 American Economic Review 1945, 519 (525–527).

[119] *Stigler*, The Theory of Price, 4. Aufl. 1987, 15.

[120] *Stigler*, The Theory of Price, 4. Aufl. 1987, 15 f.

[121] *Goldfarb/Greenstein/Tucker*, in: Goldfarb/Greenstein/Tucker (Hrsg.), Economic Analysis of the Digital Economy, 2015, 1 (9).

[122] Der „Datenpreis" ist freilich in ökonomischer Hinsicht angesichts von Nicht-Rivalität und beschränkter Knappheit personenbezogener Daten mit einem monetären Preis nur eingeschränkt vergleichbar, siehe *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (275 f.); Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 569 ff. Mit Blick auf die marktliche Steuerungwirkung kann jedoch die Transparenz und Bestimmtheit des monetären Preises mit dem Datenpreis durchaus kontrastiert werden.

[123] *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (276); Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 571.

[124] Siehe dazu oben, § 3 A.II.1.b).

[125] *Acquisti/Taylor/Wagman*, 54 Journal of Economic Literature 2016, 442 (447 f.); *Acquisti/John/Loewenstein*, 42 The Journal of Legal Studies 2013, 249 (264 f.); siehe auch *Grossklags/Acquisti*, Proceedings of the Sixth Workshop on Economics of Information Security 2007, 1 (13 f.); *OECD*, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, 2013, 30; zum *endowment effect* allgemein grundlegend *Kahneman/Knetsch/Thaler*, 98 Journal of Political Economy 1990, 1325; Übersicht bei *Hacker*, Verhaltensökonomik und Normativität, 2017, 96 ff.; *Horowitz/McConnell*, 44 Journal of Environmental Economics and Management 2002, 426.

kontextabhängig sind.[126] Schließlich wird das Datenpreissignal in der Realität nicht auf einer simplen, quantitativen, kardinalen Skala (etwa: x €) angegeben, sondern es muss aus verschiedenen Verarbeitungsvorgängen, die in unterschiedlichen Wertschöpfungsketten Anwendung finden, welche wiederum in den Nutzungsbedingungen und den Richtlinien für Datenschutz und Cookies der einzelnen Verarbeiter typischerweise verstreut angesprochen werden, aufwändig rekonstruiert werden.

Die Unverfügbarkeit eines quantitativen, schnell zu rezipierenden Preissignals setzt den Marktmechanismus nicht vollständig außer Kraft, solange die Höhe des Preises in etwa geschätzt werden kann. Dies gilt etwa für sogenannte Schattenpreise, die nicht unmittelbar quantitativ erfasst werden (z. B. Wert der Hausarbeit, oder der Kindererziehung), die jedoch dennoch gewisse Steuerungseffekte entfalten können.[127] Problematisch ist an der fehlenden Klarheit des Datenpreissignals mithin besonders, dass auch eine Abschätzung des Datenwertes, jedenfalls für Verbraucher, kaum möglich ist. Dies liegt zum einen daran, dass aufgrund rationaler Ignoranz oder Informationsüberlastung bereits die notwendigen Informationen typischerweise nicht vorliegen. Zum anderen verfügen Verbraucher regelmäßig nicht über die ökonomischen Modellierungswerkzeuge, mit denen Wissenschaftler den Wert von personenbezogenen Daten zu approximieren versuchen. Selbst in diesen Analysen offenbart sich, dass sich der Preis für personenbezogene Daten nur mit erheblicher Unschärfe, sowohl in quantitativer als auch in zeitlicher Hinsicht, bestimmen lässt.[128]

Die Folgen dieser Unschärfe für Datenmärkte sind ökonomisch noch nicht abschließend erfasst worden.[129] Es ist jedoch plausibel anzunehmen, dass die Steuerungswirkung von Angebot und Nachfrage jedenfalls dahingehend geschwächt wird, dass derartige Preise erst dann eine Steuerungswirkung entfalten, wenn sie zu absolut unerträglichen, auch für uninformierte Verbraucher offensichtlichen Fehlallokationen führen. Diese Voraussetzung wird jedoch nur selten erfüllt sein. Insgesamt offenbart sich damit ein strukturelles Marktproblem in von Datenpreisen gesteuerten Märkten.[130] Dies wird im dritten Teil der Arbeit Anstoß geben für die Kombination eines Rechts auf eine datenschonende Option mit einem *privacy score*, der die Unschärfe des Datenpreises in marktstützender Weise zumindest reduzieren kann.[131]

---

[126] *John/Acquisti/Loewenstein*, 37 Journal of Consumer Research 2011, 858 (868); *Acquisti/Brandimarte/Loewenstein*, 347 Science 2015, 509 (511).

[127] *Stigler*, The Theory of Price, 4. Aufl. 1987, 14.

[128] *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Perfomance: Contract Law 2.0?, 2020, (im Erscheinen).

[129] Sehr weitgehend insoweit *Schwintowski*, NJOZ 2018, 841 (849 f.), der den betrachteten Märkten die Funktionsfähigkeit vollkommen abspricht.

[130] Ähnlich im Ergebnis *Schwintowski*, NJOZ 2018, 841 (845, 848 f.).

[131] Siehe unten, § 6 C.II.

e) Zusammenfassung zum Marktversagen

Die Analyse der relevanten Marktparameter hat gezeigt, dass Entscheidungen über den Einsatz von Daten als Gegenleistung oder über komplexe Datenverarbeitungsvorgänge, wie sie typischerweise mit der Installation von IoT-Geräten einhergehen, nicht notwendig rational erfolgen müssen. Vielmehr ist zu vermuten, dass es um die materiellen Voraussetzungen für die tatsächliche Inanspruchnahme von Privatautonomie in diesem Kontext deutlich schlechter bestellt ist als in anderen Marktsektoren. Dies beginnt schon damit, dass rationale Ignoranz der Datenverarbeitungsvorgänge eine Informationsasymmetrie zwischen Anbietern und Nutzern hervorruft, welche durch Informationsüberlastung noch verstärkt werden kann. Verhaltensökonomische Effekte können eine Bewertung der Daten verzerren und lassen eine informierte Entscheidung über deren Überlassung im Gegenzug zur Inanspruchnahme von Anbieterleistungen als problematisch erscheinen. Während die Dimension dieser Effekte nicht pauschal abgeschätzt werden kann, sind die negativen Externalitäten der Datenpreisgabe für solche Akteure, die ihre Daten nicht offenlegen, relativ klar zu benennen. Durch zwei unterschiedliche Mechanismen, adverse und ähnlichkeitsbasierte Inferenz, kann zunehmend auch auf bewusst zurückgehaltene Merkmale geschlossen werden. Schließlich führt die Unschärfe des Datenpreissignals dazu, dass der in der ökonomischen Theorie zentrale Parameter für die Steuerung der Kräfte von Angebot und Nachfrage, der Preis, seine Wirkung nur unzureichend entfalten kann.

Dabei zeigt sich, dass die genannten Effekte nicht nur solche Akteure treffen, die besonders beschränkt rational agieren. Informationsasymmetrie infolge rationaler Ignoranz, Externalitäten entgegen der eigenen Datenschutzpräferenz und Schwierigkeiten bei der Bestimmung des Datenpreises lassen gerade auch die Möglichkeiten rationaler Akteure, eine informierte und präferenzkonforme Wahl zu treffen, als limitiert erscheinen. Damit ist freilich nicht gesagt, dass eine rationale Entscheidung nicht möglich wäre; gerade auch die zitierten empirischen Untersuchungen legen jedoch nahe, dass damit gerechnet werden muss, dass dies zu einem erheblichen Anteil nicht der Fall ist. Daher stellen die empirischen Ökonomen *Acquisti*, *Taylor* und *Wagman* in Auswertung einer Vielzahl von Studien fest: „issues associated with individuals' awareness of privacy challenges, solutions, and trade-offs cast doubts over the ability of market outcomes to accurately capture and reveal, by themselves, individuals' true privacy valuations."[132]

2. Soziale Risiken

Die *privacy*-Forschung hat in den letzten Jahren neben den soeben diskutierten ökonomischen Problemlagen auch die soziale Dimension von Privatheit und

[132] *Acquisti/Taylor/Wagman*, 54 Journal of Economic Literature 2016, 442 (448).

Datenschutz zunehmend betont.[133] Dies weist darauf hin, dass Datenschutzrisiken eine soziale Komponente haben, die sich besonders infolge von Vernetzung und Datenweitergabe entfalten kann. *Klement* hat in diesem Kontext treffend von einem *öffentlichen* Interesse an Privatheit gesprochen.[134]

a) Verhaltens- und Freiheitsverengung (*chilling effects*)

Der siebte Erwägungsgrund der DS-GVO beschreibt in seinem zweiten Satz markant eines der zentralen Ziele des Datenschutzrechts: „Natürliche Personen sollten die Kontrolle über ihre eigenen Daten besitzen." Zugleich jedoch deuten eine Reihe von empirischen Erhebungen darauf hin, dass die große Mehrheit der Betroffenen die Datenverarbeitung im Rahmen von Onlineaktivitäten als Sphäre eines signifikanten Kontrollverlusts erlebt.[135] Dies kann nicht zuletzt auf die bereits diskutierten Kollektiveffekte der Offenlegung von Information zurückgeführt werden.[136] Damit einher geht ein Schwund einer klar definierbaren Privatsphäre,[137] was wiederum konkrete Auswirkungen auf die

[133] Umfassend die Beiträge in *Roessler/Mokrosinska* (Hrsg.), Social Dimensions of Privacy: Interdisciplinary Perspectives, 2015; grundlegend *Regan*, Legislating Privacy: Technology, Social Values, and Public Policy, 1995, 212 ff.; siehe ferner *Solove*, 44 San Diego Law Review 2007, 745 (760 ff.); *Cockfeld*, 40 University of British Colombia Law Review 2007, 41; *Solove*, Understanding Privacy, 2008, 89 ff.; *Steeves*, in: Kerr et al. (Hrsg.), Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society, 2009, 191; *Nissenbaum*, Privacy in Context: Technology, Policy and the Integrity of Social Life, 2010, 85 ff.; *Solove*, 126 Harvard Law Review 2013, 1880 (1892 f.); *Willis*, 29 Berkeley Technology Law Journal 2014, 61 (133); *Fairfield/Engel*, 65 Duke Law Journal 2015, 385; *Barocas/Levy*, Washington Law Review (im Erscheinen), https://ssrn.com/abstract=3447384, Part I. („Prior research has explored privacy's socially interdependent nature"); aus dem älteren Schrifttum *P. Schwartz* 52 Vanderbilt Law Review 1999, 1609 (1647 ff.); *Post*, 77 California Law Review 1989, 957; *Simitis*, 135 University of Pennsylvania Law Review 1989, 707 (709); *Gavison*, 89 Yale Law Journal 1980, 421 (450 f., 455).

[134] *Klement*, JZ 2017, 161 (169 f.); siehe auch *Regan*, Legislating Privacy: Technology, Social Values, and Public Policy, 1995, 213, 225 (public value of privacy); *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 363 ff.; *Eichenhofer*, Der Staat 55 (2016), 41 (43 f.).

[135] *Pew Research Center*, Public Perceptions of Privacy and Security in the Post-Snowden Era, 2014, 3: Danach beklage 91 % der US-amerikanischen Erwachsenen einen Kontrollverlust hinsichtlich der Erhebung und Verarbeitung von Daten durch online tätige Unternehmen; *European Commission*, Attitudes on Data Protection and Electronic Identity in the European Union, Special Eurobarometer 359, 2011, 74–75 und 148–149: 54 % der Europäer fühlen sich unwohl mit Online-Profiling und 74 % legen Wert darauf, dass eine Einwilligung zwingende Voraussetzung für Datenverarbeitung ist; *DIVSI*, Daten – Ware und Währung, 2014, 12: 78 % der Befragten (deutsche Internetnutzer) glauben, gar keinen oder wenig Einfluss auf die Verwendung der online erhobenen Daten zu haben; 80 % der Befragten (deutsche Internetnutzer) lehnen es ab, dass mit bei „kostenlosen" Angeboten die Daten der Nutzer „zu Geld gemacht werden"; 51 % befürchten Datenmissbrauch und 50 % wissen nicht, wofür ihre Daten verwendet werden; ferner *Rothmann/Buchner*, DuD 2018, 342 (345): im Schnitt sind 75 % der Nutzer mit der Datenverarbeitung durch Facebook nicht einverstanden; Diskussion auch bei *Buchner*, WRP 2019, 1243 (1246 f.).

[136] Siehe oben, § 3 B.II.1.c).

[137] *Hoofnagle/Kesari/Perzanowski*, 87 George Washington Law Review 2019, 783 (822).

Verhaltensfreiheit hat. Das Bundesverfassungsgericht hat unmissverständlich klargestellt, dass der Kern des Rechts auf informationelle Selbstbestimmung gerade im Schutz der Verhaltensfreiheit liegt.[138]

Dabei sind Rückwirkungen auf das Verhalten von Akteuren, über die personenbezogene Daten gesammelt werden, schon deshalb nicht ausgeschlossen, weil stets ein Restrisiko dahingehend verbleibt, dass die Daten – in legaler oder illegaler Weise – in neuen, bedeutsameren Verwendungskontexten genutzt werden. So ist die Verwendung von Daten aus sozialen Netzwerken oder aus IoT-Geräten zu Zwecken der Überprüfung der Kreditwürdigkeit[139] oder der Berechnung eines Versicherungstarifs[140] bislang weitestgehend freiwillig. Allerdings lässt sich in Anbetracht der ungewissen Entwicklung der künftigen Rechts- und Sachlage nicht ausschließen, dass die Analyse von Daten, deren Erhebungskontext zunächst vergleichsweise harmlos erscheint, dereinst auch zur rechtlichen oder faktischen Voraussetzung (*unraveling*) des Abschlusses bedeutsamer oder gar existenzieller Rechtsgeschäfte erhoben wird. Über die genaue Höhe dieses Risikos mag man unter den gegenwärtigen Umständen in westlichen Gesellschaften geteilter Meinung sein. Zweifellos ist dieses Risiko jedoch größer als null und nach Einschätzung verschiedener Experten durchaus signifikant.[141] In der Konsequenz können die soziale Interaktion, der politische Diskurs und auch die Wahrnehmung von Rechten durch die Unsicherheit hinsichtlich der künftigen Verwendung über das Individuum gesammelter Daten Schaden erleiden.[142] Verwertungsrisiken werden damit zu Freiheitsrisiken.

Empirische Untersuchungen stützen diese Einschätzung: Das Gefühl, bei bestimmten Tätigkeiten beobachtet zu werden, kann zum Unterlassen spezifi-

---

[138] BVerfG NJW 1984, 419 (422) – Volkszählung; BVerfG NJW 2007, 2464 Rn. 87 – Kontostammdaten; BVerfG NJW 2008, 822 Rn. 198 – Online-Durchsuchung; siehe auch *Schantz*, in: BeckOK DatenschutzR, 26. Ed. 1.2.2017, Art. 1 DS-GVO Rn. 5.1; *Klement*, JZ 2017, 161 (162).

[139] Siehe etwa https://www.kreditech.com/solutions; https://www.zest.ai/solutions; ferner *Christl/Kopp/Riechert*, Corporate Surveillance in Everyday Life, 30 f.

[140] Siehe oben, § 3, Fn. 34 f. sowie Sachverständigenrat für Verbraucherfragen, Verbrauchergerechtes Scoring, 2018, 76 ff.; *Fisher*, Social media intelligence and profiling in the insurance industry, Medium (24.4.2017), https://medium.com/privacy-international/social-media-intelligence-and-profiling-in-the-insurance-industry-4958fd11f86f; *Reuters*, Facebook stymies Admiral's plans to use social media data to price insurance premiums (2.11.2016), https://www.Reuters.com/article/us-insurance-admiral-facebook/facebook-stymies-admirals-plans-to-use-social-media-data-to-price-insurance-premiums-idUSKBN12X1WP.

[141] *Mayer-Schönberger*, delete, 2009, 10 f., 102 ff.; *Acquisti/Brandimarte/Loewenstein*, 347 Science 2015, 509 (512, 514); *Acquisti/Taylor/Wagman*, 54 Journal of Economic Literature 2016, 442 (471); *Christl/Spiekermann*, Networks of Control, 2016, 78 ff. („customer lifetime risk"); Sachverständigenrat für Verbraucherfragen, Verbrauchergerechtes Scoring, 2018, 61 ff.; *Kummer/Schulte* 65 Management Science 2019, 3470 (3470); mit (teilweise polemischer) Zuspitzung *Zuboff*, The Age of Surveillance Capitalism, 2019, vor allem Kapitel 13.

[142] Vgl. *Regan*, Legislating Privacy: Technology, Social Values, and Public Policy, 1995, 225 f.; *Gavison*, 89 Yale Law Journal 1980, 421 (450 f.).

scher Tätigkeiten führen (*chilling effects*).[143] Dies ist nicht nur relevant im Kontext von staatlicher Überwachung,[144] sondern auch bei Profiling durch private Akteure.[145] Daher ist es beispielsweise bedenklich, wenn von IBM und anderen Unternehmen Millionen von Online-Fotos ohne Einwilligung abgegriffen werden, um ML-basierte Gesichtserkennungsmodelle zu optimieren;[146] oder wenn vernetztes Spielzeug Informationen über Kinder und ihre Umgebung ohne Einwilligung der Eltern sammelt.[147]

Ein Eingriff in die Privatsphäre ist schließlich auch zu gewärtigen, wenn personenbezogene Daten gehackt oder durch den an sich legitimierten Verantwortlichen zu illegitimen Zwecken missbraucht werden. Das dahingehende Risiko steigt mit der Menge der bereitgehaltenen Daten typischerweise an, da größere Datenmengen für Angreifer attraktiver sind. Diese Gefahren sieht auch die DS-GVO, die im 75. Erwägungsgrund ausdrücklich „Identitätsdiebstahl oder -betrug" sowie Risiken des „Verlust[s] der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten" und „der unbefugten Aufhebung der Pseudonymisierung" benennt.

b) Unentziehbarkeit

Ein weiteres Problem stellt sich durch die im Zuge der Ausweitung des IoT immer lückenlosere Abdeckung des öffentlichen Raums mit datenverarbeitenden Sensoren. In einer Smart City ist es einzelnen Individuen kaum mehr möglich, sich der Datenerfassung zu entziehen.[148] Privaträume werden zur Ausnah-

[143] Überblick bei *Büchi/Fosch Villaronga/Lutz/Tamò-Larrieux/Velidi/Viljoen*, Chilling Effects of Profiling Activities: Mapping the Issues, Working Paper, 2019, https://ssrn.com/abstract=3379275, 7 ff.

[144] Siehe dazu die empirischen Studien von *Penney*, 6(2) Internet Policy Review 2017, 1; *Stoycheff/Liu/Xu/Wibowo*, 21 New Media & Society 2018, 602.

[145] Es existieren kaum empirische Studien, die den Effekt von korporativer Überwachung isolieren, siehe *Büchi/Fosch Villaronga/Lutz/Tamò-Larrieux/Velidi/Viljoen*, Chilling Effects of Profiling Activities: Mapping the Issues, Working Paper, 2019, https://ssrn.com/abstract=3379275, 13; siehe aber *Hermstrüwer/Dickert*, 51 International Review of Law and Economics 2017, 38 (40), die als Veröffentlichungsinstrument, mithin als potenzielles Überwachungsobjekt, eine Google Website wählen und *chilling effects* messen können.

[146] *NBC News*, Facial Recognition's ‚Dirty Little Secret': Millions of Online Photos Scraped Without Consent, Communications of the ACM (15.3.2019), https://cacm.acm.org/news/235455-facial-recognitions-dirty-little-secret-millions-of-online-photos-scraped-without-consent/fulltext; *Hill*, The Secretive Company That Might End Privacy as We Know It, New York Times (18.1.2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[147] *Federal Trade Commission*, Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act, Presseerklärung (8.1.2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.

[148] Siehe etwa *Draper*, Madison Square Garden Has Used Face-Scanning Technology on Customers, New York Times (13.3.2018), https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html; *Hill*, The Secretive Company That Might End Privacy as We Know It, New York Times (18.1.2020), https://www.nytimes.

me.[149] Die Engmaschigkeit der Vernetzungsstruktur, die einerseits die oben geschilderten Vorteile verspricht, wird damit für all jene zum Stein des Anstoßes, die sich Freiräume abseits einer großflächigen Datenverarbeitung erhalten wollen.[150] Wo Rückzugsräume fehlen, stößt auch die Entfaltung der Persönlichkeit an Grenzen.[151] Diese ist jedoch Voraussetzung einer freiheitlichen Gesellschaft.[152] So sind die individuelle und die soziale Dimension der Privatheit untrennbar verzahnt.[153]

c) Mangelndes Bewusstsein der Datenerhebung

Unentziehbarkeit kann, jedenfalls bei einem Teil der Betroffenen, einhergehen mit einem mangelnden Bewusstsein dafür, dass überhaupt Daten erhoben werden. Während mittlerweile der ganz überwiegende Teil der Bevölkerung weiß, dass im Rahmen von Onlineaktivitäten typischerweise durch Webseiten und Apps jedenfalls grundsätzlich Daten gesammelt werden,[154] spitzt sich das Problem bei der Verwendung von IoT-Geräten zu.[155] Diese lassen sich von außen teilweise nicht oder nur schwer von herkömmlichen, nicht vernetzten Geräten unterscheiden. Die im Jahr 2017 von Amazon eingeführte Uhr „Echo Spot" zum Beispiel sieht von außen wie ein Radiowecker aus, hat jedoch zusätzlich eine für Unbeteiligte kaum erkennbare Kamera integriert, die intelligente Vernetzung ermöglichen soll.[156]

Die Eigentümer der jeweiligen Geräte mögen ein grundsätzliches Bewusstsein für deren Datensammlungsaktivitäten haben. Dieses wird jedoch Dritten, die mit den Geräten in Berührung kommen, häufig abgehen. Besonders markant ist der Mangel an Bewusstsein für Datensammlung bei IoT-Geräten für Kinder.[157] Selbst bei erwachsenen Eigentümern dürfte sich dieses Bewusstsein

---

com/2020/01/18/technology/clearview-privacy-facial-recognition.html; *Cobbe/Morison*, in: Slautsky (Hrsg.), The Conclusions of the Chaire Mutations de l'Action Publique et du Droit Public, 2019.

149 *Rosner/Kenneally*, Clearly Opaque. Privacy Risks of the Internet of Things, Bericht, 2018, 62.

150 *Brookman/Hans*, Why Collection Matters: Surveillance as a De Facto Harm, Center for Democracy and Technology, 2013, 4 f.

151 *Solove*, 44 San Diego Law Review 2007, 745 (762).

152 *Regan*, Legislating Privacy: Technology, Social Values, and Public Policy, 1995, 221.

153 *Gavison*, 89 Yale Law Journal 1980, 421 (455).

154 *DIVSI*, Daten – Ware und Währung, 2014, 11; siehe aber auch, zu Kenntnislücken hinsichtlich des Umfangs der Datenerhebung, *Rothmann/Buchner*, DuD 2018, 342 (345).

155 *Office of the Privacy Commissioner of Canada*, The Internet of Things, Research Paper, 2016, 20, 23; *Rosner/Kenneally*, Clearly Opaque. Privacy Risks of the Internet of Things, Bericht, 2018, 55 f.

156 *DPA*, So schlägt sich der smarte Radio-Wecker von Amazon, t-online.de (8.2.2018), https://www.t-online.de/digital/id_83196654/amazon-echo-spot-im-test-eine-kamera-im-schlafzimmer-.html.

157 Vgl. *Jones/Meurer*, 2016 IEEE International Symposium on Ethics in Engineering, Science and Technology (ETHICS), 2016, 1.

jedoch über die Zeit abschwächen.[158] Wer aber nicht weiß, dass Daten gesammelt werden, kann auch keine adäquaten Vorkehrungen für einen souveränen, selbstbestimmten Umgang mit diesen Daten treffen.

d) Diskriminierung

Schließlich ist nicht zu verkennen, dass Kenntnisse über personenbezogene Daten zu Diskriminierung führen können. Dies erkennt der 75. Erwägungsgrund der DS-GVO ausdrücklich an. Das Diskriminierungspotenzial von Datenverarbeitungsvorgängen, besonders im Bereich der Verarbeitung mittels Techniken maschinellen Lernens, ist nicht nur theoretisch[159] und empirisch[160] gut belegt, sondern hat auch eine breite rechtswissenschaftliche Literatur hervorgebracht.[161] Auch hier ist nicht zu verkennen, dass der Schutz vor Diskriminierung nicht nur dem Individuum selbst, sondern auch der Gewährleistung der Voraussetzungen für eine freie, demokratische Gesellschaft dient.[162]

---

[158] *Rosner/Kenneally*, Clearly Opaque. Privacy Risks of the Internet of Things, Bericht, 2018, 60, 90 f.; vgl. auch *Reidenberg*, 69 University of Miami Law Review 2014, 141 (149).

[159] *Calders/Žliobaitė*, in: Custers et al. (Hrsg.), Discrimination and Privacy in the Information Society, 2013, 43; *Romei/Ruggieri*, 29 The Knowledge Engineering Review 2014, 582; *Žliobaitė*, 31 Data Mining and Knowledge Discovery 2017, 1060.

[160] *Obermeyer et al.*, 366 Science 2019, 447; *Berk et al.*, Sociological Methods & Research 2018, Article 0049124118782533, 1; *Kleinberg/Mullainathan/Raghavan*, 8th Innovations in Theoretical Computer Science Conference (ITCS 2017) 2017, Article 43, 1; *Holl/Kernbeiß/Wagner-Pinter*, Das AMS-Arbeitsmarktchancen-Modell. Dokumentation zur Methode, 2018, 11; *Sweeney*, 56(5) Communications of the ACM 2013, 44; siehe auch *Reuters*, Amazon ditched AI recruiting tool that favored men for technical jobs, The Guardian (11.10.2018), https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine.

[161] Siehe repräsentativ *Barocas/Selbst*, 104 California Law Review 2016, 671; *Grimmelmann/Westreich*, 7 California Law Review Online 2016, 164; *Kim*, 58 William & Mary Law Review 2016, 857; *Selbst*, 52 Georgia Law Review 2017, 109; *Hacker*, 55 Common Market Law Review 2018, 1143; *Gillis/Spiess*, 86 University of Chicago Law Review 2019, 459; *Zehlike/Hacker/Wiedemann*, 34 Data Mining and Knowledge Discovery 2020, 163; *Wachter/Mittelstadt/Russell*, Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI, Working Paper, 2020, https://ssrn.com/abstract=3547922; *Zuiderveen Borgesius*, Strengthening legal protection against discrimination by algorithms and artificial intelligence, The International Journal of Human Rights 2020, DOI: 10.1080/13642987.2020.1743976.

[162] Vgl. *Rawls*, A Theory of Justice, 1999, 17 f.

C. Dritte rechtliche Herausforderung: Ermöglichung der Durchsetzung heterogener Datenschutzpräferenzen

Die ökonomischen, zum Teil aber auch die sozialen Risiken der Datenverarbeitung würden deutlich abgemildert, wenn die Betroffenen homogen niedrige Datenschutzpräferenzen hätten. Die Informationsasymmetrie würde einen irrelevanten Punkt betreffen, Externalitäten durch Kollektiveffekte fielen in ihrer Tragweite geringer aus, die Verhaltenseffekte des Kontrollverlusts und des Überwachungsgefühls wären eingeschränkt und die Unentziehbarkeit in stark vernetzten Umgebungen würde von allen Beteiligten akzeptiert.

Empirische Untersuchungen weisen jedoch darauf hin, dass Datenschutzpräferenzen stark heterogen und dabei nicht normal-, sondern eher U-förmig verteilt sind: Die meisten Personen haben entweder sehr geringe oder sehr ausgeprägte Präferenzen für Datenschutz, einige weitere nehmen eine mittlere Position ein.[163] In einer weiteren, groß angelegten Studie (n > 2000) legten knapp 12 % der Teilnehmer generell und weitere 18 % selektiv stark ausgeprägte Datenschutzpräferenzen an den Tag, 23 % gering ausgeprägte.[164] Diese Trennung der Regelungsadressaten in (mindestens) zwei Gruppen mit hohen und niedrigen Datenschutzpräferenzen verschärft das regulatorische Problem markant:[165] Lösungen, die für eine Gruppe zufriedenstellend ausfallen, sind typischerweise für die andere Gruppe inakzeptabel, und andersherum. Letztlich muss es daher darum gehen, effektive Möglichkeiten der (Selbst- oder Fremd-) Selektionierung bereitzustellen, sodass für die jeweiligen Gruppen praktikable und akzeptable Alternativen des Umgangs mit Daten geboten werden.

An dieser Stelle kommen regulatorisches und ermöglichendes Privatrecht zusammen.[166] Einerseits soll die Durchsetzung heterogener Datenschutzprä-

[163] *Acquisti/John/Loewenstein*, What is Privacy Worth?, Working Paper, 2009, http://pages.stern.nyu.edu/~bakos/wise/papers/wise2009-6a1_paper.pdf, 26; frühere Studien zum Westin Privacy Index, mit der Differenzierung zwischen *privacy fundamentalists* (ca. 26 %), privacy unconcerned (ca. 10 %) und privacy pramgatists (ca. 64 %), bei *Kumaraguru/Cranor*, Privacy Indexes: A Survey of Westin's Studies, Working Paper, Institute for Software Research International, School of Computer Science, Carnegie Mellon University, 2005, 16 ff. (mit methodischer Kritik); zum Westin Privacy Index auch *Hermstrüwer/Dickert*, 51 International Review of Law and Economics 2017, 38 (44); *Knijnenburg/Kobsa*, Proceedings of the 2013 ACM International Conference on Intelligent User Interfaces, 407 (408); zur Heterogenität von Datenschutzpräferenzen allgemein *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 353 f.; *Lin et al.*, 10th Symposium on Usable Privacy and Security (SOUPS) 2014, 199 (204 ff.); *Staiano et al.*, Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing 2014, 583 (592); *Jentzsch et al.*, Study on Monetising Privacy: An Economic Model for Pricing Personal Information, European Network and Information Security Agency, 2012, 36; *Grossklags/Acquisti*, Proceedings of the Sixth Workshop on Economics of Information Security 2007, 1 (14 f.); ferner unten, § 6 C.II.2.a)aa).

[164] *Lin et al.*, 10th Symposium on Usable Privacy and Security (SOUPS) 2014, 199 (205 f.).

[165] *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 353 f.

[166] Siehe zu den diesbezüglichen Begrifflichkeiten bereits oben, § 1, Fn. 61.

ferenzen ermöglicht werden. Dies bedingt, dass die effektive Wahrnehmung materieller Privatautonomie ebenso gewährleistet ist wie hinreichende Wahlfreiheit unter verschieden dateninvasiven Angeboten am Markt. Andererseits lassen sich diese Bedingungen jedoch in weiten Bereichen der digitalen Wirtschaft, wie insbesondere die Analyse des sechsten Kapitels zeigen wird, nicht ohne regulatorische Eingriffe in die Marktstruktur selbst herstellen. Damit ist die dritte rechtliche Herausforderung angesprochen, die zugleich eine zentrale Forschungsfrage der weiteren Teile dieser Arbeit darstellt.

D. Leitfälle und Leitfragen für die weiteren Teile der Arbeit

Aus der Analyse des vorangegangenen Teils ergeben sich besondere Risiken des Kontrollverlusts und eines Defizits der Voraussetzungen für die tatsächliche und effektive Ausübung von Privatautonomie. Im Folgenden werden drei kurze Leitfälle entwickelt, welche diese Probleme konkret fassbar machen und die rechtliche Analyse des zweiten Teils dieser Arbeit prägen werden (I.). Daran schließen sich zwei Leitfragen für die weiteren Teile der Arbeit an (II.).

I. Drei paradigmatische Leitfälle

Gemeinsam ist den drei Leitfällen, dass – als Ausdruck der ersten oben beschriebenen rechtlichen Herausforderung – typischerweise ein Drittbezug vorliegt, der über das konkrete Vertrags- oder Nutzungsverhältnis hinausweist. Dieser Drittbezug entspricht dem Vernetzungscharakter der Datenerhebung und -analyse, der Gegenstand des vorangegangenen Abschnitts war.

1. Datenweiterleitung an Drittunternehmen

Eine erhebliche Anzahl von großen Internetunternehmen leiten personenbezogene Daten an Drittunternehmen weiter (in der Terminologie von Art. 4 Nr. 2 DS-GVO: Übermittlung).[167] Dies ergab eine im Jahr 2017 durchgeführte Analyse der Datenschutzerklärungen führender Unternehmen.[168] Bis auf

[167] Unter Weiterleitung wird in dieser Arbeit die gezielte Weitergabe von Daten an einen anderen Empfänger als die betroffene Person bzw. an einen abgegrenzten Empfängerkreis verstanden. Damit deckt sich der Begriff mit jenem der Übermittlung in Art. 4 Nr. 2 DS-GVO, siehe etwa *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 2 DS-GVO Rn. 26; vgl. ferner *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, 2014, 412.

[168] *Bischhoff*, Comparing the privacy policy of internet giants side-by-side, comparitech (20.3.2017), https://www.comparitech.com/blog/vpn-privacy/we-compared-the-privacy-policies-of-internet-giants-side-by-side/. Untersucht wurden Google, Apple, Microsoft, Facebook, Reddit, Twitter, LinkedIn, Instagram, WhatsApp, Snapchat, Amazon, eBay, Netflix und Hulu.

WhatsApp und Reddit ermöglichten alle untersuchten Unternehmen es Drittunternehmen, Werbung zu schalten (*third-party advertisements*). Dies geht typischerweise mit der Mitteilung von Informationen über die Zielperson einher, da für derart personalisierte Werbung ein Entgelt von dem werbenden Unternehmen verlangt werden kann, das ein Vielfaches über dem Entgelt bei nicht personalisierter Werbung liegt.[169] Google, Facebook, LinkedIn, Snapchat und eBay teilten darüber hinaus auch persönliche Informationen der Nutzer mit Drittunternehmen. Da viele Datenteilungspraktiken gerade nicht offen in Datenschutzerklärungen erläutert werden, dürfte die Dunkelziffer noch deutlich höher liegen. Das Drittunternehmen kann dabei mit dem erhebenden Unternehmen in einer Konzernstruktur verbunden sein oder auch nicht. Prominentestes Beispiel für erstere Kategorie ist die Datenweitergabe zwischen den zu Facebook gehörenden Unternehmen (Facebook selbst, Instagram, WhatsApp, Oculus und Masquerade).[170] Die Personalisierung der Werbeansprache basiert dabei in jedem Fall auf einem sogenannten Werbescoring (auch: Werbeselektion), bei dem die vorhandenen Kundendaten für werbliche Zwecke aufbereitet und die betroffene Person einer oder mehreren Werbekategorien zugeordnet wird.[171] Je kleiner die Kategorien werden, desto stärker wird der Personalisierungsgrad der Werbung.

Gerade auch in IoT-Kontexten werden Daten typischerweise mit Drittunternehmen geteilt.[172] Dies kann einerseits der effizienten Aufteilung der verschiedenen technischen Schichten des IoT (Wahrnehmung; Netzwerk; Verarbeitung; Dienstleistung)[173] zwischen verschiedenen Unternehmen (z. B. Geräteproduzent, Cloud-Serviceanbieter),[174] andererseits aber auch nicht technisch-funktional begründeten Zwecken wie der Werbung dienen.[175]

Ziel nicht funktional bedingter Weiterleitung von personenbezogenen Daten an Drittunternehmen ist typischerweise die Ermöglichung von personalisierter Werbung oder weiteren Analyseverfahren. Dabei ist jedoch immer die Möglichkeit mitzudenken, dass die Datenweiterleitung tatsächlich lediglich für

---

169 *Hacker/Petkova*, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1 (23).

170 Bundeskartellamt, Fallbericht v. 15.2.2019, Az. B6–22/16 (*Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung*), 3.

171 *Tavanti*, RDV 2016, 295 (303); *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Anhang 3 zu Artikel 6: Datenverarbeitung für Zwecke der Werbung Rn. 7; *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 76.

172 *Ziegler et al.*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 9 (32).

173 Siehe dazu oben, § 2 C.II.

174 *Bolognini/Balboni*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 71 (71 f.).

175 *Deschamps-Sonsino*, in: DZone, DZone's 2019 Guide to Internet of Things, 2019, 12 (13); *Bolognini/Balboni*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 71 (78); *Article 29 Data Protection Working Party*, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240, 2016, 11; *Weidert/Klar*, BB 2017, 1858 (1863).

die Funktionalität des Produkts technisch erforderlich ist, z. B. weil die durch ein IoT-Produkt generierte Datenmenge innerhalb des Heimnetzwerks technisch nicht verarbeitet werden kann und daher an eine Cloud-Dienstleistung ausgelagert werden muss. Im Folgenden werden die spezifischen Probleme des Cloud Computing im Dienste der thematischen Zuspitzung jedoch weitgehend ausgeblendet.[176] Der erste Leitfall, der im Folgenden immer wieder thematisiert werden wird, ist daher die Datenweiterleitung an Drittunternehmen zu Zwecken personalisierter Werbung.

2. *Datenerhebung durch Drittanbieter (*third-party tracking*)*

Wie das zweite Kapitel dieser Arbeit bereits im Einzelnen gezeigt hat,[177] kann man zwischen Instrumenten des *first-party tracking* und des *third-party tracking* unterscheiden.[178] Während bei ersterem ein primäres Nutzungsverhältnis zwischen dem Anbieter des Tracking-Tools und dem Nutzer besteht, erheben Tracking-Instrumente beim *third-party tracking* direkt Daten für eine dritte Partei, mit der ein solches Nutzungsverhältnis gerade nicht besteht. Paradigmatisch für diese Form der Datenerhebung durch Drittanbieter sind Social Plug-Ins.[179] So sammelt etwa Facebook über Drittanbietercookies, die durch den in andere Webseiten eingebunden Like Button gesetzt werden, Daten über die Nutzer dieser Webseiten, auch wenn diese mit dem Like Button gar nicht interagieren.[180]

Ganz grundsätzlich erfolgt Datensammlung durch Drittunternehmen über verschiedene Tracking-Technologien,[181] vor allem aber, so auch bei Social Plug-Ins,[182] über Drittanbietercookies.[183] Dies sind, wie gesehen, kleine Textdateien, die ein Drittunternehmen, das nicht selbst die besuchte Webseite betreibt, auf dem Computer der Webseitenbesucher installiert und die für dieses Drittunternehmen Daten erheben.[184] Derartige Tracking-Technologien über Coo-

[176] Dazu aber *Artikel-29-Datenschutzgruppe*, Stellungnahme 05/2012 zum Cloud Computing, WP 196, 2012; *Bolognini/Balboni*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 71 (74 ff.). Die Hauptrisiken bestehen hier in mangelnder Kontrolle der Betroffenen über die Daten und in unzureichender Information über die Verarbeitungsvorgänge.

[177] Siehe oben, § 2 A.

[178] Siehe etwa *Mellet/Beauvisage*, Consumption Markets & Culture 2019, 1 (8).

[179] Siehe genauer oben, Text bei § 2, Fn. 13 ff.

[180] *Data Protection Commissioner*, Facebook Ireland Ltd, Report of Audit v. 21.12.2011, 52; *Acar et al.*, Facebook Tracking Through Social Plug-ins, Technical report prepared for the Belgian Privacy Commission, 2015, 5 ff.; Bundeskartellamt, Fallbericht v. 15.2.2019, Az. B6–22/16 (*Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung*), 3 f.

[181] Darunter fallen auch Tracking Pixel (§ 2, Fn. 12) und *bluetooth beacons* (§ 2, Fn. 25).

[182] *Schleipfer*, DuD 2014, 318 (319, 321).

[183] Siehe dazu *Steidle/Pordesch*, DuD 2008, 324 (325); *Clifford*, 5 JIPITEC 2014, 194 (195); siehe auch GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 40.

[184] *European Commission*, Cookies, in: The EU Internet Handbook, http://ec.europa.

kies ermöglichen dem Betreiber des Tracking-Tools eine webseitenübergreifende Beobachtung des Nutzerverhaltens,[185] werden jedoch vom Nutzer in den meisten Fällen nicht oder kaum wahrgenommen. Gleiches gilt für das technisch komplexere *fingerprinting*[186] sowie für die eindeutigen Geräteidentifizierungs-IDs (*unique strings*), die anstelle von oder zusätzlich zu Cookies bei Smartphones zum Einsatz kommen.[187] Damit eignet der Datenerhebung durch Drittanbieter nicht nur eine besonders extensive Dimension, sondern auch eine besondere Überraschungskomponente, die wiederum die informierte Ausübung von Privatautonomie durch Nutzer problematisch erscheinen lässt. Datenerhebung über Social Plug-Ins und andere Tracking-Tools von Drittanbietern bildet daher den zweiten Leitfall.

3. Datenerhebung bei Dritten

Eine dritte Fallkategorie zeichnet sich durch die Datenerhebung bei Dritten aus. Sie ist insbesondere für das Internet der Dinge relevant. Grundsätzlich erfolgt die Datenerhebung größtenteils innerhalb des primär relevanten Nutzungsverhältnisses, erfasst jedoch auch Daten von Personen, mit denen dieses Nutzungsverhältnis nicht besteht. Beispielsweise können durch IoT-Geräte Daten von Nicht-Eigentümern erhoben werden. Wenn etwa in einem vernetzten Fahrzeug die Sprache und Bewegungen von Passagieren überwacht werden, so können Mitfahrer erfasst werden, die selbst zunächst in keinem Vertragsverhältnis zu dem Hersteller des Fahrzeugs oder den Anbietern der digitalen Dienste stehen. Zum Beispiel kann der Fahrer den Mitfahrer bitten, dem vernetzten und (partiell) autonomen Fahrzeug mitzuteilen, an welches Ziel das Fahrzeug die Insassen befördern soll. Besonders klar ist die Abwesenheit einer vertraglichen Bindung zwischen Verantwortlichem und betroffener Person, wenn die Daten von unbeteiligten Außenstehenden miterfasst werden.

Diese Drittinvolvierung ist ein grundsätzliches Problem im Rahmen des Internets der Dinge. Laut einer Studie nutzte ein Viertel der Deutschen im Jahr 2019 sprachaktivierte Assistenten,[188] die jeweils signifikante datenschutzrecht-

---

eu/ipg/basics/legal/cookies/index_en.htm; *Ryte Wiki*, Third Party Cookies, https://de.ryte.com/wiki/Third_Party_Cookies.

[185] *Steidle/Pordesch*, DuD 2008, 324 (324 f.); *Knopp*, DuD 2010, 783 (784); dies kann über eine konstante Cookie-ID oder über die (für eine gewisse Zeit) konstante IP-Adresse erfolgen.

[186] Zu dieser Technik grundlegend *Kohno/Broido/Claffy*, 2 IEEE Transactions on Dependable and Secure Computing 2005, 93; *Nikiforakis et al.*, IEEE Symposium on Security and Privacy 2013, 541; *Mowery/Shacham*, Proceedings of W2SP 2012, 1.

[187] Siehe dazu *Han/Jung/Wetherall*, A study of third-party tracking by mobile apps in the wild, University of Washington Technical Report UW-CSE-12–03–01, 2012, 2 f.; *Enck et al.*, 32 ACM Transactions on Computer Systems (TOCS) 2014, 5.

[188] *Arnold et al.*, Any Sirious Concerns Yet? – An Empirical Analysis of Voice Assistants' Impact on Consumer Behavior and Assessment of Emerging Policy Challenges, Working Paper, 2019, https://ssrn.com/abstract=3426809, 8; siehe auch oben, § 2 A.

liche Risiken aufweisen: Von Echo aufgezeichnete und von dem Sprachassistenten Alexa ausgewertete Audiomitschnitte werden einem Bericht zufolge von Amazon-Mitarbeitern zum Teil gelesen, um die Qualität der ML-basierten Spracherkennung zu verbessern.[189] Allerdings können dabei eben auch Sprachmitschnitte von Dritten getätigt werden.[190] Bekannt wurden etwa Fälle, bei denen die Kinder der Eigentümer eines sprachbasierten IoT-Geräts selbstständig Produkte bestellten.[191] Amazon-Mitarbeiter teilten besonders amüsante Mitschnitte offenbar zudem in einem internen Chat,[192] was die Dringlichkeit einer wirksamen Kontrolle vor Augen führt. Hinzu kommt, dass auf maschinellem Lernen basierende Verfahren es zunehmend präziser ermöglichen, aus einer Sprachanalyse Persönlichkeitsmerkmale der betroffenen Person abzuleiten[193] – eine weitere Gruppe potenziell für die Betroffenen mit Risiko behafteter Inferenzen.[194]

II. Leitfragen

Aus den drei soeben geschilderten Leitfällen sowie der zweiten und dritten rechtlichen Herausforderung (Ambivalenz und Aktorheterogenität) ergeben sich zwei große Leitfragen, welche die Analyse des zweiten und dritten Teils dieser Arbeit prägen werden.

Einerseits ist zu eruieren, welche Ressourcen das positive Recht im Bereich des Datenschutzrechts (§ 4, besonders E.) und des allgemeinen Zivilrechts (§ 5, besonders C.) bereithält, um den geschilderten Risiken vernetzter Datenerhebung und -analyse entgegenzutreten. Zu untersuchen ist daher, welche regulatorischen Strukturen dem existierenden Recht in diesen Bereichen einbeschrieben sind, mit denen eine unkontrollierte Erhebung und Weiterleitung von Daten insoweit eingeschränkt werden kann, als diese auf Marktversagen beruht oder zu nicht mehr hinnehmbaren sozialen Risiken führt. Dies impliziert zugleich die Frage nach dem Wechselspiel und der Effektivität dieser Ordnungsmechanismen.

---

[189] *Day/Turner/Drozdiak*, Amazon Workers Are Listening to What You Tell Alexa, Bloomberg (11.4.2019), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

[190] Siehe *Wissenschaftliche Dienste – Deutscher Bundestag*, Zulässigkeit der Transkribierung und Auswertung von Mitschnitten der Sprachsoftware „Alexa" durch Amazon, WD 10 – 3000 – 032/19, Sachstand, 2019, 9.

[191] *Liptak*, Amazon's Alexa started ordering people dollhouses after hearing its name on TV, The Verge (7.1.2017), https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse.

[192] *Day/Turner/Drozdiak*, Amazon Workers Are Listening to What You Tell Alexa, Bloomberg (11.4.2019), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

[193] *Alam/Ricardi*, Proceedings of the 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 955; *Polzehl*, Personality in Speech, 2015, 143–53.

[194] Siehe dazu ausführlich *Hacker*, 7 International Data Privacy Law 2017, 266 (267 ff.).

Andererseits muss erhärtet werden, ob hinreichende entscheidungsunterstützende Normen zur Verfügung stehen, welche die Ausübung von Privatautonomie im Sinne einer souveränen und freiheitlichen Gestaltung der eigenen digitalen Austauschprozesse durch das jeweilige Individuum ermöglichen. Auch die Beantwortung dieser zweiten Leitfrage muss zunächst das bestehende Datenschutzrecht (§ 4, besonders D.) und Zivilrecht (§ 5, besonders B.) in den Blick nehmen. Erst in einem letzten Schritt ist dann danach zu fragen, welcher Reformbedarf sich hinsichtlich der beiden Leitfragen aus den Beschränkungen des positiven Rechts ergibt (§ 6).

E. Ergebnisse von § 3

1. Als Zwischenergebnis kann damit festgehalten werden, dass die Vernetzung von Geräten im Rahmen des IoT und der Einsatz von Daten als Gegenleistung, wie fast alle neuen Technologien, erhebliches Potenzial bieten, zugleich aber auch signifikante Risiken bereithalten. Dies mag trivial erscheinen, generiert jedoch ein manifestes regulatorisches Problem. Mögliche Gewinne entfalten sich einerseits auf individueller Ebene, wo eine stärkere Präferenzerfüllung einhergehen kann mit Zeitersparnis und einer Kaufkraftsteigerung in Form der Aufstockung des Verbraucherbudgets um die eigenen Daten. Soziale Gewinne andererseits lassen sich gerade durch die Vernetzung erzielen, die präzisere Steuerung und genauere Vorhersage sozialer Phänomene ermöglicht.

2. Dem stehen jedoch ökonomische wie auch soziale Risiken gegenüber, die drei spezifische rechtliche Herausforderungen mit sich bringen. Erstens eignet personenbezogenen Daten ein Drittbezug. Diese Multirelationalität weist über das primäre Vertrags- oder Nutzungsverhältnis hinaus und erhöht die Komplexität privatautonomer Gestaltung bezogen auf die Verwendung personenbezogener Daten.

3. Die Ambivalenz der Verarbeitung personenbezogener Daten stellt eine zweite regulatorische Herausforderung dar. Einerseits wohnt ihnen erhebliches Potenzial sowohl für individuelle als auch soziale Nutzengewinne inne. Andererseits konnten vier für den hiesigen Kontext relevante Typen von Marktversagen identifiziert werden, die suggerieren, dass die materiellen Voraussetzungen für die Inanspruchnahme von Privatautonomie nur sehr eingeschränkt vorliegen. Während verhaltensökonomische Effekte bei der Einschätzung des Datenwertes und der Entscheidung über die Datenpreisgabe lediglich solche Akteure betreffen, die in der konkreten Situation beschränkt rational handeln, sehen sich auch rationale Akteure mit den drei übrigen Typen von Marktversagen konfrontiert: Informationsasymmetrie (aufgrund rationaler Ignoranz), Externalitäten durch Kollektiveffekte und einer Unschärfe des Preissignals infolge der intrinsischen Unbestimmtheit des Marktwertes von Daten. Hinzu kommen soziale Risiken, wie etwa eine Verengung der Verhaltensfreiheit auf-

grund von (eingebildetem oder tatsächlichem) Kontrollverlust über die eigenen Daten sowie eine Unentziehbarkeit, die in dem Maße zunimmt, in dem IoT-Geräte den öffentlichen Raum erobern und steuern.

4. Verschärft wird dieser Befund drittens durch stark unterschiedlich verteilte Präferenzen hinsichtlich der Wichtigkeit von Datenschutz. Ein rechtliches Regime sollte es jedenfalls auch Personen mit hoher Datenschutzpräferenz ermöglichen, diese selbstbestimmt wahrzunehmen und umzusetzen. Hinsichtlich derjenigen Personen mit gering ausgeprägten Datenschutzpräferenzen sollte zugleich die Kollektivdimension von Datenschutz nicht unterschätzt werden: Die angesprochenen Externalitäten bilden gleichsam eine, im Einzelnen zu verhandelnde, Grenze der rechtlichen Akzeptabilität von freiwilliger Datenpreisgabe. Insgesamt kommt in dieser dritten rechtlichen Herausforderung regulatorisches und ermöglichendes Privatrecht zusammen: Um die effektive Wahrnehmung von Privatautonomie, inklusive der Durchsetzung heterogener Präferenzen, am Markt zu ermöglichen, muss teilweise regulierend in die Marktstruktur eingegriffen werden.

Teil 2

Datenschutzrecht und allgemeines Privatrecht

§ 4 Vernetzte Datenerhebung und -analyse im Datenschutzrecht

Ausgehend von den drei soeben skizzierten Leitfällen der Datenweiterleitung an Dritte, der Datenerhebung durch Drittanbieter und der Datenerhebung bei Dritten zeichnet das folgende Kapitel nach, wie das Datenschutzrecht mit den skizzierten Problemen der Vernetzung umgeht. Das Datenschutzrecht ist jedoch ein weites Feld. Daher werden zunächst datenschutzrechtliche Grundlagen gelegt (A.). Daran schließt sich eine Analyse der materiellen Rechtmäßigkeitsvoraussetzungen der DS-GVO, ergänzend auch anderer datenschutzrechtlicher Instrumente, an, jeweils unter dem Blickwinkel der positivrechtlichen Ressourcen, welche diese Instrumente bereitstellen, um den in § 3 genannten Herausforderungen der Vernetzung zu begegnen. Anders als das auf dem Grundsatz der Vertragsfreiheit aufruhende allgemeine Zivilrecht ist jedoch das Datenschutzrecht grundsätzlich geprägt durch seinen regulatorischen Ordnungscharakter: Art. 6 Abs. 1 DS-GVO statuiert ein Verbot mit Erlaubnisvorbehalt, in dessen Folge jeweils nach spezifischen Erlaubnistatbeständen für Datenverarbeitungsvorgänge gesucht werden muss, um diese zu legalisieren. Zwar bestehen hier insbesondere mit den Erlaubnistatbeständen der Einwilligung und der vertragserforderlichen Datenverarbeitung durchaus auch ermöglichende Strukturen, innerhalb derer sich privatautonome Verständigung vollziehen kann (B.). Daneben ist das Datenschutzrecht jedoch durch spezifische regulatorischen Strukturen gekennzeichnet, die wiederum mit Blick auf die Vernetzungsproblematik analysiert werden können (C.).

A. Datenschutzrechtliche Grundlagen

Um eine Basis für die Diskussion der ermöglichenden und regulatorischen Strukturen des unionalen Datenschutzrechts zu gewinnen, müssen zunächst rechtliche Grundlagen gelegt werden. So werden in aller gebotenen Kürze die Rechtsgrundlagen des Datenschutzrechts dargestellt (I.). Zentrales Instrument des gegenwärtigen Datenschutzrechts ist die DS-GVO. Insofern ist die Frage nach ihrer territorialen und sachlichen Anwendbarkeit in Vernetzungssituationen als erste substanzielle Fragestellung zu behandeln (II.). Daran schließt sich die Diskussion von Grundkonzepten wie datenschutzrechtlicher Verantwortlichkeit und den Grundsätzen der Datenverarbeitung an (III.).

I. Rechtsgrundlagen des Datenschutzrechts im Kurzüberblick

Das Datenschutzrecht zeichnet sich durch ein Ineinandergreifen verschiedener Rechtsgrundlagen aus, die zum Teil auf europäischer, zum Teil aber auch auf nationaler Ebene angesiedelt sind.

1. Europäische Ebene

Auf europäischer Ebene ist das Datenschutzrecht primärrechtlich, wie bereits verschiedentlich angesprochen, als Grundrecht in Art. 8 GRCh und Art. 16 AEUV geschützt.[1] Dass das Datenschutzrecht, auch wenn es im privatrechtlichen Bereich marktregulierenden Charakter hat, immer zugleich Ausgestaltung eines Grundrechts ist, wird noch an verschiedenen Stellen zu berücksichtigen sein. Hinzu tritt das in Art. 7 GRCh und Art. 8 EMRK verankerte Recht auf Achtung des Privatlebens und der Kommunikation, das vom EuGH häufig gemeinsam mit Art. 8 GRCh geprüft wird.[2] Sekundärrechtlich existieren neben der DS-GVO verschiedene Rechtsakte, die sachbereichsspezifische Datenschutzrechtsvorgaben enthalten.

a) DS-GVO

Die DS-GVO[3] stellt die Zentralvorschrift des europäischen sekundären Datenschutzrechts dar.[4] Gemäß ihrem Art. 99 Abs. 2 in Geltung seit dem 25.5.2018, löste sie die DSRL[5] von 1995 ab.[6] Schon die DSRL sollte ausweislich ihres achten Erwägungsgrunds „ein gleichwertiges Schutzniveau hin-

[1] Zum umstrittenen Verhältnis der beiden Normen *Britz*, EuGRZ 2009, 1 (2 ff.); *Schneider*, DV 44 (2011), 499 (502 ff.); *Schröder*, in: Streinz, EUV/AEUV, 3. Aufl. 2018, AEUV, Art. 16 Rn. 5 f.; *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 16 Rn. 3; *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, 19. Nach herrschender Meinung ist Art. 8 GRCh entgegen Art. 52 Abs. 2 GRCh vorrangig, um die Schrankenregelung des Art. 8 Abs. 2 GRCh, die bei Art. 16 AEUV fehlt, nicht leerlaufen zu lassen.

[2] Siehe nur EuGH, Urt. v. 8.4.2014 – verb. Rs. C-293/12 und C-594/12 (*Digital Rights Ireland*) – Rn. 31; Urt. v. 13.5.2014 – Rs. C-131/12 (*Google Spain*) – Rn. 74 und 97; Urt. v. 6.10.2015 – Rs. C-362/14 (*Schrems*) – Rn. 66 und 91; Urt. v. 24.9.2019 – Rs. C-136/17 (*GC u. a.*) – Rn. 59; dazu ausführlich *Lynskey*, The Foundations of EU Data Protection Law, 2015, 89 ff.; *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, 2014, 254 ff.; grundsätzlich zu Art. 8 EMRK ebd., 23 ff.

[3] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119/1.

[4] *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Einleitung Rn. 209; *Kühling/Raab*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Einführung Rn. 3a.

[5] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281/31.

[6] Siehe Art. 94 DS-GVO.

sichtlich der Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten" sicherstellen. Dieser Harmonisierungsaufgabe jedoch wurde die Richtlinie aufgrund der Vielzahl im Detail abweichender Umsetzungsbestimmungen und deren unterschiedlicher Anwendung in den verschiedenen Mitgliedstaaten jedenfalls aus Sicht des europäischen Gesetzgebers nicht gerecht.[7] Insofern erschien es nur folgerichtig, im Rahmen der Novellierung der DSRL von einer Richtlinie zu einer Verordnung überzugehen. Die DS-GVO ist daher, auch wenn dies nicht ausdrücklich festgehalten wurde, grundsätzlich vollharmonisierend.[8] Allerdings lassen die mehr als 70 Öffnungsklauseln zugunsten der Mitgliedstaaten zumindest Zweifel an der Harmonisierungswirkung aufkommen.[9] Der vollharmonisierende Charakter derjenigen Vorschriften der DS-GVO, die nicht mit einer Öffnungsklausel ausgestattet sind, wird hierdurch jedoch nicht angetastet. Nichtsdestoweniger wird die DS-GVO in der Literatur auch als „atypischer Hybrid aus Verordnung und Richtlinie"[10] – was nur metaphorisch und nicht formal rechtlich zutrifft[11] – sowie als „Ko-Regulierung zwischen Union und Mitgliedstaaten"[12] bezeichnet. Jedenfalls verweisen die Öffnungsklauseln darauf, dass die Regelungen der DS-GVO nicht gänzlich allein die Ordnung der digitalen Wirtschaft bewältigen können und sollen, sondern der Ergänzung durch nationales Recht bedürfen.

b) ePrivacy-Instrumente

Der zweite für das Privatrecht besonders bedeutsame europäische Regelungsakt im Rahmen des Datenschutzrechts ist die ePrivacy-Richtlinie, ursprünglich von 1997,[13] novelliert 2002[14] und nochmals überarbeitet 2009.[15] Sie regelt

---

[7] 9. Erwägungsgrund der DS-GVO.

[8] *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Einleitung Rn. 211; *Schantz*, in: BeckOK DatenschutzR, 27. Ed. 1.2.2019, Art. 1 DS-GVO Rn. 8; vgl. den 3. und 10. Erwägungsgrund sowie Art. 1 Abs. 3 der DS-GVO.

[9] *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 342; *Buchner*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 1 DS-GVO Rn. 5, 7; *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Einleitung Rn. 227; *Laue*, ZD 2016, 463 (463 f.); *Kühling/Martini*, EuZW 2016, 448 (449 f.); *Roßnagel*, DuD 2016, 553 (553).

[10] *Kühling/Martini*, EuZW 2016, 448 (449); siehe auch *Kühling/Raab*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Einführung Rn. 2.

[11] *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Einleitung Rn. 226.

[12] *Roßnagel*, DuD 2017, 290 (291).

[13] Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. 1997 L 24/1.

[14] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. 2002 L 201/37.

sektorspezifisch den Datenschutz in der elektronischen Kommunikation, genauer die „Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft", Art. 3 Abs. 1 ePrivacy-Richtlinie. Auch hier ist eine weitere Novellierung geplant in Form des Erlasses einer ePrivacy-Verordnung, deren Entwurf die Kommission im Jahr 2017 vorlegte[16] und deren Erlass ursprünglich zeitgleich mit der DS-GVO abgeschlossen sein sollte. Aufgrund von Verzögerungen im Rechtsetzungsprozess wurde jedoch zunächst die DS-GVO selbstständig, ohne flankierende ePrivacy-Verordnung, verabschiedet.[17]

Ihre besondere Relevanz erfahren die ePrivacy-Instrumente dadurch, dass die ePrivacy-Richtlinie für die praktisch besonders bedeutsamen Cookies (Art. 5 Abs. 3), aber auch für die Direktwerbung (Art. 13), das maßgebliche Regelungsinstrument im Rahmen des Datenschutzes darstellt. Insofern handelte es sich um eine *lex specialis* zur DSRL.[18] Gleiches wird (wohl) auch für die ePrivacy-Verordnung gegenüber der DS-GVO gelten.[19]

Das Verhältnis von ePrivacy-*Richtlinie* und DS-GVO bestimmt sich hingegen nach Art. 95 DS-GVO. Umstritten ist hier insbesondere, inwiefern für die Zwischenzeit, nach Beginn der Geltung der DS-GVO und vor Geltungsbeginn der ePrivacy-Verordnung, Cookies der Regelung der ePrivacy-Richtlinie oder aber der DS-GVO unterfallen.[20]

c) Sonstige Instrumente

Auf unionaler Ebene existieren eine Reihe weiterer spezifischer Rechtsakte zum Datenschutz in verschiedenen Bereichen. Gleichzeitig mit der DS-GVO wurde für den Bereich der Gefahrenabwehr und der Strafverfolgung die JI-Richtlinie[21] verabschiedet, als Nachfolge eines Rahmenbeschlusses zur selben

---

[15] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl. 2009 L 337/11.

[16] *Europäische Kommission*, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, COM(2017) 10 final; dazu etwa *Engeler/Felber*, ZD 2017, 251; *Maier/Schaller*, ZD 2017, 373; *Article 29 Data Protection Working Party*, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 2017.

[17] *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Einleitung Rn. 221.

[18] Art. 1 Abs. 2 ePrivacy-Richtlinie.

[19] 173. Erwägungsgrund der DS-GVO.

[20] Siehe dazu im Einzelnen unten, § 4 B.I.4.

[21] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April

Thematik.[22] Die Verarbeitung von Fluggastdaten richtet sich nach der PNR-Richtlinie,[23] die ebenfalls der Gefahrenabwehr und Strafverfolgung dient und auch gemeinsam mit der DS-GVO verabschiedet wurde. Verschiedene weitere Rechtsakte im Sicherheitsbereich regeln zudem den Datenaustausch zwischen Sicherheitsbehörden.[24]

Die bereits im Jahr 2006 erlassene Richtlinie zur Vorratsdatenspeicherung[25] hingegen wurde vom EuGH für ungültig erklärt.[26] Die Datenverarbeitung durch Unionsinstitutionen schließlich ist in einer eigenen Verordnung geregelt.[27] Hinzukommen werden künftig noch Durchführungsrechtsakte der Kommission, im Bereich der DS-GVO zu Bildsymbolen (Icons, Art. 12 Abs. 8 DS-GVO), zu Verhaltensregeln (Art. 40 Abs. 9 DS-GVO), zu Zertifizierungsverfahren (Art. 43 Abs. 8 und 9 DS-GVO), zur Datenübermittlung an Drittländer (Art. 45 Abs. 3, 46 Abs. 2 DS-GVO) sowie zu internen Datenschutzvorschriften (Art. 47 Abs. 3 DS-GVO).

2. *Nationale Ebene*

Neben diesen unionalen Regelungen verbleibt jedoch dem nationalen Gesetzgeber nicht unwesentlicher Spielraum zur Gestaltung von Datenschutzvorschriften. Dies zeigt sich vor allem an der Vielzahl der Öffnungsklauseln in der DS-GVO. Hinzu treten die Umsetzungsvorschriften für die ePrivacy-Richt-

---

2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. 2016 L 119/89; dazu etwa *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Einleitung Rn. 215–217; *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, 326 ff.

[22] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. 2008 L 350/60.

[23] Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität, ABl. 2016 L 119/132.

[24] *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Einleitung Rn. 223–225.

[25] Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. 2006 L 105/54.

[26] EuGH, Urt. v. 8.4.2014 – verb. Rs. C-293/12 und C-594/12 (*Digital Rights Ireland*).

[27] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABl. 2018 L 295/39.

linie. Soweit ein Spielraum besteht, ist dabei insbesondere das Recht auf informationelle Selbstbestimmung, welches das Bundesverfassungsgericht aus Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG ableitet,[28] maßgeblich zu beachten.[29]

a) BDSG

In Deutschland ist der zentrale nationale Datenschutzrechtsakt das Bundesdatenschutzgesetz (BDSG). Soweit die DS-GVO abschließende Regelungen enthält, ist sie aufgrund des Anwendungsvorrangs des Europarechts ohnehin vorrangig, § 1 Abs. 5 BDSG.[30] Materiellrechtliche Regelungen von Belang finden sich insbesondere in den §§ 26–31 BDSG mit Regelungen zum Beschäftigtendatenschutz, § 26 BDSG; zur Datenverarbeitung zu wissenschaftlichen, historischen oder statistischen Zwecken, § 27 BDSG; zur Datenverarbeitung zu Archivzwecken, § 28 BDSG; zu Verbraucherkrediten, § 30 BDSG; und schließlich zu Scoring und Bonitätsauskünften, § 31 BDSG.[31] Ferner enthält das BDSG eine Reihe von Durchsetzungsvorschriften, §§ 41–43, 84 BDSG für den Bereich des Straf- und Ordnungswidrigkeitenrechts sowie § 83 BDSG für Schadensersatz bei Verstoß gegen Vorschriften, welche der Umsetzung der JI-Richtlinie dienen. Der Schadensersatzanspruch für einen Verstoß gegen die DS-GVO ist hingegen unmittelbar in Art. 82 DS-GVO normiert.

b) UWG

Praktisch besonders relevant sind ferner die ebenso sehr datenschutz- wie wettbewerbsrechtlich geprägten Vorschriften zur Direktwerbung, die in Umsetzung von Art. 13 der ePrivacy-Richtlinie in § 7 Abs. 2 und 3 UWG normiert wurden.[32] Sie beziehen sich vor allem auf Werbung mithilfe von Telefonanrufen, automatischen Anrufmaschinen, Faxgeräten und E-Mails. Die detaillierte Untersuchung dieser Vorschriften muss jedoch einer eigenständigen Publikation vorbehalten bleiben.[33]

---

[28] Grundlegend BVerfG NJW 1984, 419 (422) – Volkszählung; dazu etwa *Schantz*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 143 ff.; *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, 31 ff.

[29] BVerfG GRUR 2020, 74 Rn. 48 – Recht auf Vergessen I; BVerfG GRUR 2020, 88 Rn. 77 ff. – Recht auf Vergessen II; BVerfG NVwZ 2007, 937 (938); siehe auch *Reiserer/Christ/Heinz*, DStR 2018, 1501 (1502); siehe noch unten, § 5 C.III.4.a)bb)(1).

[30] Zum Anwendungsvorrang ausführlich unten, § 5 A.I.

[31] Siehe speziell zu § 31 BDSG etwa *Taeger*, ZRP 2016, 72; *Taeger*, RDV 2017, 3; Sachverständigenrat für Verbraucherfragen, Verbrauchergerechtes Scoring, 2018, 118 ff.; *Guggenberger*, ZBB 2019, 254 (260 f.); interdisziplinäre Perspektive in *Schröder/Taeger* (Hrsg.), Scoring im Fokus: Ökonomische Bedeutung und rechtliche Rahmenbedingungen im internationalen Vergleich, 2014.

[32] Siehe etwa *Buchner*, WRP 2018, 1283.

[33] Siehe allerdings die Hinweise im Text bei § 4, Fn. 448 und 964 und § 5, Fn. 713.

c) Sonstige Regelungen

Die weiteren Vorschriften der ePrivacy-Richtlinie wurden im deutschen Recht in den §§ 91 ff. TKG, 12 ff. TMG umgesetzt.[34] Sie sind insbesondere für das Telekommunikationsrecht von Bedeutung, werden jedoch mit Inkrafttreten der ePrivacy-Verordnung ihre Geltung verlieren. Sachbereichsspezifische Sonderregelungen existieren weiterhin im Bereich des Sozialrechts für Sozialdaten, etwa nach § 35 SGB I und §§ 67 ff. SGB X.[35] Schließlich finden sich weitere Regelungen in Landesdatenschutzgesetzen, insbesondere für Landesbehörden[36] und im Bereich der Durchsetzung.[37]

II. Anwendbarkeit der DS-GVO

Im Zentrum der folgenden Überlegungen wird die DS-GVO stehen, das Herzstück des europäischen Datenschutzrechts. Einen rechtlichen Rahmen für die digitale Wirtschaft kann diese jedoch nur dann abgeben, wenn sie überhaupt anwendbar ist. Gerade in vernetzten Umgebungen, in denen Daten teilweise über Ländergrenzen hinweg verschoben, teilweise aber auch rein national verarbeitet werden, stellt sich zunächst die Frage der territorialen Anwendbarkeit. Darüber hinaus ist bei bestimmten Erhebungs- und Verarbeitungsformen zu bestimmen, ob die DS-GVO sachlich anwendbar ist. Dafür müssen personenbezogene Daten in spezifischer Weise verarbeitet werden. Dies kann insbesondere bei stark anonymisierten Trainingsdaten, wie sie im Bereich maschinellen Lernens Verwendung finden, fraglich werden.

1. Territoriale Anwendbarkeit

Zwar lässt sich bereits wenige Jahre nach Verabschiedung der DS-GVO eine starke Ausstrahlung der Verordnung auf das internationale Datenschutzregime, auch über die EU hinaus, konstatieren.[38] Für die formal-rechtliche Wirkung der DS-GVO und ergänzender nationaler Regelungen ist jedoch die Eröffnung des jeweiligen territorialen Anwendungsbereichs notwendig. Diese hängt im europäischen und deutschen Datenschutzregime von einer Reihe von Faktoren ab.

---

[34] *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, 330 ff.

[35] Dazu etwa *Freund/Shagdar*, SGb 2018, 195; *Bieresborn/Giesberts-Kaminski*, SGb 2018, 449.

[36] Allerdings ist auf nicht-öffentliche Stellen, mit Ausnahme der Regelung in § 2 Abs. 4 S. 2 BDSG, grundsätzlich wegen Art. 74 Abs. 1 Nr. 11 und Nr. 12 GG das BDSG, nicht Landesrecht, anwendbar, siehe *Gusy/Eichenhofer*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2018, Art. 1 DS-GVO Rn. 76 und 128.

[37] Siehe § 40 BDSG.

[38] *P. Schwartz*, 94 NYU Law Review 2019, 771; *Rubinstein/Petkova*, in: Cole/Boehm (Hrsg.), Commentary on the General Data Protection Regulation, im Erscheinen, https://ssrn.com/abstract=3167389; *Buttarelli*, 6 International Data Privacy Law 2016, 77; grundlegend zum Brussels Effect *Bradford*, 107 Northwestern University Law Review 2012, 1.

Die DS-GVO hat im Zuge einer der markanten Neuerungen gegenüber der DSRL das Marktortprinzip konsequent eingeführt.[39] Danach ist die DS-GVO zwar weiterhin, wie bereits die DSRL, territorial anwendbar, wenn personenbezogene Daten im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der EU verarbeitet werden (Art. 3 Abs. 1 DS-GVO). Ferner unterfällt jedoch nun auch die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, der DS-GVO, wenn die Verarbeitung entweder im Zusammenhang mit dem Angebot von Waren oder Dienstleistungen in der EU oder aber im Zusammenhang mit der Beobachtung des Verhaltens der betroffenen Person steht (Art. 3 Abs. 2 DS-GVO). Diese Vorgaben sind nicht abdingbar.[40]

Ganz ähnlich formuliert der deutsche Gesetzgeber bei der Absteckung des Anwendungsbereichs des BDSG, der etwa für die in Ausfüllung der Öffnungsklauseln erlassenen Vorschriften relevant ist.[41] Für die hier interessierende Datenverarbeitung durch nicht-öffentliche Stellen statuiert § 1 Abs. 4 S. 2 BDSG, dass eines von drei Kriterien erfüllt sein muss: Der Verantwortliche oder der Auftragsverarbeiter verarbeitet Daten im Inland (Nr. 1);[42] die Verarbeitung erfolgt im Rahmen der Tätigkeit einer inländischen Niederlassung (Nr. 2); oder der Verantwortliche oder Auftragsverarbeiter hat keine Niederlassung in der EU oder dem EWR, er unterfällt jedoch dem Anwendungsbereich der DS-GVO (Nr. 3).[43] Das BDSG spiegelt mithin im Wesentlichen die Kriterien der DS-GVO bezogen auf das deutsche Staatsgebiet und verweist im Übrigen, für Nicht-EU/Nicht-EWR-Verarbeiter, auf die Anwendbarkeit der DS-GVO. Damit rückt diese in das Zentrum des Interesses.

Problematisch ist die territoriale Anwendbarkeit der DS-GVO vor allem in zwei Fällen: bei der Datenerhebung und -verarbeitung durch multinationale Unternehmen mit Hauptsitz im EU-Ausland (eine typische Konstellation in allen drei Leitfällen); und bei dezentralen Netzwerken (z. B. Blockchains), auf die hier jedoch nur kursorisch eingegangen werden kann.

a) Art. 3 Abs. 1 DS-GVO: Niederlassungsprinzip

In Art. 3 Abs. 1 DS-GVO knüpft der europäische Gesetzgeber mithin für die territoriale Anwendbarkeit zentral an die Existenz einer Niederlassung in der EU an. Ganz ausdrücklich spielt es dabei nach dem Wortlaut der Vorschrift

[39] *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 15.

[40] *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 105.

[41] *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 10.

[42] Dies widerspricht allerdings dem Herkunftslandprinzip, wenn der Verarbeiter in einem anderen Mitgliedstaat niedergelassen ist. Kritisch daher *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 13.

[43] Hier ist richtigerweise ferner ein deutscher Inlandsbezug zu fordern, siehe *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 15.

keine Rolle, ob die Verarbeitung selbst innerhalb der EU stattfindet oder außerhalb; ferner auch nicht, ob die betroffenen Personen Unionsbürger sind oder nicht. Die Regelung entspricht im Wesentlichen Art. 4 Abs. 1 lit. a DSRL. Hier wie auch dort war bzw. ist entscheidend, dass die Verarbeitung im Rahmen einer Tätigkeit der EU-Niederlassung erfolgt.

aa) Der Begriff der Niederlassung

Dies bedeutet zunächst, dass nur solche international operierenden Verarbeiter von Art. 3 Abs. 1 DS-GVO erfasst werden, die überhaupt eine Niederlassung in der Union besitzen. Der Begriff der Niederlassung wird nicht, wie andere zentrale Begriffe der DS-GVO, in Art. 4 DS-GVO definiert. Vielmehr findet sich eine, gleichwohl nicht bindende, Umschreibung im 22. Erwägungsgrund der Verordnung.[44] Danach gilt: „Eine Niederlassung setzt die effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus. Die Rechtsform einer solchen Einrichtung, gleich, ob es sich um eine Zweigstelle oder eine Tochtergesellschaft mit eigener Rechtspersönlichkeit handelt, ist dabei nicht ausschlaggebend."

Dabei knüpft die Formulierung in erkennbarer Weise an die Rechtsprechung des EuGH zur Niederlassungsfreiheit nach Art. 49 AEUV an.[45] Bei größeren Unternehmen lässt sich typischerweise die Existenz einer Niederlassung leicht aus dem jeweiligen Handelsregister erkennen. Allerdings ist die formale Eintragung keine Voraussetzung für das Bestehen einer Niederlassung, wie der EuGH in *Weltimmo* feststellte. Vielmehr ist der Begriff unter Bezug auf „sowohl de[n] Grad an Beständigkeit der Einrichtung als auch die effektive Ausübung der wirtschaftlichen Tätigkeiten […] unter Beachtung des besonderen Charakters dieser Tätigkeiten und der in Rede stehenden Dienstleistungen auszulegen."[46] Eine Niederlassung ist daher anzunehmen, wenn mittels einer festen Einrichtung eine tatsächliche und effektive Tätigkeit ausgeübt wird, selbst wenn sie nur geringfügig ist.[47]

Problematisch sind hier insbesondere dezentrale Netzwerke, etwa offene Blockchains wie Bitcoin.[48] In deren Rahmen werden zwar Daten verarbeitet, sie besitzen jedoch keine zentralisierten, festen Einrichtungen.[49] Nichtsdestoweniger lässt sich hier mit guten Argumenten vertreten, dass die einzelnen Mit-

[44] *Thon*, RabelsZ 84 (2020), 24 (31 f.).

[45] EuGH, Urt. v. 25.7.1991 – Rs. C-221/89 (*Factortame*) – Rn. 20: „tatsächliche Ausübung einer wirtschaftlichen Tätigkeit mittels einer festen Einrichtung in einem anderen Mitgliedstaat auf unbestimmte Zeit".

[46] EuGH, Urt. v. 1.10.2015 – Rs. C-230/14 (*Weltimmo*) – Rn. 29.

[47] EuGH, Urt. v. 1.10.2015 – Rs. C-230/14 (*Weltimmo*) – Rn. 31; zu Rechtsscheinkonstellationen *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 102 f.

[48] Dazu ausführlich *de Filippi/Wright*, Blockchain and the Law, 2018; *Hacker/Lianos/Dimitropoulos/Eich* (Hrsg.), Regulating Blockchain, 2019.

[49] Technische Details bei *Narayanan et al.*, Bitcoin and Cryptocurrency Technologies, 2016, Kapitel 1.

glieder (*full nodes*) des Netzwerks jeweils als Niederlassung gelten, da sie jedenfalls für eine gewisse Dauer an einem bestimmten Ort für das Netzwerk unverzichtbare Tätigkeiten der Validierung, Informationspropagation und Revision (*updating*) der Datenkette übernehmen.[50] Für die drei oben beschriebenen Leitfälle stellt dies solange kein Problem dar, als die Datenverarbeitung nicht über stark dezentralisierte Netzwerke abgewickelt wird, was gegenwärtig jedenfalls für größere Verarbeiter wie die führenden Internetunternehmen (GAFAM) nicht als eine realistische Entwicklungsperspektive erscheint.[51]

bb) Verarbeitung im Rahmen der Tätigkeit der Niederlassung

Vielmehr kann bei Verarbeitung durch international tätige Unternehmen problematisch sein, inwiefern etwa die Datenverarbeitung von Facebook oder Google im Rahmen der Tätigkeit einer EU-Niederlassung erfolgt, und nicht im Rahmen der Tätigkeit des US-amerikanischen Hauptsitzes. In der Literatur[52] und auch von der Artikel-29-Datenschutzgruppe[53] wird hier gefordert, dass die Niederlassung jedenfalls in die spezifische Datenverarbeitung einbezogen sein muss. Teilweise wird verschärfend sogar darauf abgestellt, ob die Niederlassung die Datenverarbeitung selbstständig inhaltlich steuert oder kontrolliert.[54] Damit werden jedoch Kriterien zur Bestimmung des Verantwortlichen im Sinne von Art. 4 Nr. 7 DS-GVO mit jenen zur Bestimmung der Anwendbarkeit der DS-GVO vermengt.

Der EuGH hat zur identischen Formulierung in der DSRL in der Rechtssache *Google Spain* entschieden, dass die Wendung „im Rahmen der Tätigkeiten" weit zu verstehen sei. Konkret stand die Anwendbarkeit spanischen Datenschutzrechts infrage, weil die maßgebliche Datenverarbeitung, die Speicherung und Verlinkung von Webseiten mit personenbezogenen Daten, durch die in den USA ansässige Google, Inc. durchgeführt wurde. Die spanische Niederlassung war hingegen lediglich für die spanienbezogene Vermarktung der Werbeflächen zuständig, welche eine wesentliche Einkommensquelle für Google darstellen. Wortlaut („im Rahmen") und Ziel der DSRL, einen wirksamen und umfassenden Datenschutz zu gewährleisten, implizieren nach dem

[50] *Buocz*, *et al.*, 35 Computer Law & Security Review 2019, 182 (191).

[51] Zwar hat Facebook eine Kryptowährung namens *Libra* gestartet, die jedoch als *permissioned blockchain* keinen hohen Dezentralisierungsgrad aufweist; siehe zu *Libra* etwa *Werbach*, The Real Reason for Facebook's New Cryptocurrency, The New York Times, (20.6.2019), https://www.nytimes.com/2019/06/20/opinion/facebook-libra-cryptocurrency.html.

[52] *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 55; *Voigt*, ZD 2014, 15 (17); *Beyvers/Herbrich*, ZD 2014, 558 (562).

[53] Artikel 29-Datenschutzgruppe, Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, WP 148, 2008, 11.

[54] *Borges* in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil 1 Kap. 3 Rn. 75 f.; ähnlich *Ott*, MMR 2009, 158 (160); *Karg*, ZD 2013, 371 (374); *Pauly/Ritzer/Geppert*, ZD 2013, 423 (425).

EuGH jedoch, dass die Niederlassung nicht selbst die Datenverarbeitung vornehmen muss.[55] Vielmehr genügt es, wenn die Tätigkeit der EU-Niederlassung mit der Tätigkeit der eigentlich datenverarbeitenden Stelle untrennbar verbunden ist.[56] Dies nahm der EuGH deshalb an, weil die Werbeanzeigen notwendig immer mit den verlinkten Inhalten, die wiederum personenbezogene Daten darstellen (können), angezeigt werden.[57] Das Kriterium der untrennbaren Verbundenheit ist jedoch über den Fall Google hinaus verallgemeinerungsfähig.[58] Für Facebook gilt demnach a fortiori die DS-GVO bereits nach Art. 3 Abs. 1, da hier die Verarbeitung europäischer Daten (offenbar) durch die irische Niederlassung selbst, und nicht durch die US-amerikanische Facebook, Inc. vorgenommen wird.[59]

Trotz mannigfacher Kritik aus der Literatur,[60] die hierin teilweise einen ungerechtfertigten Konzernmalus erkennen will,[61] ist der Entscheidung, welche der EuGH in der Sache *Weltimmo* nochmals bestätigte,[62] letztlich zuzustimmen.[63] Zwar kann eine rein wirtschaftliche Verbindung zwischen den Tätigkeiten nicht genügen. Wenn jedoch die Datenverarbeitung, erfolgt sie auch durch ein rechtlich selbständiges Unternehmen, faktisch untrennbar mit der Aktivität der Niederlassung verbunden ist, etwa weil die Aktivität der Niederlassung, soweit sie für den Endkunden nach außen in Erscheinung tritt, gerade immer oder typischerweise mit der Verarbeitung personenbezogener Daten einhergeht, so kann in der Tat bereits nach dem Wortlaut von einer Verarbeitung „im Rahmen" der Tätigkeit der Niederlassung gesprochen werden. Sonst hätte der EU-Gesetzgeber eine Verarbeitung „durch" die EU-Niederlassung fordern müssen.[64] Die teleologischen Erwägungen geben dann nach hier vertretener Auffassung den Ausschlag für die Erfüllung von Art. 3 Abs. 1 DS-GVO. Zwar überzeugt das teleologische Argument des EuGH nicht vollends, da die DS-GVO nicht nur dem Schutz personenbezogener Daten, sondern eben auch dem freien Datenverkehr zwischen den Mitgliedstaaten dient.[65] Allerdings steht bei den fraglichen Konstellationen regelmäßig gerade kein Verkehr zwischen den Mitgliedstaaten, sondern aus der EU hinaus in Rede, sodass dem Datenschutz insofern Vorrang zukommen dürfte. Zu der vom EuGH gegebenen teleologischen Begründung tritt als weiteres Argument hinzu, dass bei einer untrenn-

[55] EuGH, Urt. v. 13.5.2014 – Rs. C-131/12 (*Google Spain*) – Rn. 52 f.
[56] EuGH, Urt. v. 13.5.2014 – Rs. C-131/12 (*Google Spain*) – Rn. 56.
[57] EuGH, Urt. v. 13.5.2014 – Rs. C-131/12 (*Google Spain*) – Rn. 57.
[58] *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 58.
[59] *Beyvers/Herbrich*, ZD 2014, 558 (561).
[60] *Ziebarth*, ZD 2014, 394 (395); *Voigt*, ZD 2014, 15 (17); *Beyvers/Herbrich*, ZD 2014, 558 (561); *Pauly/Ritzer/Geppert*, ZD 2013, 423 (425).
[61] *Arning/Moos/Schefzig*, CR 2014, 447 (450).
[62] EuGH, Urt. v. 1.10.2015 – Rs. C-230/14 (*Weltimmo*) – Rn. 37.
[63] Im Ergebnis ebenso *Kühling*, EuZW 2014, 527.
[64] So auch EuGH, Urt. v. 13.5.2014 – Rs. C-131/12 (*Google Spain*) – Rn. 52; *Kühling*, EuZW 2014, 527 (528).
[65] Vgl. auch *Beyvers/Herbrich*, ZD 2014, 558 (561).

baren Verbundenheit der beiden Tätigkeiten jedenfalls mittelbar die ökonomischen Vorteile einer EU-Niederlassung durch den Verarbeiter genutzt werden; dann sollten jedoch auch die Rahmenbedingungen dieser Rechtsordnung in Form der DS-GVO Geltung beanspruchen dürfen, um *regulatory arbitrage*[66] zu verhindern und Wettbewerbsgleichheit herzustellen.[67] Dass die Niederlassung über die Einhaltung datenschutzrechtlicher Pflichten gegebenenfalls nicht selbst entscheiden kann, ist nicht relevant, da insofern nur der Verantwortliche Adressat ist, welcher von der Niederlassung selbst verschieden sein kann.[68]

Zwar dürfte dieser Streit wegen des nunmehr in Art. 3 Abs. 2 DS-GVO verankerten Marktortprinzips, das in der DSRL fehlte, durch die Entscheidung *Google Spain* jedoch bereits partiell verwirklicht wurde,[69] an Relevanz verlieren.[70] Sofern Art. 3 Abs. 2 DS-GVO greift, gelten in der Tat die teleologischen Erwägungen nur noch in abgeschwächter Form.[71] Nichtsdestoweniger ist zu konstatieren, dass eine Verarbeitung im Rahmen der Tätigkeit der EU-Niederlassung erfolgt, wenn die Verarbeitung mit dieser Tätigkeit faktisch untrennbar verbunden ist.

b) Art. 3 Abs. 2 DS-GVO: Marktortprinzip

Das auch sonst im Marktrecht weitestgehend geltende Marktortprinzip[72] hat mit Art. 3 Abs. 2 DS-GVO nun auch in das europäische Datenschutzrecht Einzug gehalten.[73] Danach gilt die DS-GVO auch dann, wenn die Datenverarbeitung nicht im Rahmen der Tätigkeit einer EU-Niederlassung erfolgt, sofern entweder (lit. a) ein spezifisches Marktangebot in der Union erbracht oder

---

[66] Dazu grundlegend *Fleischer*, 89 Texas Law Review 2010, 227.

[67] *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 20; *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 4.

[68] *Karg*, ZD 2013, 371 (374); *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 52; *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 35.

[69] *Kühling*, EuZW 2014, 527 (528).

[70] Vgl. *Borges* in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz, 3. Aufl. 2019, Teil 1 Kap. 3 Rn. 87; *Thon*, RabelsZ 84 (2020), 24 (33).

[71] Vgl. *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 59; weitergehend *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 30, der Art. 3 Abs. 1 DS-GVO in diesen Fällen gar nicht mehr für anwendbar hält.

[72] Siehe nur Art. 6 Abs. 1 und 3 der Verordnung (EG) Nr. 864/2007 des Europäischen Parlaments und des Rates vom 11. Juli 2007 über das auf außervertragliche Schuldverhältnisse anzuwendende Recht (Rom II), ABl. 2007 L 199/40; *Engel*, Internationales Kapitalmarktdeliktsrecht, 2019, 110, 168 ff. und 282 ff.; *Drexl*, in: MüKo, BGB, 7. Aufl. 2018, Internationales Wirtschaftsrecht Teil 9. Internationales Wettbewerbs- und Kartellrecht, Internationales Lauterkeitsrecht Rn. 2; *Maier*, Marktortanknüpfung im internationalen Kartelldeliktsrecht, 2011; *Kamann/Miller*, NZKart 2016, 405 (410).

[73] Vgl. kontrastiv Art. 4 Abs. 1 lit. c DSRL; früh dafür bereits *Hoeren*, NJW 1998, 2849 (2851).

(lit. b) das Verhalten natürlicher Personen in der Union beobachtet wird. Voraussetzung nach dem Wortlaut von Art. 3 Abs. 2 DS-GVO ist jeweils, dass sich die betroffenen Personen in der Union befinden. Damit hat der Gesetzgeber auch hier auf das Erfordernis einer Unionsbürgerschaft, oder auch nur eines längerfristigen Aufenthalts in der EU, bewusst verzichtet.[74] Dies setzt konsequent den Inhalt des zweiten und 14. Erwägungsgrunds der DS-GVO um, wonach das Datenschutzgrundrecht unabhängig von Staatsbürgerschaft oder (gewöhnlichem) Aufenthaltsort geschützt werden soll.[75]

aa) Art. 3 Abs. 2 lit. a DS-GVO: Marktangebot

Nach Art. 3 Abs. 2 lit. a DS-GVO vermittelt ein Marktangebot in der EU die Anwendbarkeit der DS-GVO. Dafür genügt auch eine *invitatio ad offerendum*, wie sie bei den meisten Onlineangeboten anzutreffen sein dürfte.[76] Genauer muss die Datenverarbeitung im Zusammenhang damit stehen, in der EU betroffenen Personen[77] Waren oder Dienstleistungen anzubieten, „unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist." Damit stellt die DS-GVO klar, dass ihre Anwendbarkeit nicht davon abhängt, ob eine monetäre oder eine datenbasierte Gegenleistung – oder überhaupt eine Gegenleistung – von den betroffenen Personen erbracht wird. Die Parallelen zu Art. 3 Abs. 1 DIDD-Richtlinie[78] sind augenfällig, jedoch hat die entsprechende Passage der DS-GVO, die schon ursprünglich lediglich als objektives Anwendungskriterium ausgearbeitet war und nicht von einer Gegenleistung durch die Überlassung von Daten spricht,[79] keine auch nur im Ansatz vergleichbare Diskussion wie die Passage in der DIDD-Richtlinie ausgelöst.[80] Jedenfalls lässt sich festhalten, dass auch die Fälle, in denen Daten als Zahlungsmittel verwen-

[74] *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 64; *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 40 f.; *Thon*, RabelsZ 84 (2020), 24 (36).

[75] *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 64.

[76] *Uecker*, ZD 2019, 67 (68 f.); *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 66; *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 50.

[77] Damit fällt das Angebot lediglich gegenüber juristischen Personen (z. B. Cloud-Betreiber gegenüber AG) nicht unter Art. 3 Abs. 2 lit. a DS-GVO, siehe *Roßnagel/Richter/Nebel* ZD 2013, 103 (104 Fn. 11).

[78] Richtlinie (EU) 2019/770 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen, ABl. 2019 L 136/1.

[79] Anders Art. 3 Abs. 1 des Kommissionsentwurfs zur DIDD-Richtlinie: *Europäische Kommission*, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM(2015) 634 final; dazu *Metzger*, AcP 216 (2016), 817 (819 ff.); *Wendehorst/Graf von Westphalen*, NJW 2016, 3745; *Specht*, JZ 2017, 763 (763 f.); *Hacker*, ZfPW 2019, 148 (157 ff.); *Metzger et al.*, 9 JIPITEC 2018, 90 Rn. 12 ff.

[80] Siehe zu Art. 3 Abs. 1 DIDD-Richtlinie nur *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen);

det werden, unproblematisch in den Anwendungsbereich von Art. 3 Abs. 2 lit. a DS-GVO fallen, wenn die übrigen Voraussetzungen erfüllt sind.[81]

(1) Dienstleistung oder Ware

Dafür muss zunächst eine Dienstleistung oder Ware überhaupt angeboten werden. Dies ist regelmäßig unproblematisch. Zwar vermengt das Internet der Dinge die Kategorien von Dienstleistung und Ware zunehmend. Aber diese Hybrideigenschaft führt nicht zur Verneinung der Anwendbarkeit, da ausreichend ist, dass jedenfalls eine der beiden Alternativen dem Schwerpunkt nach erfüllt ist. Da sich die Rechtsfolgen insoweit hinsichtlich der Anwendbarkeit der DS-GVO nicht unterscheiden, kann eine Abgrenzung regelmäßig dahinstehen.[82]

Etwas weniger evident ist wiederum das Angebot im Falle von dezentralen Netzwerken wie etwa von offenen Blockchains. Hier dürfte die Verarbeitung von Daten auf einer Blockchain, die zu einem Transfer von kryptographisch gesicherten privaten Zahlungseinheiten (*coins*) führt, das maßgebliche Dienstleistungsangebot darstellen.[83]

(2) Spezifisches Angebot

Es genügt jedoch nicht ein beliebiges Angebot, vielmehr muss dieses spezifisch auf die EU oder einzelne Mitgliedstaaten ausgerichtet sein.[84] Nach dem 23. Erwägungsgrund der DS-GVO muss der Verantwortliche (oder Auftragsverarbeiter) offensichtlich beabsichtigen, Kunden in zumindest einem Mitgliedstaat anzusprechen. Diese Absicht muss sich objektiv in einem klar nachweisbaren Bezug zu dem Mitgliedstaat manifestieren. Der Erwägungsgrund zählt eine Reihe von Anhaltspunkten auf, die nicht genügen sollen: „die bloße Zugänglichkeit der Website des Verantwortlichen, des Auftragsverarbeiters oder eines Vermittlers in der Union, einer E-Mail-Adresse oder anderer Kontaktdaten oder die Verwendung einer Sprache, die in dem Drittland, in dem der Verantwortliche niedergelassen ist, allgemein gebräuchlich ist." All diesen Kriterien ist gemein, dass sie gerade nicht für einen spezifischen Bezug zu einem Mitgliedstaat sprechen, sondern zunächst lediglich Ausdruck eines globalen Angebots

Metzger, JZ 2019, 577 (579); *Staudenmayer*, NJW 2019, 2497 (2498); *Spindler/Sein*, MMR 2019, 415 (418).

[81] *Kühling*, EuZW 2014, 527 (529); *Plath*, in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 3 DSGVO Rn. 24; *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 49; *Thon*, RabelsZ 84 (2020), 24 (37).

[82] *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 78.

[83] *Buocz*, *et al.*, 35 Computer Law & Security Review 2019, 182 (191); *Hacker/Lianos/Dimitropoulos/Eich*, in: *Hacker/Lianos/Dimitropoulos/Eich* (Hrsg.), Regulating Blockchain, 2019, 1 (15); siehe auch *Berberich/Steiner*, 2 European Data Protection Law Review 2016, 422 (423).

[84] *Lüttringhaus*, ZVglRWiss 117 (2018), 50 (63); *Thon*, RabelsZ 84 (2020), 24 (35).

an alle Märkte sind, aus denen etwa die Produktwebseite aufgerufen werden kann. Nach dem Willen des Verordnungsgeber ist vielmehr eine Gesamtwürdigung anzustellen, bei der folgende Punkte für einen spezifischen Bezug zu einem Mitgliedstaat sprechen können: „die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern, die sich in der Union befinden".

Ein klarer Fall liegt daher vor, wenn eine Webseite auf Deutsch verfasst ist und auch über diese Produkte erworben oder Dienstleistungen genutzt werden können.[85] Dies ist bei allen großen, international operierenden Internetfirmen (z. B. GAFAM) der Fall. Schwieriger zu beurteilen sind Fälle, in denen lediglich eine englische Webseite existiert und aufgrund einer Zahlung mit Daten („kostenloser" Online-Währungsrechner), oder der Inexistenz einer Gegenleistung (Nutzung einer offenen Blockchain mittels *lightweight node*[86]), auch keine in der EU gebräuchliche Währung als Zahlungsmittel angegeben ist. Legt man den 23. Erwägungsgrund zu Grunde, so dürfte in diesem Fall eine offensichtliche Absicht der Kundenansprache in einem EU-Mitgliedstaat zumindest äußerst fraglich, im Zweifel eher abzulehnen sein.[87]

Denkbar ist zwar, dass auch ein derartiges globales, nicht spezifisch auf einen Mitgliedstaat der EU ausgerichtetes Angebot genügt, wenn Angebote zumindest aus einem Mitgliedstaat abgerufen werden können.[88] Immerhin wäre sonst derjenige, der seine Waren oder Dienstleistungen nur in der EU anbietet, schlechter gestellt als ein globaler Anbieter, der aber faktisch genauso den EU-Markt bedient. Ferner ist zu berücksichtigen, dass das Kriterium der offensichtlichen Absicht nur im 23. Erwägungsgrund zu finden ist und in Art. 3 Abs. 2 lit. a DS-GVO keinen Niederschlag gefunden hat. Daher stünde auch der Wortlaut einer solchen Auslegung nicht notwendig im Wege.

Nach hier vertretener Auffassung ist jedoch auf dem Kriterium der spezifischen Ausrichtung auf den Markt eines Mitgliedstaats zu beharren.[89] Das Marktortprinzip kann demnach gerade auch als Prinzip der Begrenzung der

---

[85] *Plath*, in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 3 DSGVO Rn. 21.

[86] Bei Bitcoin ergibt sich allerdings aus den verschiedenen Sprachfassungen der Webseite https://bitcoin.org eine spezifische Adressierung von Mitgliedstaaten der EU, u. a. auch von Deutschland (https://bitcoin.org/de/, zuletzt abgerufen am 13.6.2019); siehe auch *Buocz, et al.*, 35 Computer Law & Security Review 2019, 182 (192).

[87] Ebenso für soziale Netzwerke *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 111; für *Amazon China Lüttringhaus*, ZVglRWiss 117 (2018), 50 (63 f.).

[88] So OLG Hamburg, NJW-RR 2011, 1611 (1612) für die Anwendbarkeit des BDSG aF; für die DS-GVO *Plath*, in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 3 DSGVO Rn. 23 (wenn ein Vertrag zustande kommt); *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 50 (bei explizit weltweitem Angebot).

[89] *Spindler*, GRUR 2013, 996 (1003); *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 81, 87; *Plath*, in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 3 DSGVO Rn. 21; *Borges* in: Forgó/Helfrich/Schneider, Betrieblicher Datenschutz,

zu beachtenden Rechtsordnungen verstanden werden: Nur die Regeln desjenigen Markts, auf den sich ein Anbieter aktiv einstellt, müssen von ihm beachtet werden.[90] Andernfalls droht in der Tat eine innovationsfeindliche Parallelität von (sich potenziell widersprechenden) Rechtsgeboten bei globaler Diensterbringung, die hohe, mitunter gar prohibitive Rechtsinformationskosten mit sich bringen.[91] Dies geht gerade zulasten von kleinen und mittleren Unternehmen mit begrenzten Ressourcen für rechtliche Expertise.[92] Daher greift Art. 3 Abs. 2 lit. a DS-GVO nur dann, wenn Hinweise darauf bestehen, dass der EU-Markt bewusst bedient wird (z. B. Nutzung eines Internetreferenzierungsdienstes für die EU;[93] personalisierte Werbung für Nutzer, deren Aufenthalt in der EU mittels Geo-Lokalisierung der IP-Adresse ermittelt wurde[94]).

Die Problematik wird rein praktisch freilich dadurch abgemildert, dass sie insbesondere für Fälle relevant ist, in den nicht mit einer monetären Währung (die zumeist EU-spezifisch sein dürfte), sondern mit Daten gezahlt wird. In diesem Fall dürfte jedoch typischerweise zumindest Art. 3 Abs. 2 lit. b DS-GVO einschlägig sein.

bb) Art. 3 Abs. 2 lit. b DS-GVO: Verhaltensbeobachtung

Die datenschutzrechtliche Spiegelseite des aktiven Marktangebots stellt die Verhaltensbeobachtung nach Art. 3 Abs. 2 lit. b DS-GVO dar, die jedenfalls im Rahmen der digitalen Wirtschaft typischerweise mittelfristig auch auf ein Produktangebot abzielt. Insofern handelt es sich nicht um eine Durchbrechung, sondern eine konsequente Fortschreibung des Marktortprinzips unter den Bedingungen der digitalen Wirtschaft.[95] Lediglich wenn keinerlei Produktangebot intendiert ist, wird das Marktortprinzip verlassen; diese (aus der Perspektive des Marktortprinzips) falsch positiv erfassten Fälle sind jedoch hinzunehmen, da es im umgekehrten Fall zu einer wohl deutlich höheren Rate von falsch negativen Nichtanwendungsfällen käme, bei denen längerfristig ein Angebot durchaus intendiert ist. Abgemildert wird die Problematik dadurch, dass auch in Fällen, in denen kein Angebot intendiert ist, in sachlicher Hinsicht

3. Aufl. 2019, Teil 1 Kap. 3 Rn. 144; *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 53; *Uecker*, ZD 2019, 67 (69).

[90] *Hoeren*, NJW 1998, 2849 (2851); *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 18 f.

[91] *Chen*, 25 University of Pennsylvania Journal of International Law 2004, 423 (446 f.); *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 13.

[92] *Chen*, 25 University of Pennsylvania Journal of International Law 2004, 423 (446 f.).

[93] EuGH, Urt. v. 7.12.2010 – verb. Rs. C-585/08 und C-144/09 (*Pammer*) – Rn. 81.

[94] Vgl. zu dieser Möglichkeit *Schleipfer*, DuD 2014, 318 (323); zur technischen Ebene *Poese et al.*, 41 ACM SIGCOMM Computer Communication Review 2011, 53.

[95] Vgl. *Uecker*, ZD 2019, 67 (70 f.); implizit auch *Lüttringhaus*, ZVglRWiss 117 (2018), 50 (62, 64); aA *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 23.

der Personenbezug der Daten festgestellt werden muss (dazu im nächsten Abschnitt).[96]

Die Datenverarbeitung muss, um die Anwendbarkeit nach Abs. 3 Abs. 2 lit. b DS-GVO auszulösen, im Zusammenhang mit der Beobachtung eines Verhaltens in der Union stehen. Dies erfasst insbesondere Tracking-Technologien unabhängig von ihrer genauen technologischen Implementierung.[97] Da mittlerweile fast alle Webseiten mit Cookies oder anderen Tracking-Instrumenten arbeiten, erlangt die DS-GVO durch Art. 3 Abs. 2 lit. b faktisch globale Geltung.[98] Allerdings muss ein Tracking von gewisser Dauer, über einen lediglich punktuellen Kontakt hinaus, erfolgen.[99] Unter den Voraussetzungen von Art. 27 Abs. 1 DS-GVO muss sodann ein Vertreter in der EU bestimmt werden, was die Durchsetzung des europäischen Datenschutzrechts gegenüber Unternehmen ohne eigene EU-Niederlassung erleichtert.

Insbesondere die im ersten Leitfall angesprochenen Social Plug-Ins werden damit unabhängig von der Existenz einer Niederlassung in der EU dem europäischen Datenschutzrecht unterworfen. Hierdurch wird eine Verhaltensbeobachtung von hinreichender Dauer technisch gewährleistet.[100] Insgesamt zeigt sich damit, dass die DS-GVO auf alle relevanten Konstellationen der drei Leitfälle territorial anwendbar ist.

2. Sachliche Anwendbarkeit

In sachlicher Hinsicht ist die DS-GVO anwendbar, wenn nach Art. 2 Abs. 1 DS-GVO personenbezogene Daten in spezifischer Weise verarbeitet werden (1.) und keiner der in den folgenden Absätzen geregelten Ausnahmetatbestände greift (2.).

a) Grundtatbestand: Art. 2 Abs. 1 DS-GVO

Der Grundtatbestand von Art. 2 Abs. 1 DS-GVO umfasst zwei Voraussetzungen, die kumulativ erfüllt sein müssen: personenbezogene Daten (aa)) müssen spezifisch verarbeitet werden (bb)).

---

[96] *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 61.

[97] 24. Erwägungsgrund der DS-GVO; *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 23, 91; *Uecker*, ZD 2019, 67 (69); siehe auch *Lüttringhaus*, ZVglRWiss 117 (2018), 50 (64).

[98] *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 24; kritisch *Svantesson*, 5 International Data Privacy Law 2015, 226 (232): „the proposed Regulation ‚bites off more than it can chew'"; zweifelnd auch *Thon*, RabelsZ 84 (2020), 24 (37 f.); überzeugende Einschränkung hinsichtlich der Cookie-Typen bei *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 112.

[99] *Klar*, ZD 2013, 109 (113); *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 57.

[100] *Klar*, ZD 2013, 109 (113); *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 3 DS-GVO Rn. 98; *Hornung*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 3 DS-GVO Rn. 60.

aa) Personenbezogene Daten

Das Merkmal der personenbezogenen Daten wiederum ist legaldefiniert in Art. 4 Nr. 1 DS-GVO als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen". Der Begriff der Information ist denkbar weit zu verstehen und umfasst jegliche Inhalte, die in einer Art. 4 Nr. 2 DS-GVO entsprechenden Weise verarbeitet werden können.[101]

(1) Bezug zu einer Person

Die Information muss sich zunächst überhaupt auf eine Person beziehen. Dieser Personenbezug kann eine Inhalts- (Aussage direkt zur Person), eine Zweck- (bestimmte Behandlung oder Beurteilung der Person) oder eine Ergebnisdimension (Konsequenzen für die Rechte oder Interessen der Person) aufweisen.[102] Daran fehlt es beispielsweise, wenn lediglich eine Information über einen Gegenstand, etwa die Höhe eines Berggipfels, mitgeteilt wird (Sachdaten).[103] Anders liegt es wiederum, wenn kontextbezogen der Gegenstand mit einer Person in Verbindung gebracht wird.[104] Steht etwa ein Foto eines Berges in Rede, von dem jedoch bekannt ist, dass es von einer bestimmten Person aufgenommen wurde, so ist das Inhaltselement des Personenbezugs dadurch erfüllt, dass dann bekannt ist, dass die Person an dem Ort war, von welchem aus das Foto aufgenommen wurde.[105] Dies ist für Landschaftsaufnahmen relevant, die in sozialen Medien geteilt werden. Irrelevant ist damit, ob die Information öffentlich zugänglich ist, gegebenenfalls von der betroffenen Person auch selbst verbreitet wurde, oder ob sie der Privatsphäre der Person entstammt.[106] Der abstrakte Personenbezug liegt daher bei den hier behandelten drei Leitfällen typischerweise vor.

---

[101] *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 25.

[102] EuGH, Urt. v. 20.12.2017 – Rs. C-434/16 (*Nowak*) – Rn. 35; *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 2007, 11–13.

[103] *Klar/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 DS-GVO Rn. 12; *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 21.

[104] *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 2007, 11.

[105] Vgl. *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 34; *Artikel-29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 2007, 11.

[106] *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 30.

(2) Identifizierbarkeit einer konkreten Person

Über den Bezug überhaupt auf eine Person hinaus muss jedoch noch hinzutreten, dass eine konkrete natürliche Person als Bezugspunkt identifizierbar ist.[107] Darauf liegt regelmäßig der Schwerpunkt der rechtlichen Fragestellung.

(a) Grundsätzliche Kriterien

Art. 4 Nr. 1 DS-GVO nennt eine Reihe von Kriterien, nach denen sich bemisst, ob eine Person identifizierbar ist: „[A]ls identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann". Es kommt mithin entscheidend auf die Möglichkeit an, die Person mit einer eindeutigen Referenzierung (Name, Kennnummer, Merkmalskombination) verbinden zu können (*singling out*).[108]

Damit die Referenzierung allerdings dem Schutzbereich des Datenschutzrechts unterfällt, ist einschränkend zu fordern, dass sie von einer gewissen Dauer ist und mit einer konkreten, dahinterstehenden natürlichen Person verbunden werden kann.[109] Eine Einmal-Kennung, etwa als durchlaufende Nummer in einer namenlosen Liste, reicht nicht aus, wenn aus den in der Liste enthaltenen Informationen nicht auf eine konkrete natürliche Person zurückgeschlossen werden kann. Angesichts der verschiedenen von Art. 4 Nr. 1 DS-GVO erwähnten Referenzierungen erscheint es jedoch zu eng, zu fordern, dass gerade die Verbindung mit einem Klarnamen möglich sein muss.[110] Dies zeigt sich schon daran, dass viele Klarnamen (Franz Müller) keine eineindeutige Zuordnung ermöglichen und daher andere, eineindeutige Referenzierungen (z. B. die Steueridentifikationsnummer[111]) eine deutlich bessere Identifizierung ermöglichen.[112]

---

[107] Alternativ kann die Person bereits identifiziert sein, was ein logischer Unterfall der Identifizierbarkeit ist. Zur Unterscheidung auch *Schwartz/Solove*, 86 NYU Law Review, 2011, 1814 (1877 ff.).

[108] Vgl. *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (681); *Zuiderveen Borgesius*, 32 Computer Law & Security Review 2016, 256 (260); *Artikel-29-Datenschutzgruppe*, Stellungnahme 16/2011 zur Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung, WP 188, 2011, 9; genauer unten, Text bei § 4, Fn. 175–185.

[109] Vgl. EuGH, Urt. v. 19.10.2016 – Rs. C-582/14 (*Breyer*) – Rn. 38.

[110] So aber für die DSRL *Moos/Rothkegel*, MMR 2016, 845 (846), für die DS-GVO zweifelnd (ebd., 847).

[111] *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 56.

[112] Vgl. aber *Klar/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 DS-GVO Rn. 39.

Entscheidend für den konkreten Personenbezug ist mithin, ob die Daten hinreichend anonymisiert sind.[113] Anonymisierung kann wiederum in verschiedenen Graden vorliegen gemessen daran, mit welchem Aufwand eine Person identifiziert werden kann (sog. Robustheit der Anonymisierung).[114] Ist die Anonymisierung so stark, dass technisch oder mit sonstigen Mitteln eine Person nicht mit ausreichender Wahrscheinlichkeit (re-)identifiziert werden kann, muss eine Identifizierbarkeit verneint werden.[115] Dies spielt insbesondere eine Rolle bei Trainingsdaten für maschinelles Lernen, die typischerweise anonymisiert werden, indem Namen und andere direkt identifizierende Informationen abgetrennt werden.

(aa) (Re-)Identifizierungsstrategien

Eine (Re-)Identifizierung kann grundsätzlich auf zwei Arten stattfinden.[116] Einerseits kann auf eine an einem bestimmten Ort gespeicherte direkte Identifizierungsinformation zugegriffen werden. Dies umfasst Fälle, in denen etwa Internet Service Provider Protokolle bereithalten, welche die Zuordnung einer dynamischen IP-Adresse zu einem bestimmten Anschluss, dem diese IP-Adresse zugewiesen wurde, ermöglichen.[117] Andererseits kann, ohne dass eine derartige explizite Identifizierungsinformation existiert, auf technischem Wege durch Abgleich verschiedener Daten der Kreis derjenigen Personen, auf welche bestimmte Merkmale kumulativ zutreffen, soweit reduziert werden, dass am Ende (mit einer gewissen Wahrscheinlichkeit) nur noch eine einzige Person übrigbleibt.[118] Eine solche technische Re-Identifizierung kann durch verschiedene De-Anonymisierungsstrategien erfolgen,[119] z. B. durch Zusammenführung verschiedener Daten oder Datensätze (*linkage*)[120] oder durch probabilistische Inferenz in Verbindung mit Zusatzinformationen, die ein Angreifer kennt.[121]

---

[113] Siehe den Überblick über Anonymisierungstechniken bei *Winter/Battis/Halvani*, ZD 2019, 489 (490 ff.).

[114] *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 2014, 13 ff.; *Kühling/Klar*, NJW 2013, 3611 (3613).

[115] Vgl. auch *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 55.

[116] Vgl. *Ziegenhorn*, NVwZ 2017, 216 (217).

[117] Diese Konstellation lag dem Fall *Breyer* zugrunde, dazu sogleich im nächsten Abschnitt.

[118] Siehe etwa *Sweeney*, Uniqueness of Simple Demographics in the U.S. Population, Laboratory for International Data Privacy, Working Paper LIDAP-WP4, 2000.

[119] Übersicht bei *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 2014, 13; *Ohm*, 57 UCLA Law Review 2009, 1701 (1723 ff.); siehe auch *Fluitt et al.*, 5 European Data Protection Law Review 2019, 285 (287 ff.).

[120] Siehe etwa *Sweeney*, Uniqueness of Simple Demographics in the U.S. Population, Laboratory for International Data Privacy, Working Paper LIDAP-WP4, 2000, 2 f.; *Merener*, 5 Transactions on Data Privacy 2012, 377; *Shu et al.*, 18 ACM SIGKDD Explorations Newsletter 2017, 5; *Ziegler et al.*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 9 (33).

[121] Siehe etwa *Narayanan/Shmatikov*, Proceedings of the 2008 IEEE Symposium on Security and Privacy 2008, 111; *Gambs/Killijian/Del Prado Cortez*, 80 Journal of Computer

Besonders virulent ist *linkage* etwa im Internet der Dinge: Dort werden typischerweise Datensätze aus verschiedenen Quellen bei einem Anbieter zusammengeführt, um die Produktqualität und die Qualität des laufend erbrachten Services zu verbessern.[122] Verhältnismäßig einfach kann eine Re-Identifizierung auch über lokationsbasierte Daten erfolgen,[123] die bei Daten als Gegenleistung eine erhebliche Rolle spielen.[124]

(bb) Die Rechtssache *Breyer*

Allerdings führt nicht jedes technische Mittel, das von irgendeiner Person angewandt werden kann, oder jede Zugriffsmöglichkeit auf eine explizite Identifizierungsinformation zu einer Identifizierbarkeit im Sinne der DS-GVO. Der EuGH hat in der Rechtssache *Breyer* zu den insofern identischen Vorgaben der DSRL vielmehr entschieden, dass die eingesetzten Mittel rechtmäßig sein und zudem gerade dem Verarbeiter zur Verfügung stehen müssen.[125] Unerheblich ist allerdings, ob der Verantwortlichen selbst, ohne Zugriff auf fremde Daten, alle für die Identifizierung erforderlichen Informationen in den Händen hält.[126] Vielmehr kommt es nach dem EuGH darauf an, ob es für den Verantwortlichen vernünftigerweise wahrscheinlich ist, die Mittel zu nutzen, um eine Identifizierung durchzuführen oder durchführen zu lassen. Dies ist dann nicht der Fall, wenn das Mittel rechtswidrig wäre oder einen „unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, so dass das Risiko einer Identifizierung *de facto* vernachlässigbar" erscheint.[127] Zu den rechtlich erlaubten und faktisch für den EuGH hinreichenden Mitteln gehört auch die Inanspruchnahme der Strafverfolgungsbehörden, welche auf explizite Identifizierungsinformationen zugreifen können.[128] Nach dem BGH gilt dasselbe für Behörden der Gefahrenabwehr.[129] Die Identifizierungsmög-

and System Sciences 2014, 1597; *Qian et al.*, 16 IEEE Transactions on Dependable and Secure Computing 2017, 679; *Rocher/Hendrickx/de Montjoye*, 10 Nature Communications 2019, Article 3069.

[122] *Madaan/Ahad/Sastry*, 34 Computer Law & Security Review 2018, 125 (126–128); *Mainetti/Mighali/Patrono*, IEEE International Conference on Communications (ICC) 2015, 704.

[123] *de Montjoye et al.*, 3 Scientific Reports 2013, Article 1376; *Kondor et al.*, IEEE Transactions on Big Data 2018, 1.

[124] *Matheson*, The privacy risks of compiling mobility data, MIT News (7.12.2018), https://news.mit.edu/2018/privacy-risks-mobility-data-1207.

[125] EuGH, Urt. v. 19.10.2016 – Rs. C-582/14 (*Breyer*) – Rn. 45–49; zum Rechtmäßigkeitserfordernis speziell *Kühling/Klar*, ZD 2017, 27 (28).

[126] EuGH, Urt. v. 19.10.2016 – Rs. C-582/14 (*Breyer*) – Rn. 43; zum alten Streit um die relative oder absolute Bestimmung des Personenbezugs, in dem der EuGH eine Mittelstellung eingenommen hat, siehe etwa *Kühling/Klar*, NJW 2013, 3611 (3614 f.); *Bergt*, ZD 2015, 365; *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 58–60.

[127] EuGH, Urt. v. 19.10.2016 – Rs. C-582/14 (*Breyer*) – Rn. 46.

[128] EuGH, Urt. v. 19.10.2016 – Rs. C-582/14 (*Breyer*) – Rn. 47.

[129] BGH NJW 2017, 2416 Rn. 26 – Breyer. Beide Gerichte, EuGH und BGH, gehen im

lichkeit muss nur abstrakt bestehen und, bei gegebenem Anlass, hinreichend wahrscheinlich sein.[130]

(cc) Der 26. Erwägungsgrund der DS-GVO: Illegale Re-Identifizierung

Diese Kriterien finden sich auch im 26. Erwägungsgrund der DS-GVO, der sich mit pseudonymen Informationen beschäftigt. Bei pseudonym gespeicherten Informationen werden einzelne identifizierende Merkmale ausgetauscht, z. B. von den übrigen Informationen abgetrennt und separat aufbewahrt, sodass nur derjenige, der über die Zuordnungsregel verfügt, eine direkte Identifizierung vorzunehmen vermag.[131] Dazu konstatiert der 26. Erwägungsgrund: „Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren […]. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind."

Übrigen dem Wortlaut der Entscheidungen nach nicht zwingend davon aus, dass die Identifizierungsinformationen dem Verantwortlichen selbst zur Verfügung gestellt werden müssen, siehe EuGH, Urt. v. 19.10.2016 – Rs. C-582/14 (*Breyer*) – Rn. 49 aE: „bestimmen zu lassen"; BGH NJW 2017, 2416 Rn. 26 aE – Breyer; *Richter*, EuZW 2016, 912 (913). Dies ist allerdings richtigerweise zu fordern (so im Ergebnis auch GA Campos Sánchez-Bordona, Schlussanträge v. 12.5.2016 – Rs. C-582/14 [*Breyer*] – Rn. 68 ff.; *Bierekoven*, NJW 2017, 2420 [2421]; *Kipker/Kubis*, MMR 2017, 608 [609]; *Richter*, EuZW 2016, 912 (913)), denn es ist nicht einsichtig, warum der Personenbezug davon abhängen sollte, dass gerade der Verantwortliche eine Zusammenführung bei einer Behörde veranlasst hat, ohne dass er selbst letztlich Kenntnis von der Identität der Person erhält. Der Umweg über die Behörde wäre dann gar nicht notwendig: Es müsste dann ausreichen, dass der Internet Service Provider selbst die Identifizierung vornehmen kann (allenfalls auf Veranlassung des Verantwortlichen), siehe *Moos/Rothkegel*, MMR 2016, 845 (845 f.). Dies entspricht auch dem Sinn und Zweck der DS-GVO: Die Betroffenenrechte richten sich jeweils gegen einen konkreten Verantwortlichen. Dann müssen auch bei diesem die datenschutzrechtlichen Risiken eintreten. Dafür wiederum ist Identifizierbarkeit grundsätzlich Voraussetzung. Allerdings ist diese Frage wegen der Möglichkeit des Verantwortlichen, Akteneinsicht bei der Behörde zu beantragen (z. B. nach § 406e StPO), jedenfalls typischerweise in der Praxis letztlich nicht relevant.

[130] *Kühling/Klar*, ZD 2017, 27 (28).

[131] Vgl. Art. 4 Nr. 5 DS-GVO; technisch genauer *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 2014, 24 ff.; *Limniotis/Hansen*, Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation, ENISA Report, 2018, 9, 19 ff.; siehe auch *Roßnagel*, ZD 2018, 243 (243).

Einzig nicht erwähnt ist mithin die Einschränkung, dass die verwendeten Mittel legal sein müssen. In der Literatur wird teilweise vertreten, dass diese in der Rechtssache *Breyer* getätigte Einschränkung übertragbar sein müsse.[132] Denn die reine Möglichkeit illegaler Identifizierung könne nicht den Anwendungsbereich des Datenschutzrechts bestimmen.[133] Dafür spricht immerhin, dass die Einschränkung auf legale Mittel auch im 26. Erwägungsgrund der DSRL nicht enthalten war.

Letztlich kann die vollkommene Irrelevanz illegaler Re-Identifikation jedoch nicht überzeugen. Zwar ist das, auch grundrechtlich geschützte, Interesse der Verantwortlichen an einer Minimierung des Eingriffs in die unternehmerische Freiheit zu berücksichtigen. Die Anwendbarkeit des Datenschutzrechts würde ins Uferlose wachsen, wenn *jegliche* Möglichkeit des Einsatzes illegaler Strategien für die Identifizierung relevant würde.[134] Ferner bestünden dann kaum Anreize, überhaupt aus Datenschutzgründen eine Anonymisierung vorzunehmen.[135] Aus teleologischer Perspektive ist jedoch entscheidend, dass betroffene Personen bei illegaler-Re-Identifizierung typischerweise besonders des Schutzes der DS-GVO dürfen und es daher wertungswidersprüchlich wäre, gerade diese Fälle vom Anwendungsbereich auszunehmen.[136] Wenn eine Identifikation mit illegalen Mitteln *möglich* ist, so muss dieses Risiko daher im Rahmen eines risikobasierten Ansatzes, entgegen den Ausführungen in der Rechtssache *Breyer*,[137] bei der Wahrscheinlichkeit der Re-Identifizierung berücksichtigt werden.[138] Zwar wird die Wahrscheinlichkeit des Einsatzes illegaler Mittel regelmäßig geringer, aber eben nicht gleich null sein.[139] Definitiv wird man eine illegale Identifizierung hingegen dann berücksichtigen müssen, wenn sie tatsächlich erfolgt und die Person damit identifiziert *ist*.[140]

---

[132] *Kühling/Klar*, ZD 2017, 27 (28); *Mantz/Spittka*, NJW 2016, 3582 (3583); implizit auch *Roßnagel*, ZD 2018, 243 (245); *Kring/Marosi*, K&R 2016, 773 (776); zweifelnd *Klar/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 DS-GVO Rn. 29; *Krügel*, ZD 2017, 455 (459).

[133] Übersicht über den Streitstand vor Geltungsbeginn der DS-GVO bei *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 61; gegen eine Berücksichtigung von illegaler Identifizierung etwa *Brink/Eckhardt*, ZD 2015, 205 (211); dafür etwa *Bergt*, ZD 2015, 365 (370).

[134] Vgl. *Nink/Pohle*, MMR 2015, 563 (565).

[135] *Kühling/Klar*, NJW 2013, 3611 (3613); *Nink/Pohle*, MMR 2015, 563 (565).

[136] Vgl. auch *Bergt*, ZD 2015, 365 (370); *Klar/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 DS-GVO Rn. 29; *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 64; *Hacker*, A Legal Framework for AI Training Data, 13 Law, Innovation and Technology (im Erscheinen), https://ssrn.com/abstract=3556598, III.1.a)ii.

[137] EuGH, Urt. v. 19.10.2016 – Rs. C-582/14 (*Breyer*) – Rn. 46; *Purtova*, 10 Law, Innovation and Technology 2018, 40 (64).

[138] *Bergt*, ZD 2015, 365 (370); siehe auch *Finck/Pallas*, They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data Under the GDPR, International Data Privacy Law (im Erscheinen), https://ssrn.com/abstract=3462948, 15 f.

[139] *Purtova*, 10 Law, Innovation and Technology 2018, 40 (65).

[140] So auch *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 64; *Brink/Eckhardt*, ZD 2015, 205 (211).

(dd) Folgerungen

Zu beachten ist also immer die Alternativität von technischer Re-Identifizierung einerseits und Zugriff auf (indirekt) identifizierende Informationen andererseits. Zwar können avancierte Anonymisierungsverfahren (wie etwa *differential privacy*[141] oder *k-anonimity*[142]) eine technische Re-Identifizierung erheblich erschweren und fast unmöglich machen.[143] Grundlage dieser Verfahren ist jeweils, dass der gesamte Datensatz bei einer Verwahrungspartei liegt und der jeweilige Verantwortliche nur auf einzelne Elemente oder veränderte Versionen des Datensatzes zugreifen darf, aus denen (mit hinreichender Wahrscheinlichkeit) eine Re-Identifizierung der betroffenen Personen nicht möglich ist.[144] Allerdings besteht bei diesem Verfahren das Problem, dass der gesamte (Original-)Datensatz, der typischerweise eine Re-Identifizierung ermöglichen dürfte, bei der Verwahrungspartei vorliegt. Auch wenn eine technische Re-Identifizierung daher fernliegt, so ist nach dem EuGH zusätzlich zu berücksichtigen, dass der Verantwortliche möglicherweise mit rechtlichen Mitteln auf den Originaldatensatz zugreifen kann, solange dieser noch existiert. Dies ist eine Frage der Risikoabwägung im Einzelfall,[145] bei der jedoch wiederum die vom EuGH äußerst niedrig angesetzte Hürde für die hinreichende Wahrscheinlichkeit der Inanspruchnahme von rechtlichen Mitteln des Zugriffs zu beachten ist.

Demnach können insbesondere größere Datenmengen, auch wenn sie anonymisiert sind,[146] wegen der technischen Re-Identifizierungsmöglichkeiten oder der Zugriffsmöglichkeit auf (indirekt) identifizierende Informationen mit personenbezogenen Daten bestückt sein. Dies gilt auch für Trainingsdaten für maschinelles Lernen.[147] Vorzunehmen ist nach *Breyer* eine Risikoanalyse, in der anhand des potenziellen Aufwands für die Re-Identifizierung danach gefragt wird, ob das Risiko der indirekten Identifizierung vernachlässigbar ist.[148]

---

[141] *Dwork*, in: van Tilborg/Jajodia (Hrsg.), Encyclopedia of Cryptography and Security, 2011, 338.

[142] *Sweeney*, 10 International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 2002, 557.

[143] Für einen Überblick siehe *de Montjoye et al.*, 5 Nature Scientific Data 2018, 180286 (1, 3–5); *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 2014, 17 ff.

[144] Siehe nochmals *de Montjoye et al.*, 5 Nature Scientific Data 2018, 180286 (1, 3–5).

[145] Ebenso im Ergebnis *Roßnagel*, ZD 2018, 243 (244).

[146] Dies setzt voraus, dass etwaige Abgleichtabellen zwischen numerischer Identifikation und Klarnamen vom Verantwortlichen vernichtet wurden oder jedenfalls bei ihm nicht vorliegen, siehe *Artikel-29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 2014, 10 f.

[147] Siehe *Ostveen*, 6 International Data Privacy Law 2016, 299 (307); ausführlich *Hacker*, A Legal Framework for AI Training Data, 13 Law, Innovation and Technology (im Erscheinen), https://ssrn.com/abstract=3556598, V.2.b)i.

[148] Vgl. nochmals EuGH, Urt. v. 19.10.2016 – Rs. C-582/14 (*Breyer*) – Rn. 46; siehe auch *Nink/Pohle*, MMR 2015, 563 (565); *Kühling/Klar*, NJW 2013, 3611 (3613); *Klar/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 DS-GVO Rn. 22; *Arning/*

Dabei müssen auch normative Kriterien einfließen:[149] Je sensitiver die enthaltenen Informationen bzw. generell je höher die datenschutzrechtlichen Risiken sind, desto weniger ist das Risiko der Re-Identifizierung vernachlässigbar.[150] Dies gebietet eine auf Sinn und Zweck des Datenschutzrechts ausgerichtete Interpretation. Denn gerade die potenzielle Verwirklichung von datenschutzrechtsspezifischen Risiken (dazu oben, § 3 B.II.) erfordert die Anwendbarkeit der DS-GVO. Hier zeigt sich zum ersten Mal in aller Deutlichkeit der risikobasierte Ansatz des modernen Datenschutzrechts.[151] Danach dürfte die Risikoanalyse z. B. zulasten des Verantwortlichen ausfallen, wenn Fotos von Gesichtern verwendet werden, um auf maschinellem Lernen basierende Modelle der Gesichtserkennung zu trainieren.[152]

Fraglich kann dann einzig weiterhin sein, ob die potenziell vom Verantwortlichen anwendbaren Strategien rechtswidrig wären. Dies kann insbesondere deshalb der Fall sein, weil sie in der Konsequenz zur Herstellung eines Personenbezugs genutzt werden und daher zumindest in der letzten Stufe des technischen Re-Identifizierungsverfahrens die DS-GVO anwendbar ist.[153] Mangels Einwilligung der betroffenen Person kommt es zur Beurteilung der Rechtmäßigkeit der Re-Identifizierung darauf an, ob diese im Einzelfall durch eine andere Rechtsgrundlage in Art. 6 Abs. 1 DS-GVO gedeckt wäre. Insbesondere bei der Verhinderung von Cyber-Kriminalität dürfte dies regelmäßig der Fall sein.[154]

(b) Anwendung auf die drei Leitfälle

Diese Kriterien lassen sich zwar auf eine Vielzahl von Fällen anwenden, liefern jedoch aufgrund der offenen Struktur der Risikoabwägung und der Frage der

---

Rothkegel, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 4 DS-GVO Rn. 31; *Krügel*, ZD 2017, 455 (459).

[149] Der EuGH spricht zwar nur davon, dass das Risiko „*de facto*" vernachlässigbar sein müsse (§ 4, Fn. 127); jedoch enthält jedes Urteil über die Vernachlässigbarkeit notwendig eine normative Dimension, da insofern keine harten quantitativen Grenzen angebbar sind.

[150] So auch *Klar/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 DS-GVO Rn. 22; *Herbst*, NVwZ 2016, 902 (905); LG Berlin ZD 2013, 618 (620); aA *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 15.

[151] Dazu bereits oben, Text bei § 1, Fn. 82 f.

[152] Vgl. auch den 51. Erwägungsgrund der DS-GVO; zum Beispiel instruktiv *NBC News*, Facial Recognition's ‚Dirty Little Secret': Millions of Online Photos Scraped Without Consent, Communications of the ACM (15.3.2019), https://cacm.acm.org/news/235455-facial-recognitions-dirty-little-secret-millions-of-online-photos-scraped-without-consent/fulltext; *Hill*, The Secretive Company That Might End Privacy as We Know It, New York Times (18.1.2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html; zur Technologie bereits oben, § 2, Fn. 59.

[153] Darin liegt auch keine Zirkularität der Form, dass die DS-GVO anwendbar ist, wenn und weil die DS-GVO anwendbar ist, da es um zwei verschiedene Verarbeitungsformen geht: einerseits um die Erhebung von Nutzerdaten und andererseits um Re-Identifizierung.

[154] Vgl. 49. Erwägungsgrund DS-GVO; EuGH, Urt. v. 19.10.2016 – Rs. C-582/14 (*Breyer*) – Rn. 60.

Rechtmäßigkeit von technischen De-Anonymisierungsverfahren häufig kein eindeutiges Ergebnis, was die drei Leitfälle im Folgenden zeigen.

(aa) Datenweiterleitung an Dritte (personalisierte Werbung)

In der ersten Fallgruppe werden Daten an ein Drittunternehmen zu Werbezwecken weitergeleitet. Sofern diese Daten Klarnamen oder andere Informationen beinhalten, mit welcher konkrete natürliche Personen eindeutig identifiziert werden können, liegen unproblematisch personenbezogene Daten vor.

α. Namenlose Profile

Fraglich wird diese Kategorisierung jedoch dann, wenn eine Werbeplattform (sog. *ad exchange*, z. B. Googles AdX/Ad Manager) nur ein Profil ohne Namen erhält. Auf einer solchen Plattform werden, grob vereinfacht,[155] innerhalb von Millisekunden Auktionen durchgeführt, bei denen Werbetreibende angeben können, wie viel sie für eine Werbung auszugeben bereit sind für eine Person, deren Profil den übermittelten Daten entspricht.[156] Diese Daten können etwa Lokalisierungsinformationen, vergangene Suchaktivitäten und vergangene Kaufentscheidungen beinhalten, sie müssen jedoch keinesfalls notwendig den Klarnamen der Person umfassen. Hier ist mit *Breyer* danach zu fragen, ob für den jeweiligen Verantwortlichen (übermittelndes Unternehmen, Werbeplattform, Werbetreibender) eine Identifizierung hinreichend wahrscheinlich ist. Dies hängt zunächst davon ab, ob direkte Identifizierungsinformationen von Dritten (auf legalen Weg) mit überschaubarem Aufwand erlangt werden können. Da in den klassischen Werbefällen jedoch, aufgrund des Marketingkontextes, Cyberkriminalität eher fernliegt, dürfte eine Identifizierung über Strafverfolgungsbehörden oder Behörden der Gefahrenabwehr eher unwahrscheinlich sein.

Demnach käme es zweitens darauf an, ob eine technische Re-Identifizierung möglich ist. Wird ein hinreichend reichhaltiges Datenprofil übermittelt, so dürfte eine Re-Identifizierung technisch zumeist möglich sein.[157] Ob diese Maßnahme jedoch rechtmäßig ist, hängt entscheidend von der Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO ab. Abseits der Abwehr von illegalen Nutzerhand-

[155] Für eine ausführliche Beschreibung der Akteure und Funktionsweisen, siehe *Geradin/Katsifis*, European Competition Journal 2019, DOI: 10.1080/17441056.2019.1574440, 1 (9–11, 40–42).

[156] *Mansour/Muthukrishnan/Nisan*, Doubleclick Ad Exchange Auction, Working Paper, 2012, https://arxiv.org/pdf/1204.0535, 2; *Balseiro et al.*, 60 Management Science 2014, 2886 (2886); *Arning/Moos*, ZD 2014, 242 (242 f.); *Mellet/Beauvisage*, Consumption Markets & Culture 2019, 1 (11).

[157] Hinsichtlich Geodaten, siehe *Gambs/Killijian/Del Prado Cortez*, 80 Journal of Computer and System Sciences 2014, 1597; für Daten über Filmratings, siehe *Narayanan/Shmatikov*, Proceedings of the 2008 IEEE Symposium on Security and Privacy 2008, 111; für demographische Daten *Sweeney*, Uniqueness of Simple Demographics in the U.S. Population, Laboratory for International Data Privacy, Working Paper LIDAP-WP4, 2000.

lungen dürfte die Abwägung eher zugunsten der Nutzer ausfallen. Dann wäre die De-Anonymisierung illegal und in der Konsequenz grundsätzlich eher unwahrscheinlich. Unklar ist allerdings, ob es für die Legalität der Re-Identifizierung ausreichen kann, dass diese lediglich in einem kleinen Teil der Fälle rechtmäßig wäre. Das *Breyer*-Urteil lässt sich in dieser Weise verstehen, da der EuGH und der BGH nicht geprüft haben, ob im konkreten Fall die Aufdeckung der Identität des hinter einer dynamischen IP-Adresse versteckten Nutzers wirklich der Strafverfolgung dient.[158]

Vorzugswürdig scheint es demgegenüber, im Rahmen der Risikoabwägung einerseits zu berücksichtigen, dass eine legale Re-Identifizierung nur selten stattfinden wird, andererseits aber in Abwägung zu stellen, welche Daten das Datenprofil enthält. Sind dies solche, welche über die Präferenzen der Nutzer signifikant Auskunft geben (Kaufhistorie; Lokalisierungsdaten), so sind die in § 3 dargestellten Risiken besonders einschlägig und die Risikoabwägung sollte daher zugunsten der Nutzer im Sinne einer Bejahung des Personenbezugs ausfallen.

β. Machine-to-machine-Kommunikation

Im Rahmen des Internets der Dinge ist ferner zu entscheiden, wann die automatisierte Kommunikation von Sensordaten durch Geräte untereinander (*machine-to-machine communication*) einen Personenbezug aufweist. Dies dürfte typischerweise der Fall sein, da die Geräte im System mit einer eindeutigen Kennziffer identifiziert werden und somit zumindest klar ist, aus welchem lokalen Netz (zum Beispiel WLAN) die Informationen stammen.[159] Somit kann typischerweise ein Bezug zum Inhaber des Netzes als natürlicher Person hergestellt werden.[160] Dies kann lediglich dann fraglich werden, wenn mehrere Personen das jeweilige lokale Netz oder Gerät nutzen.[161] Da dies jedoch von außen zumeist kaum automatisiert feststellbar ist, muss die Praxis diese Daten regelmäßig unisono als personenbezogen behandeln.[162] Dies ist auch die Posi-

---

[158] Vgl. *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 61.

[159] *Ning*, Unit and Ubiquitous Internet of Things, 2013, 36 f.

[160] Anders dürfte dies liegen im Fall von durch Unternehmen betriebenen Netzen, es sei denn, die Kennziffer des Geräts kann einem Mitarbeiter zugeordnet werden. Vgl. auch *Klar/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 DS-GVO Rn. 14; *Grünwald/Nüßing*, MMR 2015, 378 (382); *Lüdemann*, ZD 2015, 247, (249 f.); *Kinast/Kühnl*, NJW 2014, 3057 (3058).

[161] *Bergt*, ZD 2015, 365 (370); *Klar/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 DS-GVO Rn. 35; *Zuiderveen Borgesius*, 32 Computer Law & Security Review 2016, 256 (260 f.). Allerdings kann auch eine Gruppenaussage als Tendenzaussage einen Personenbezug haben, wenn die Gruppe hinreichend klein ist, siehe *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 37. Ferner können bei IoT-Geräten auch nutzerspezifische Kennungen vergeben werden, siehe *Ning*, Unit and Ubiquitous Internet of Things, 2013, 37.

[162] *Bergt*, ZD 2015, 365 (371).

tion der Artikel-29-Datenschutzgruppe: Denn schon aufgrund der erheblichen Menge der übermittelten Daten könnten häufig De-Anonymisierungstechniken erfolgreich zur Anwendung kommen.[163] Zur Legalität dieser Verfahren gilt wiederum das soeben zu namenlosen Profilen Gesagte.[164]

(bb) Datenerhebung durch Dritte (*third-party tracking*)

Die zweite Fallgruppe von Leitfällen behandelt Tracking durch Drittunternehmen. Eine besonders typische Form ist die Sammlung von Informationen durch Social Plug-Ins. Dabei wird, wie oben ausgeführt, externer Content eines Drittunternehmens über ein iframe geladen, das in eine Webseite integriert ist. Dabei wird notwendigerweise die (dynamische) IP-Adresse des Nutzers, der auf die Webseite zugreift, abgefragt und erfasst.[165] Daher ist typischerweise nach den Erwägungen des EuGH und des BGH in der Rechtssache *Breyer* davon auszugehen, dass beim Einsatz von Social Plug-Ins personenbezogene Daten verarbeitet werden und daher die DS-GVO anwendbar ist.[166]

Ferner werden unterschiedliche Cookies durch den Inhaber des Social Plug-Ins gesetzt in Abhängigkeit davon, ob der Nutzer bei diesem Unternehmen (z. B. Facebook) registriert ist oder nicht.[167] Facebook bestreitet, dass der für Nicht-Facebook-Nutzer vergebene Cookie (datr) für Werbung verwendet wird und beruft sich auf Schutz vor illegitimen Logins durch Angreifer.[168] Andere Cookies, die bei Facebook-Nutzern durch das Social Plug-In vergeben werden, nutzt Facebook jedoch nach eigenen Angaben durchaus für personalisierte Werbung.[169]

---

[163] *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 12.

[164] Das Problem der Legalität dieser Anwendungen wird dabei durch die *Artikel-29-Datenschutzgruppe* nicht diskutiert, was verständlich ist, da die Stellungnahme zum Internet der Dinge zwei Jahre vor *Breyer* entstand.

[165] *Data Protection Commissioner*, Facebook Ireland Ltd, Report of Audit v. 21.12.2011, 81, 83; GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 1; verhindern kann dies lediglich der Inhaber der Webseite, etwa mit der 2-Klick-Lösung oder der Shariff-Lösung, siehe *Föhlisch/Pilous*, MMR 2015, 631 (635 f.); *Schleipfer*, DuD 2014, 318 (324).

[166] So auch GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 58; dasselbe gilt demnach für den durch den Cookie übermittelten Browser String (= Browser ID).

[167] *Acar et al.*, Facebook Tracking Through Social Plug-ins, Bericht, 2015, 5 ff., insbesondere 9 f.: bisweilen kein Cookie durch Like Button gesetzt, wenn vorher kein Besuch einer Facebook-Seite; *Data Protection Commissioner*, Facebook Ireland Ltd, Report of Audit v. 21.12.2011, 82; *Schleipfer*, DuD 2014, 318 (321), jeweils zum datr-Cookie beim Facebook Like Button.

[168] *Data Protection Commissioner*, Facebook Ireland Ltd, Report of Audit v. 21.12.2011, 84.

[169] So etwa der fr Cookie, siehe *Acar et al.*, Facebook Tracking Through Social Plug-ins, Bericht, 2015, 16.

Unabhängig von dieser faktischen Frage wird jedenfalls durch das Plug-In, bei bestehenden Facebook-Nutzern, vermittels eines Cookies an Facebook die Facebook ID des Nutzers gemeldet,[170] die wiederum mit einem Profil eineindeutig verknüpft ist. Darin muss, für Facebook, ein personenbezogenes Datum erblickt werden.[171] Gleiches gilt für Cookies von Google Analytics, wenn die Betroffenen Konten bei Gmail unterhalten und dort ihren Klarnahmen verwenden.[172] Etwas komplexer gestaltet sich die Lage bei Betroffenen, die nicht zu den registrierten Nutzern des Drittanbieters (Facebook, Google) gehören. Hier wird eine eindeutige ID vergeben,[173] welche für die Lebensdauer des Cookies (bei Facebook datr: zwei Jahre[174]) z. B. mit Browsermerkmalen verknüpft ist. Ob jedoch solche Cookie-IDs isoliert personenbezogene Daten darstellen, ist umstritten. Der 30. Erwägungsgrund der DS-GVO formuliert sibyllinisch, die Cookie-Kennung könne „Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren."

Nach einer Literaturansicht müssen daher noch weitere eindeutig identifizierende Informationen hinzutreten, um die Schwelle zum personenbezogenen Datum zu überschreiten.[175] Nach der Gegenauffassung soll es genügen, wenn konkrete Personen eindeutig über die Cookie-ID referenziert werden, auch wenn zum Beispiel ihr Klarname nicht bekannt ist.[176] Die letztgenannte Auffassung überzeugt aus drei Gründen. Erstens spricht der 30. Erwägungsgrund lediglich davon, dass „insbesondere" in Kombination mit anderen Informationen eine Identifizierbarkeit gegeben sein kann. Dies lässt jedoch darauf schließen, dass auch ohne das Vorliegen solcher weiteren Informationen Art. 4 Nr. 1 DS-GVO einschlägig sein kann. Auch der 26. Erwägungsgrund der DS-GVO spricht ausdrücklich davon, dass ein „Aussondern" genügt. Dies scheint auch der Lesart des EuGH zur DSRL zu entsprechen, der festhält, dass der Name einer Person, aber auch *andere* Mittel geeignet sind, eine hinreichende Identifi-

[170] So bei eingeloggten Facebook-Nutzern, welche Webseiten mit Like Button besuchen: *Acar et al.*, Facebook Tracking Through Social Plug-ins, Bericht, 2015, 14 f.

[171] *Föhlisch/Pilous*, MMR 2015, 631 (632).

[172] *Knopp*, DuD 2010, 783 (783); *Steidle/Pordesch*, DuD 2008, 324 (327).

[173] Siehe etwa *ULD Schleswig-Holstein*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 2011, 7.

[174] *Acar et al.*, Facebook Tracking Through Social Plug-ins, Bericht, 2015, 5.

[175] *Härting*, Internetrecht, 6. Aufl. 2017, Rn. 225 (allerdings einschränkend für die DS-GVO, ebd., Rn. 227); *Knopp*, DuD 2010, 783 (785); wohl auch *Klar/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 DS-GVO Rn. 36; dies erwägend auch *BVerwG*, ZD 2016, 393 Rdnr. 25.

[176] *Zuiderveen Borgesius*, 32 Computer Law & Security Review 2016, 256 (260); *Artikel-29-Datenschutzgruppe*, Stellungnahme 16/2011 zur Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung, WP 188, 2011, 9; *ULD Schleswig-Holstein*, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 2011, 15; *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 49; *Karg/Kühn*, ZD 2014, 285 (288); *Steidle/Pordesch*, DuD 2008, 324 (327).

zierung vorzunehmen, etwa die „Telefonnummer oder […] Informationen über ihr Arbeitsverhältnis oder ihre Freizeitbeschäftigungen."[177]

In teleologischer Hinsicht ist dies zweitens dann überzeugend, wenn sich die datenschutzrechtlichen Risiken verwirklichen können, auch wenn ein Klarname nicht bekannt ist. Dies ist jedoch jedenfalls dann der Fall, wenn Cookie-Kennungen genutzt werden, um über einen gewissen Zeitraum Verhalten zu beobachten und Personen gezielt (wieder) zu adressieren.[178] Werden daran anknüpfend individualisierte Interventionen veranlasst (personalisierte Werbung oder Ähnliches), so dürfte dem Nutzer typischerweise klar werden, dass er einer Beobachtung unterliegt. Die Risiken von *chilling*-Effekten, Diskriminierung[179] und der Einschränkung der Verhaltensfreiheit, welche gerade das Bundesverfassungsgericht immer wieder betont,[180] bestehen dann ebenso, als wenn die betreffende Person unter Kenntnis des Klarnamens targetiert würde.[181] Kontrollverlust kann diese Effekte verstärken, und Cookies (sowie andere Tracking-Technologien) sind plausiblerweise gerade ein zentraler Grund für dieses Gefühl.[182]

Schließlich kommt drittens hinzu, dass Cookie-IDs, im Gegensatz zu Klarnamen, besonders gut zur Identifizierung geeignet sind, da sie lediglich einmal vergeben werden.[183] Damit können Nutzer aus einer Gruppe nach geeigneten Kriterien gezielt „ausgewählt" werden (*singling out*).[184] Dasselbe gilt für andere Formen des Tracking, etwa *fingerprinting*.[185] Dass die Setzer von Drittanbietercookies oder Social Plug-Ins möglicherweise nicht allein, sondern nur gemeinsam mit dem jeweiligen Webseiteninhaber datenschutzrechtlich verantwortlich sind, steht wiederum auf einem anderen Blatt.[186]

---

[177] EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 27; allerdings ist damit noch nicht gesagt, dass eine solche Identifizierung auch tatsächlich auf Grundlage dieser Daten möglich ist.

[178] Vgl. *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 49.

[179] Siehe etwa für den Werbekontext *Sweeney*, 56 Communications of the ACM 2013, 44.

[180] Siehe oben, § 3, Fn. 138.

[181] Ebenso *Zuiderveen Borgesius*, 32 Computer Law & Security Review 2016, 256 (266 f.).

[182] *Zuiderveen Borgesius*, 32 Computer Law & Security Review 2016, 256 (267).

[183] *Zuiderveen Borgesius*, 32 Computer Law & Security Review 2016, 256 (267). Zur Nutzung desselben Anschlusses/Endgeräts durch mehrere Nutzer siehe bereits oben, Text bei § 4, Fn. 161 f.

[184] *Zuiderveen Borgesius*, 32 Computer Law & Security Review 2016, 256 (260); *Artikel-29-Datenschutzgruppe*, Stellungnahme 16/2011 zur Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung, WP 188, 2011, 9.

[185] *Artikel-29-Datenschutzgruppe*, Stellungnahme 16/2011 zur Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung, WP 188, 2011, 9; *Karg/Kühn*, ZD 2014, 285 (288); Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 580.

[186] Dazu unten, § 4 A.II.1.b)bb) und dd).

(cc) Datenerhebung bei Dritten

Die letzte Fallgruppe umfasst die Datenerhebung bei Dritten, also etwa durch IoT-Geräte bei Personen, die mit diesem Gerät in keinem primären Nutzungsverhältnis stehen. Ein Beispiel wäre etwa der Fall, in dem der Inhaber eines vernetzten Fahrzeugs einen Freund, der auf dem Beifahrersitz Platz nimmt, bittet, dem Steuerungssystem des Autos das gewünschte Ziel anzusagen. Der Personenbezug der Zielangabe kann hier fraglich sein, wenn lediglich der Zielwunsch dieser sonst nicht weiter identifizierten Begleitperson im Auto erfasst wird.

Grundsätzlich werden bei Dritten nur dann personenbezogene Daten erhoben, wenn die Identifizierbarkeit des Dritten, der gerade nicht dem Gerät zugeordnet ist, gewährleistet ist. Auch hier ist wieder eine Risikoabwägung unter Berücksichtigung der technischen Möglichkeiten und der rechtlichen Rahmenbedingungen durchzuführen. Bei Zufallsmitschnitten auditiver oder visueller Art dürfte eine Identifizierung zwar unwahrscheinlich, durch Spracherkennung und Gesichtserkennung jedoch prinzipiell möglich[187] und im Rahmen von Strafverfahren auch rechtmäßig sein. Damit dürfte es sich nach den Kriterien in der Rechtssache *Breyer* um personenbezogene Daten handeln. Dies wird gestützt durch die Erwägung, dass Sprach- und Videomitschnitte typischerweise mit nicht unerheblichen Risiken für die Privatheit der jeweils aufgenommenen Person einhergehen. Die Risikoabwägung wird daher in vielen Fällen ergeben, dass letztlich personenbezogene Daten verarbeitet werden.

(3) Ergebnis zu personenbezogenen Daten

Insgesamt lässt sich damit festhalten, dass in den hier betrachteten drei Leitfällen (Datenweiterleitung an Drittunternehmen; Datenerhebung durch Drittunternehmen; Datenerhebung bei Dritten) grundsätzlich personenbezogene Daten verarbeitet werden, auch wenn im Einzelfall keine Klarnamen unmittelbar bei der erhebenden Instanz mit den Informationen verknüpft sind. An einem klaren Personenbezug kann es insbesondere dann fehlen, wenn von einer Kennung eine ganze Reihe von Nutzern erfasst werden (zum Beispiel Nutzung eines Gerätes durch verschiedene Gäste eines Internetcafés), wenn namenlose Profile keine besonders aussagekräftigen Informationen beinhalten oder wenn Dritte nur punktuell, ohne weitere identifizierende Merkmale, erfasst werden.

(4) Regelung nicht personenbezogener Daten

Die Regelung nicht personenbezogener Daten erfolgt außerhalb der DS-GVO. Dies kann im Bereich der digitalen Wirtschaft etwa Maschinendaten be-

[187] Dies ist insbesondere der Fall, wenn es sich um regelmäßig beiläufig erfasste Personen handelt, etwa die Ehefrau des Eigentümers des vernetzten Autos oder um einen häufigen Gast in einem Smart Home.

treffen,[188] die keinen hinreichenden Bezug zu einer konkreten Einzelperson aufweisen. Auch Daten mit Bezug auf juristische Personen fallen nicht unter die DS-GVO. Schließlich endet die Anwendbarkeit der DS-GVO mit dem Tod der Person,[189] sodass auch das postmortale Datenschutzrecht außerhalb der DS-GVO entwickelt werden muss. Dafür bietet sich insbesondere das Primärrecht (Art. 7 f. GRCh) an. Ferner schließen spezifische Rechtsakte[190] sowie die ePrivacy-Gesetzgebung weitere Lücken. Verbliebene Regelungslücken müssen dann durch das allgemeine Privatrecht aufgefangen werden, sofern es um privatrechtliche Konstellationen geht. Ein Regelungsrahmen für nicht personenbezogene Trainingsdaten,[191] die für Techniken maschinellen Lernens genutzt werden, fehlt jedoch beispielsweise.[192]

Hinsichtlich der Daten mit Bezug auf juristische Personen hat der EuGH in der Rechtssache *Schecke* bereits entschieden, dass sie insoweit Art. 7 f. GRCh unterliegen, wie sie Rückschlüsse auf natürliche Personen erlauben,[193] jedenfalls soweit der Name der juristischen Person eine oder mehrere natürliche Personen bestimmt.[194] Der Anwendungsbereich des Primärrechts ist insofern weiter gespannt als jener der DS-GVO.[195]

Auf sekundärrechtlicher Ebene erfasst ferner Art. 5 Abs. 3 ePrivacy-Richtlinie gerade auch nicht personenbezogene Daten, sofern Daten aus dem Privatbereich abgeschöpft werden.[196] Denn die Vorschrift ist anwendbar auf alle „Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind", ohne insoweit zwischen personenbezogenen und nicht personenbezogenen Daten zu unterscheiden.[197] Dies ist, sofern man die ePrivacy-

---

[188] Siehe hierzu *European Commission*, Building a European Data Economy, COM(2017) 9 final, 5 ff.

[189] 27. Erwägungsgrund der DS-GVO; *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 DS-GVO Rn. 39.

[190] Erwähnt sei vor allem die Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union, ABl. 2018 L 303/59, die in Art. 4 Abs. 1 ein grundsätzliches Verbot von Datenlokalisierungsauflagen beinhaltet.

[191] Zur Frage des Personenbezugs dieser Daten oben, Text bei § 4, Fn. 147.

[192] Siehe dazu *Hacker*, A Legal Framework for AI Training Data, 13 Law, Innovation and Technology (im Erscheinen), https://ssrn.com/abstract=3556598, unter V.

[193] So lesbar EuGH, Urt. v. 9.11.2010 – Rs. C-92/09 und C-93/09 (*Schecke*) – Rn. 53 i. V. m. Rn. 52; gleiches Verständnis bei *Schantz*, in: BeckOK DatenschutzR, 28. Ed. 1.2.2019, Art. 1 DS-GVO Rn. 1; *Hornung*, MMR 2011, 127 (127); kritisch hinsichtlich dieser Verengung des persönlichen Schutzbereichs *Schneider*, DV 44 (2011), 499 (509 f.); einen Schutz juristischer Personen gänzlich ablehnend *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, 2014, 258 ff.

[194] EuGH, Urt. v. 9.11.2010 – Rs. C-92/09 und C-93/09 (*Schecke*) – Rn. 53.

[195] *Pötters*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 1 DS-GVO Rn. 23.

[196] *Artikel-29-Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, WP 171, 2010, 10; GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 107 f.; siehe auch den 24. und 25. Erwägungsgrund der ePrivacy-Richtlinie.

[197] GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 107.

Richtlinie nach Geltungsbeginn der DS-GVO für anwendbar hält, relevant für durch Cookies erhobene Daten, die im Einzelfall einmal keine personenbezogenen Daten darstellen.[198]

bb) Spezifische Verarbeitungsformen

Ferner sei der Abrundung halber erwähnt, dass die DS-GVO gem. ihrem Art. 2 Abs. 1 nur Anwendung findet, wenn personenbezogene Daten in spezifischer Form verarbeitet werden. Die Verarbeitung muss entweder ganz oder teilweise automatisiert erfolgen oder aber, sofern dies wegen rein manueller Erfassung nicht der Fall ist, die Absicht der Speicherung in einem Dateisystem umfassen.

(1) Ganz oder teilweise automatisierte Verarbeitung

Jede Verarbeitung mithilfe von elektronischen Datenverarbeitungsanlagen erfüllt den Tatbestand der (teilweise) automatisierten Verarbeitung.[199] Die Veröffentlichung von Daten im Internet ist z. B. regelmäßig mit einer jedenfalls teilweise automatisierten Verarbeitung (beim Hochladen der Informationen auf einen Server) verbunden.[200] An einer auch nur partiell automatisierten Verarbeitung fehlt es etwa beim händischen Notieren von Informationen durch einen Privatdetektiv.[201] In praktisch allen hier relevanten Fällen der Verarbeitung von Daten in der digitalen Wirtschaft dürfte dieses Kriterium jedoch erfüllt sein.

(2) Speicherung oder Speicherungsabsicht in Dateisystem

Die manuelle Verarbeitung personenbezogener Daten löst gem. Art. 2 Abs. 1 DS-GVO nur dann die Anwendbarkeit der DS-GVO aus, wenn zumindest die Absicht besteht, die Daten in einem Dateisystem zu speichern. Ein Dateisystem ist legaldefiniert in Art. 4 Nr. 6 DS-GVO als „strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird." Der EuGH entschied, dass die Strukturierungskomponente immer dann schon erfüllt sei, wenn die Daten so gespeichert werden, dass sie leicht und in für den jeweiligen Zweck tauglicher Weise wieder aufgefunden werden können.[202] Insgesamt

---

[198] Dazu ausführlich oben, § 4 A.II.2.a)aa)(2)(b)(bb).

[199] *Kühling/Raab*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 2 DS-GVO Rn. 15; siehe auch EuGH, Urt. v. 11.12.2014 – Rs. C-212/13 (*Ryneš*) – Rn. 25 zur Videoüberwachung.

[200] EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 26.

[201] Vgl. 15. Erwägungsgrund der DS-GVO; *Kühling/Raab*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 2 DS-GVO Rn. 17.

[202] EuGH, Urt. v. 10.7.2018 – Rs. C-25/17 (*Zeugen Jehovas*) – Rn. 57.

spielen diese Tatbestände jedoch in der digitalen Wirtschaft keine erkennbar relevante Rolle.

b) Ausnahmen: Art. 2 Abs. 2–3 DS-GVO

Von erheblicher Relevanz jedoch sind die Ausnahmetatbestände des Art. 2 Abs. 2–3 DS-GVO, welche die Anwendbarkeit der DS-GVO ausschließen. Besonders umstritten und auch für Belange der digitalen Wirtschaft entscheidend ist dabei die Abgrenzung des Anwendungsbereichs des Unionsrechts nach Art. 2 Abs. 2 lit. a DS-GVO (aa)). Weitere Ausnahmen bestehen etwa für persönliche oder familiäre Tätigkeiten oder die Strafverfolgung und Gefahrenabwehr (bb)).

aa) Kein Anwendungsbereich des Unionsrechts, Art. 2 Abs. 2 lit. a DS-GVO

Art. 2 Abs. 2 lit. a DS-GVO beinhaltet eine Ausnahme für Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen. Die Regelung ist zwar einerseits deklaratorisch, da sie die Kompetenzgrenzen von Art. 16 Abs. 2 AEUV widerspiegelt.[203] Andererseits ist im Detail durchaus schwer festzustellen und höchst umstritten, bei welchen Tätigkeiten der Anwendungsbereich des Unionsrechts nicht eröffnet ist. Einigkeit besteht lediglich darin, dass, wie auch der 16. Erwägungsgrund der DS-GVO festhält, Tätigkeiten mit unmittelbarer Relevanz für die nationale Sicherheit nicht erfasst sind. Diese Fallgruppe ist jedoch zugleich durch Art. 2 Abs. 2 lit. d DS-GVO vom Anwendungsbereich ausgenommen.

Besonders umstritten ist die Frage der Anwendbarkeit der DS-GVO auf rein innerstaatliche Sachverhalte. Zwar ist in vernetzten Umgebungen die Überschreitung einer EU-Binnengrenze bei der Datenverarbeitung durchaus nicht unüblich;[204] ob sie jedoch für die Anwendbarkeit der DS-GVO strikt notwendig ist, ist bislang nicht abschließend geklärt. So wird teilweise nur eine potenzielle Relevanz des Sachverhalts für den Datenverkehr zwischen den Mitgliedstaaten für erforderlich gehalten, ohne dass dieser in jedem Einzelfall tatsächlich vorliegen müsste.[205] Andere Autoren betonen demgegenüber, dass jeder Datenverarbeitungsvorgang im Einzelfall ein grenzüberschreitendes Element besitzen muss.[206]

---

[203] *Kühling/Raab*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 1a; Ingold, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 2 DS-GVO Rn. 21; zu den Kompetenzgrenzen eingehend *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 336 ff.

[204] Vgl. den fünften Erwägungsgrund der DS-GVO.

[205] *Sobotta*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 16 Rn. 32 zur insofern identischen Frage bei der Art. 3 Abs. 2 Spstr. 1 DSRL; *Roßnagel*, DuD 2017, 290 (291).

[206] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 2 DS-GVO Rn. 21.

(1) Die Fälle *Österreichischer Rundfunk* und *Lindqvist* – Argumente des EuGH und Kritik

Der EuGH hat sich in zwei frühen und grundlegenden Entscheidungen zum Datenschutzrecht der erstgenannten Position angeschlossen. Im Fall *Österreichischer Rundfunk*, der ersten überhaupt vom EuGH zur DSRL entschiedenen Rechtssache, stand eine nationale Regelung in Rede, nach der die Gehälter von hohen Beamten in Österreich einer Prüfungsbehörde mitgeteilt und veröffentlicht werden mussten.[207] Der Sachverhalt war daher, jedenfalls grundsätzlich, innerstaatlicher Natur.[208] Der EuGH entschied jedoch, entgegen der Einschätzung des Generalanwalts *Tizzano*,[209] dass die DSRL auf den Sachverhalt anwendbar ist.[210] Diese Linie bestätigte er kurz darauf, wiederum entgegen dem Vorschlag von Generalanwalt *Tizzano*,[211] in der Rechtssache *Lindqvist*,[212] in der es um die Internetveröffentlichung von Informationen über die Mitarbeiter einer schwedischen Kirchengemeinde durch eine ehrenamtliche Mitarbeiterin derselben Gemeinde ging.[213]

Die Urteile des EuGH beruhten auf vier unabhängigen, letztlich jedoch nicht überzeugenden Argumenten.[214] Hinsichtlich des Wortlauts der Richtlinie stellte der EuGH fest, dass ein grenzüberschreitendes Element nicht ausdrücklich als Voraussetzung für die Anwendbarkeit der Richtlinie genannt sei; zudem wäre die Ausnahmebestimmung für den Anwendungsbereich in Art. 3 Abs. 2 DSRL (heute im Wesentlichen Art. 2 Abs. 2 DS-GVO) anders formuliert worden, wenn jeweils ein hinreichender Zusammenhang mit der Ausübung von Grundfreiheiten (im grenzüberschreitenden Bereich) für die Anwendbarkeit notwendig wäre.[215] Dem ist jedoch entgegenzuhalten, dass Art. 3 Abs. 2 Spstr. 1 DSRL eine Ausnahme enthielt für die Verarbeitung personenbezogener Daten, wenn sie für die „Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen." Dies deckt sich mit der

---

[207] EuGH, Urt. v. 20.5.2003 – verb. Rs. C-465/00, C-138/01 und C-139/01 (*Österreichischer Rundfunk u. a.*) – Rn. 2.

[208] *Lynskey*, The Foundations of EU Data Protection Law, 2015, 51.

[209] GA *Tizzano*, Schlussanträge v. 14.11.2002 – verb. Rs. C-465/00, C-138/01 und C-139/01 (*Österreichischer Rundfunk u. a.*) – Rn. 43, 49.

[210] EuGH, Urt. v. 20.5.2003 – verb. Rs. C-465/00, C-138/01 und C-139/01 (*Österreichischer Rundfunk u. a.*) – Rn. 47.

[211] GA *Tizzano*, Schlussanträge v. 19.9.2002 – Rs. C-101/01 (*Lindqvist*) – Rn. 35.

[212] EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 48.

[213] EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 2.

[214] Ein fünftes Argument findet sich in Rn. 46 des Urteils, ist jedoch abwegig: Aus der Tatsache, dass die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung oder im öffentlichen Interesse rechtmäßig sein muss (Art. 7 lit. c und e DSRL) folgt mitnichten, dass alle Datenverarbeitungsvorgänge, die diesen Zielen dienen, auch vom Anwendungsbereich umfasst sein müssen. Dies vermengt vielmehr unzulässig Anwendungsbereich Richtlinie und Tatbestand der Zulässigkeit der Verarbeitung.

[215] EuGH, Urt. v. 20.5.2003 – verb. Rs. C-465/00, C-138/01 und C-139/01 (*Österreichischer Rundfunk u. a.*) – Rn. 43.

Formulierung in Art. 2 Abs. 2 lit. a DS-GVO. Wie gleich noch zu zeigen sein wird, macht dies jedenfalls im Grundsatz ein grenzüberschreitendes Element erforderlich, da typischerweise eben nur dann der Anwendungsbereich des Gemeinschafts- bzw. Unionsrechts eröffnet ist.[216]

Weiterhin folgerte der EuGH aus der beispielhaften Aufzählung von aus dem Anwendungsbereich ausgenommenen Tätigkeiten in Art. 3 Abs. 2 Spstr. 1 DSRL – solche nach den Titeln V und VI des EUV aF sowie Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates und die Tätigkeiten des Staates im strafrechtlichen Bereich –, dass andere nach dieser Vorschrift ausgenommene Tätigkeiten „derselben Kategorie zugeordnet werden können [müssen] (ejusdem generis)".[217] Sie müssen also diesen ausdrücklich genannten Tätigkeiten gleichgestellt sein; daher würden Tätigkeiten von Einzelpersonen nicht unter die Ausnahme nach Art. 3 Abs. 2 DSRL fallen.[218] Diese Auslegung ist jedoch bereits für die DSRL äußerst zweifelhaft, da Art. 3 Abs. 2 Spstr. 1 DSRL grundsätzlich eine Ausnahme für Tätigkeiten außerhalb des Anwendungsbereichs des Gemeinschaftsrechts vorsieht und lediglich beispielhaft und deklaratorisch einige besonders wichtige Bereiche benennt. Dass diese Leitbildcharakter für jegliche Ausnahmen haben sollen, ist gerade nicht erkennbar.[219]

Der EuGH argumentierte drittens in den genannten Fällen, dass in teleologischer Perspektive die Notwendigkeit der Feststellung eines grenzüberschreitenden Elements den Anwendungsbereich der Richtlinie ungewiss und zufällig erscheinen ließe, was ihrem Harmonisierungszweck diametral entgegenlaufe.[220] Diese Auffassung ist in der Literatur auf Zustimmung gestoßen.[221] Während sie rechtspolitisch durchaus nachvollziehbar ist, muss hierzu jedoch bemerkt werden, dass die klare tatbestandliche Voraussetzung der Eröffnung des Anwendungsbereichs des Gemeinschafts- bzw. Unionsrechts nicht dadurch überspielt werden darf, dass sie als zu vage und unsicher bezeichnet wird. Sie mag in Grenzfällen zwar durchaus zu Abgrenzungsschwierigkeiten führen; hätte man dies vermeiden wollen, hätte jedoch eine andere Formulierung gewählt werden müssen, wie dies in praktisch allen anderen Sekundärrechtsakten bei der Bestimmung des Anwendungsbereichs geschieht.[222] Es kann mithin nicht angehen, einerseits den Anwendungsbereich des Unionsrechts zur Voraussetzung zu machen, diese Voraussetzung jedoch andererseits mit dem Verweis darauf

---

[216] So auch *Classen*, 41 Common Market Law Review 2004, 1377 (1381 f.).

[217] EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 44.

[218] EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 43.

[219] Kritisch auch *Lynskey*, The Foundations of EU Data Protection Law, 2015, 54; aA *Fechner*, JZ 2004, 246 (247).

[220] EuGH, Urt. v. 20.5.2003 – verb. Rs. C-465/00, C-138/01 und C-139/01 (*Österreichischer Rundfunk u. a.*) – Rn. 42; EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 41 f.

[221] *Siemen*, EuR 2004, 306 (313); *Lynskey*, The Foundations of EU Data Protection Law, 2015, 60; implizit auch *Roßnagel*, MMR 2004, 95 (99).

[222] Siehe zum Alleinstellungscharakter der DSRL insofern *Siemen*, EuR 2004, 306 (312).

umgehend wieder außer Kraft zu setzen, dass der Anwendungsbereich schwer zu bestimmen sei. Eine derartige Argumentation bringt vielmehr das Kompetenzgefüge zwischen Union und Mitgliedstaaten, das von dem Grundsatz der begrenzten Einzelermächtigung geprägt ist, ins Wanken.

Schließlich verwies der EuGH in *Österreichischer Rundfunk* und *Lindqvist* noch darauf, dass die DSRL nach Art. 100a EGV, nunmehr Art. 114 AEUV, erlassen wurde. Diese Rechtsgrundlage zur Harmonisierung des Binnenmarkts setzt jedoch nach der Rechtsprechung des EuGH gerade nicht voraus, dass ein unmittelbarer Binnenmarktbezug in jedem einzelnen Sachverhalt besteht, der durch auf diese Kompetenzgrundlage gestützte Rechtsakte erfasst wird.[223] Daraus ergibt sich, dass Maßnahmen nach dieser Rechtsgrundlage lediglich „die Bedingungen für die Errichtung und das Funktionieren des Binnenmarktes verbessern sollen und tatsächlich dieses Ziel verfolgen müssen, indem sie zur Beseitigung von Hemmnissen für den freien Waren- oder Dienstleistungsverkehr oder aber von Wettbewerbsverzerrungen beitragen."[224]

Ob selbiges für die nunmehr für die DS-GVO herangezogene Kompetenzgrundlage, Art. 16 Abs. 2 AEUV, gilt, hat der EuGH bislang noch nicht entschieden. Da jedoch jedenfalls hinsichtlich der Regelung des freien Datenverkehrs Art. 16 Abs. 2 AEUV als *lex specialis* zu Art. 114 Abs. 1 AEUV gilt,[225] dürfte eine Übertragung der Rechtsprechung zu erwarten sein, so dass auch für auf Grundlage von Art. 16 Abs. 2 AEUV erlassene Rechtsakte nicht in jedem Fall ein grenzüberschreitendes Element Anwendungsvoraussetzung sein muss. Diese Argumentation ist in sich durchaus nachvollziehbar. Sie gibt jedoch für die Frage des Anwendungsbereichs der DSRL, und für jenen der DS-GVO, nichts her, weil damit nur feststeht, dass ganz grundsätzlich in derartiger Weise Rechtsakte ohne Bezug auf ein konkretes grenzüberschreitendes Element erlassen werden *können*. Es dürfte jedoch unstreitig sein, dass einzelne Rechtsakte dies andererseits genauso zur Voraussetzung erheben können.

(2) Der Anwendungsbereich des Unionsrechts nach der DS-GVO

Diese Diskussion wirft erneut die Frage auf, wie die Voraussetzung der Eröffnung des Anwendungsbereichs des Unionsrechts zu verstehen ist. Nach hier

---

223 EuGH, Urt. v. 20.5.2003 – verb. Rs. C-465/00, C-138/01 und C-139/01 (*Österreichischer Rundfunk u. a.*) – Rn. 41, unter Verweis auf EuGH, Urt. v. 5.10.2000 – Rs. C-376/98 (*Deutschland/Parlament und Rat*) – Rn. 85; Urt. v. 10.12.2002 – Rs. C-491/01 (*British American Tobacco [Investments] und Imperial Tobacco*) – Rn. 60; bestätigt in EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 40; kritisch *Classen*, 41 Common Market Law Review 2004, 1377 (1382).

224 EuGH, Urt. v. 10.12.2002 – Rs. C-491/01 (*British American Tobacco [Investments] und Imperial Tobacco*) – Rn. 60.

225 *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 335; *Klement*, JZ 2017, 161 (164); *Schneider*, DV 44 (2011), 499 (505); *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 16 Rn. 7; *M. Schröder*, in: Streinz, EUV/AEUV, 3. Aufl. 2018, AEUV, Art. 16 Rn. 10.

vertretener Auffassung hat sich die Antwort einerseits an den etablierten Kriterien für die Ermittlung des Anwendungsbereichs des Unionsrechts zu orientieren, muss aber andererseits die partielle Bestätigung der Rechtsprechung des EuGH durch die DS-GVO berücksichtigen.

(a) Die klassischen Kriterien der Eröffnung des Anwendungsbereichs des Unionsrechts

Zunächst ist für die Interpretation von Art. 2 Abs. 2 lit. a DS-GVO auf tradierte Kriterien der Eröffnung des Anwendungsbereichs des Unionsrechts abzustellen, die zwar im Einzelnen umstritten sind, jedoch einen weitgehend konsentierten Kern aufweisen.[226] Danach ist die Eröffnung in drei hier interessierenden Fällen zu bejahen.[227] Erstens ist der Anwendungsbereich des Unionsrechts gegeben, wenn der Sachverhalt auf unionsrechtlicher Ebene, durch Primärrecht[228] oder Sekundärrecht[229] (unter Ausblendung des Instruments, dessen Anwendbarkeit gerade festgestellt werden soll), tatbestandlich erfasst wird.[230] Zweitens hat der Vollzug von Unionsrecht dieselbe Wirkung.[231] Zudem ist jedoch nach dem EuGH drittens der Anwendungsbereich ebenfalls eröffnet, wenn (auch nur mittelbar) die tatsächliche Ausübung der Grundfreiheiten betroffen ist.[232] Zumindest dies dürfte bei in mehreren Mitgliedstaaten tätigen Datenverarbeitern regelmäßig der Fall sein.

---

[226] Siehe etwa die Übersicht bei *Epiney*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 18 Rn. 22; *von Bogdandy*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 18 Rn. 38.

[227] Vgl. GA *Tizzano*, Schlussanträge v. 19.9.2002 – Rs. C-101/01 (*Lindqvist*) – Rn. 36; *Klement*, JZ 2017, 161 (165 f.); weitergehend (abstrakte unionale Gesetzgebungskompetenz ausreichend) *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 337 f.; *von Lewinski*, DuD 2012, 564 (565); wohl auch *Brühann*, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 16 AEUV Rn. 65.

[228] Siehe etwa EuGH, Urt. v. 6.10.2009 – Rs. C-123/08 (*Wolzenburg*) – Rn. 46; dies ist jedoch dann nicht weiterführend, oder gar zirkulär, wenn die Durchführung von Unionsrecht, oder die Eröffnung von dessen Anwendungsbereich, selbst Voraussetzung für die Anwendbarkeit von Primärrecht ist, siehe etwa Art. 51 Abs. 1 S. 1 GRCh.

[229] EuGH, Urt. v. 18.3.2014 – Rs. C-628/11 (*International Jet Management*) – Rn. 53.

[230] *Kainer*, LMK 2014, 359381, unter 2; *von Bogdandy*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 18 Rn. 34.

[231] So implizit EuGH, Urt. v. 23.1.1977 – Rs. C-29/95 (*Pastoors*) – Rn. 13 ff.; ausdrücklich *Epiney*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 18 Rn. 17; wohl auch GA *Tizzano*, Schlussanträge v. 14.11.2002 – verb. Rs. C-465/00, C-138/01 und C-139/01 (*Österreichischer Rundfunk u. a.*) – Rn. 43.

[232] EuGH, Urt. v. 13.2.1985 – Rs. 293/83 (*Gravier*) – Rn. 19–25; Urt. v. 7.7.2005 – Rs. C-147/03 (*Kommission/Österreich*) – Rn. 31–35; *Epiney*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 18 Rn. 18; implizit wohl auch GA *Tizzano*, Schlussanträge v. 14.11.2002 – verb. Rs. C-465/00, C-138/01 und C-139/01 (*Österreichischer Rundfunk u. a.*) – Rn. 44 ff.

(b) Die partielle Fortgeltung der EuGH-Rechtsprechung

Bliebe man hierbei stehen, so müsste grundsätzlich die Eröffnung des Anwendungsbereichs des Unionsrechts nach diesen Kriterien in jedem Einzelfall geprüft werden. Dies würde jedoch die partielle Fortgeltung der gerade kritisierten EuGH-Rechtsprechung übersehen, welche durch die DS-GVO jedenfalls in Teilen bestätigt wurde.

(aa) Fortgeltung des Falls *Österreichischer Rundfunk*

Der EuGH schloss in der Rechtssache *Österreichischer Rundfunk* die Prüfung eines grenzüberschreitenden Elements in jedem Einzelfall gerade aus. Wie soeben gezeigt, wurde dieser Fall zwar nach hier vertretener Auffassung falsch entschieden. Dies ändert jedoch nichts an dem Umstand, dass die DS-GVO deutlich nach diesem Urteil erneut zur Bestimmung ihres Anwendungsbereichs auf den Anwendungsbereich des Unionsrechts verweist. Es muss davon ausgegangen werden, dass dem europäischen Gesetzgeber durchaus bewusst war, dass der EuGH dieses Kriterium in der Rechtssache *Österreichischer Rundfunk* wie dargestellt ausgelegt hatte.[233] Wäre eine Änderung dieser Rechtsprechung bezweckt gewesen, so wäre eine Abänderung der Vorschrift zu erwarten gewesen. Man hätte etwa die Notwendigkeit des Nachweises eines grenzüberschreitenden Elements im Einzelfall ohne Weiteres in Art. 2 Abs. 2 lit. a DS-GVO aufnehmen können.

Damit unterscheidet sich die Ausgangslage unter der Geltung der DS-GVO deutlich von derjenigen unter der DSRL. Hatte unter dieser der klare Wortlaut von Art. 3 Abs. 2 Spstr. 1 DSRL noch entscheidend gegen das Urteil des EuGH gesprochen, so lässt sich dies von Art. 2 Abs. 2 lit. a DS-GVO nicht mehr sagen. Durch die unmodifizierte Wiederholung des Kriteriums der Eröffnung des Anwendungsbereichs des Unionsrechts wird der Wortlaut der Vorschrift implizit durch die prägende Rechtsprechung der Vorgängervorschrift aufgeladen. Ferner wird in der Literatur argumentiert, dass teleologisch zu berücksichtigen sei, dass in Zeiten von Cloud Hosting und ubiquitärem Datentransfer zumindest potenziell jedes Datum auch grenzüberschreitend übermittelt wird.[234] Hinzu kommt entscheidend, dass dem EuGH in teleologischer Hinsicht durchaus dahingehend zuzustimmen ist, dass eine Anwendung der DS-GVO, die von der Notwendigkeit eines grenzüberschreitenden Elements im Einzelfall abstrahiert, effektiver und vorhersehbarer harmonisiert und insofern den freien Verkehr von Daten zwischen den Mitgliedstaaten besser ermöglicht. Das an sich fehlerhafte Urteil des EuGH wird damit durch die kritiklose Übernahme des Wortlauts der DSRL in die DS-GVO gewissermaßen (*de lege lata*) ins Recht gesetzt.

[233] Vgl. *Albrecht*, CR 2016, 88 (90).

[234] *Siemen*, EuR 2004, 306 (313); *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 315.

(bb) Keine Fortgeltung des Falls *Lindqvist*

Für die zentrale Aussage des Urteils in der Rechtssache *Lindqvist* kann dies jedoch nicht gelten. Der EuGH hatte die Möglichkeit kategorisch abgelehnt, dass Tätigkeiten von Einzelpersonen unter die Ausnahmeregelung der Nicht-Eröffnung des Anwendungsbereichs des Unionsrechts fielen. Denn der Aufzählung verschiedener, jedenfalls im Anwendungsbereich des Unionsrechts ausgenommener Bereiche wurde ein Leitbildcharakter zugesprochen, der nur auf die Verarbeitung durch staatliche Stellen passen sollte.[235]

Für die DS-GVO hingegen stellt sich diese Frage nach dem Leitbild richtigerweise schon gar nicht, da eine derartige exemplarische Aufzählung in Art. 2 Abs. 2 lit. a DS-GVO schlicht unterblieben ist. Der 16. Erwägungsgrund nennt als einziges Beispiel Tätigkeiten betreffend die nationale Sicherheit. Aus diesem Einzelbeispiel lassen sich jedoch schlechterdings keine Kriterien für die Natur der übrigen vom Anwendungsbereich der Richtlinie nach Art. 2 Abs. 2 lit. a DS-GVO ausgenommenen Tätigkeiten ableiten. Daher ist die Tätigkeit von Einzelpersonen, anders als noch unter der DSRL, keineswegs automatisch von der Ausnahme nach Art. 2 Abs. 2 lit. a DS-GVO ausgeschlossen.

(3) Folgerungen

Abschließend stellt sich daher die Frage, unter welchen Voraussetzungen eine datenverarbeitende Tätigkeit nach Art. 2 Abs. 2 lit. a DS-GVO nicht mehr vom Anwendungsbereich des Unionsrechts umfasst ist. In Betracht kommen nur rein innerstaatliche Sachverhalte, da sonst aufgrund des grenzüberschreitenden Bezugs typischerweise bereits nach den etablierten Kriterien der Anwendungsbereich des Unionsrechts eröffnet ist. Allerdings kann die DS-GVO nach den (nunmehr ins Recht gesetzten) Ausführungen in der Rechtssache *Österreichischer Rundfunk* auch in einem Einzelfall auf einen rein innerstaatlichen Sachverhalt angewandt werden.

Damit für die Ausnahme von Art. 2 Abs. 2 lit. a DS-GVO überhaupt noch ein Regelungsbereich jenseits der kompetenziell bereits nicht dem Unionsrecht zugewiesenen Bereiche wie der nationalen Sicherheit (16. Erwägungsgrund) verbleibt, müssen daher solche Sachverhalte ausgeschieden werden, die einer Konstellation entspringen, bei der nicht nur im Einzelfall, sondern im Regelfall und unter keinem Gesichtspunkt der Anwendungsbereich des Unionsrechts nach den etablierten, genannten Kriterien eröffnet ist. Dies können etwa rein innerstaatliche Sachverhalte sein, bei denen sich, anders als im Fall *Österreichischer Rundfunk*,[236] nicht einmal entfernt Berührungspunkte zu

[235] Siehe oben, Text bei § 4, Fn. 219.

[236] EuGH, Urt. v. 20.5.2003 – verb. Rs. C-465/00, C-138/01 und C-139/01 (*Österreichischer Rundfunk u. a.*) – Rn. 32–34; aA insoweit *Classen*, 41 Common Market Law Review 2004, 1377 (1382).

den Grundfreiheiten und zum Binnenmarkt konstruieren lassen.[237] Angesichts der permissiven Auslegung von Art. 114 Abs. 1 AEUV und der engen Verbindung dieser Vorschrift zu Art. 16 Abs. 2 AEUV dürfte diese Auslegung auch primärrechtskonform sein.[238] Allerdings ist nach dem in diesem Fall zur Geltung kommenden deutschen Datenschutzrecht gemäß § 1 Abs. 8 BDSG die DS-GVO auf öffentliche Stellen doch wieder anwendbar, wenngleich kraft nationalen Rechtsanwendungsbefehls. Für private Verarbeiter gilt dann jedoch rein nationales Datenschutzrecht, in Deutschland mithin das BDSG nach Maßgabe des § 1 Abs. 1 S. 2, Abs. 4 S. 2–3 BDSG sowie, zumindest mittelbar, Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG.[239]

Zugleich bedeutet die hier vorgeschlagene Auslegung von Art. 2 Abs. 2 lit. a DS-GVO, dass praktisch alle Datenverarbeitungsvorgänge der digitalen Wirtschaft, die ganz grundsätzlich durch einen stark grenzüberschreitenden Bezug der Erbringung von Dienstleistungen geprägt sind, nicht unter die Ausnahme von Art. 2 Abs. 2 lit. a DS-GVO fallen dürften.[240] Damit ist die DS-GVO insoweit grundsätzlich in den hier betrachteten Fallgruppen der drei Leitfälle sachlich anwendbar.

bb) Weitere Ausnahmen

Weitere Ausnahmen bestehen für den Bereich der Gemeinsamen Außen- und Sicherheitspolitik, Art. 2 Abs. 2 lit. b DS-GVO; für familiäre oder persönliche Tätigkeiten, Art. 2 Abs. 2 lit. c DS-GVO; und für Strafverfolgung und Gefahrenabwehr, Art. 2 Abs. 2 lit. d DS-GVO. Erstere und letztere Ausnahme sind für die digitale Wirtschaft kaum relevant.

Zu der bereits in Abs. 3 Abs. 2 Spstr. 2 DSRL enthaltenen Ausnahme für persönliche oder familiäre Tätigkeiten hat der EuGH entschieden, dass „mit ihr nur Tätigkeiten gemeint sind, die zum Privat- oder Familienleben von Einzelpersonen gehören, was offensichtlich nicht der Fall ist bei der Verarbeitung personenbezogener Daten, die in deren Veröffentlichung im Internet besteht, so dass diese Daten einer unbegrenzten Zahl von Personen zugänglich gemacht werden."[241] Dem ist vollumfänglich zuzustimmen.[242] Der 18. Erwägungsgrund der DS-GVO zeigt ferner auf, dass zur Haushaltsausnahme nur Tätigkeiten gehören „ohne Bezug zu einer beruflichen oder wirtschaftlichen

[237] Ähnlich *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 2 DS-GVO Rn. 21; *Bäcker*, in: BeckOK DatenschutzR, 27. Ed. 1.8.2018, Art. 2 DS-GVO Rn. 7.

[238] Dazu oben, Text bei § 4, Fn. 224.

[239] Siehe oben, Text bei § 4, Fn. 28 f.

[240] Im Ergebnis ähnlich *Bäcker*, in: BeckOK DatenschutzR, 27. Ed. 1.8.2018, Art. 2 DS-GVO Rn. 8.

[241] EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 47.

[242] Ebenso *Fechner*, JZ 2004, 246 (247); *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 90 f.

Tätigkeit". Daher ist auch diese Ausnahme für die im Rahmen der digitalen Wirtschaft tätigen Anbieter ohne nennenswerten Belang.[243]

Die Verarbeitung durch Unionsinstitutionen richtet sich wiederum gemäß Art. 2 Abs. 3 DS-GVO nach einer eigenen Verordnung.[244] Für die Übermittlung personenbezogener Daten über EU-Außengrenzen hinweg gelten schließlich eigene Vorschriften (Art. 44 ff. DS-GVO), die ein Minimum an datenschutzrechtlicher Äquivalenz oder zumindest Risikobeherrschung durch die Betroffenen sicherstellen sollen.

3. Ergebnis zur Anwendbarkeit der DS-GVO

Die DS-GVO ist auf die drei Leitfälle, und auch sonst im Rahmen der digitalen Wirtschaft, grundsätzlich territorial und sachlich anwendbar. Sie muss daher in den bestehenden privatrechtlichen Ordnungsrahmen eingepasst werden. Ausnahmsweise kann die Anwendbarkeit zu verneinen sein, wenn keinerlei Personenbezug bei den verarbeiteten Daten besteht, insbesondere die Identifizierbarkeit bei einer Risikoabwägung nicht als hinreichend wahrscheinlich anzusehen ist. Dies kann etwa bei namenlosen Profilen (*ad exchanges*) der Fall sein, sofern keine für Kundenpräferenzen besonders signifikanten Informationen darin enthalten sind. Auch bei Trainingsdaten für maschinelles Lernen kann im Einzelfall ein Personenbezug fehlen. Wird der Personenbezug verneint, können allenfalls die Regeln der ePrivacy-Instrumente zum Tragen kommen.

Schließlich sind zumindest denkbar Fälle rein national geprägter Verarbeitungssituationen, in denen kein auch nur entfernter Bezug zu einer der Grundfreiheiten besteht. Dann erst richtet sich die Verarbeitung nach hier vertretener Auffassung nach nationalem Datenschutzrecht, mithin dem BDSG und dem Recht auf informationelle Selbstbestimmung.

III. Datenschutzrechtliche Grundkonzepte

Die Anwendung der DS-GVO wird ferner geprägt durch eine Reihe von Grundkonzepten, welche auf die einzelnen Zulässigkeitskriterien, aber auch die übrigen Vorschriften, in erheblicher Weise ausstrahlen. Dies betrifft einerseits den Begriff des datenschutzrechtlich Verantwortlichen (1.) und andererseits die Grundsätze der Datenverarbeitung nach Art. 5 Abs. 1 DS-GVO (2.).

---

[243] Siehe aber für die Anwendung auf die Tätigkeit von Nutzern in einem sozialen Netzwerk *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 91 ff.; *Kampert*, Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, 2016, 80 ff.

[244] Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG, ABl. 2018 L 295/39.

Die Anwendung dieser Grundkonzepte auf die drei Leitfälle der Datenverarbeitung in der digitalen Wirtschaft erweist sich dabei als keineswegs trivial.

1. Stufen datenschutzrechtlicher Verantwortlichkeit in vernetzten Umgebungen

Im technischen Sinne vollzieht sich die Architektur von Informationsanbieterverhältnissen, besonders im Rahmen des sogenannten Web 2.0, typischerweise auf verschiedenen Ebenen oder Stufen.[245] Im Rahmen von sozialen Netzwerken etwa, bei denen Daten als Gegenleistung fungieren, stellt das Netzwerk selbst häufig eine informationstechnische Infrastruktur bereit, innerhalb derer Drittanbieter eigene Seiten innerhalb des Netzwerks eröffnen können, die wiederum kommerziell auf Endkunden ausgerichtet sind.[246] Dies ist etwa der Fall bei den sogenannten Fanpages von Facebook, in deren Rahmen Unternehmen eine eigene Präsenz auf dem sozialen Netzwerk unterhalten können. Umgekehrt wurde bereits ausgeführt,[247] dass bei Social Plug-Ins der Betreiber einer Webseite ein Plug-In durch einen iframe einbindet, das von einem Drittanbieter zur Verfügung gestellt wird und innerhalb der Webseite eigenständig und unmittelbar, unter „Umgehung" des Webseiteninhabers, Daten für den Betreiber des Plugins erhebt.

Diese Schattierungen technischer Ebenen und Verantwortlichkeiten werden jedoch durch das Konzept der datenschutzrechtlichen Verantwortlichkeit nur unzureichend gespiegelt. Art. 4 Nr. 7 DS-GVO bestimmt als Verantwortlichen „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Neben der alleinigen existiert damit dem Wortlaut nach lediglich noch die – jedenfalls grundsätzlich gleichrangige – gemeinsame Verantwortlichkeit, die in Art. 26 DS-GVO näher umschrieben wird.

a) Relevanz der Bestimmung der Verantwortlichkeit

Die Bestimmung des oder der datenschutzrechtlich Verantwortlichen ist jedoch für das datenschutzrechtliche Gefüge zentral. Der Verantwortliche ist gemäß Art. 5 Abs. 2 DS-GVO zuständig für die Einhaltung der Grundsätze der Datenverarbeitung; ferner ist er der Adressat von Betroffenenrechten nach Art. 12 ff. DS-GVO, inklusive der Informationspflichten. Sachgerecht erscheint dann insoweit, dass auch der Verantwortliche Adressat von Sanktionen gemäß Art. 82 ff. DS-GVO ist.

---

[245] *Zaglia*, 66 Journal of Business Research 2013, 216; ferner BVerwG, ZD 2016, 393 Rn. 30 f.; *Hacker*, MMR 2018, 779 (779).

[246] *Ryte Wiki*, Facebook Fanpage, https://de.ryte.com/wiki/Facebook_Fanpage.

[247] Siehe oben, § 2 A.I. und § 4 A.II.2.a)aa)(2)(b)(bb).

b) Typen von Verantwortlichkeit

Wie soeben bereits angedeutet, unterscheidet die in Art. 4 Nr. 7 DS-GVO enthaltene Legaldefinition des Verantwortlichen zwischen der alleinigen und der gemeinsamen Verantwortung als den zwei der DS-GVO bekannten Typen von Verantwortlichkeit. Beiden Typen ist gemeinsam, dass jeder Verantwortliche nach dem Regelungsmodell der DS-GVO einer Direktwirkung unterliegt: Die datenschutzrechtlichen Pflichten bestehen unmittelbar im Verhältnis zur betroffenen Person unabhängig davon, ob zwischen den Parteien ein vertragliches oder sonstiges schuldrechtliches Verhältnis besteht.[248]

aa) Alleinige Verantwortlichkeit

Alleinig verantwortlich ist nach dem Wortlaut von Art. 4 Nr. 7 DS-GVO diejenige natürliche oder juristische Person, welche „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Diese Bestimmung wird vom EuGH weit ausgelegt, um einen wirksamen und umfassenden Betroffenenschutz zu gewährleisten.[249]

Maßgeblich ist damit für die Eigenschaft als Verantwortlicher die Entscheidungsgewalt über die Verarbeitung. Dies ist sinnvoll insoweit, als gerade der Verantwortliche Betroffenenrechte erfüllen muss, was vor allem im Fall der Berichtigung oder Löschung von Daten oder der Einschränkung der Verarbeitung nach Art. 16–18 DS-GVO einen Zugriff auf die Verarbeitung bzw. die Daten voraussetzt. Damit installiert die DS-GVO ein Prinzip der Korrespondenz von Kontrolle und Verantwortung, ähnlich dem Rechtssatz *qui habet commoda ferre debet onera*.[250]

bb) Gemeinsame Verantwortlichkeit

Demgegenüber impliziert gemeinsame Verantwortlichkeit nach Art. 4 Nr. 7 DS-GVO, dass mindestens zwei Entitäten gemeinsam die Entscheidungsgewalt über Zwecke und Mittel der Verarbeitung innehaben.[251] Beide müssen selbstständig und im Wesentlichen gleichrangig über Zwecke und Mittel bestimmen, da bei einer vollständigen Unterordnung,[252] z. B. einem einseitigen Weisungsrecht, eine Auftragsverarbeitung nach Art. 4 Nr. 8 DS-GVO vorliegt,[253] bei

[248] *Wendehorst*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen).

[249] EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 28; Urt. v. 13.5.2014 – Rs. C-131/12 (*Google Spain*) – Rn. 34.

[250] *Hacker*, MMR 2018, 779 (780); vgl. auch *Schulz*, ZD 2018, 363 (364); GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 91; zum Rechtssatz selbst, siehe etwa *Zimmermann*, The Law of Obligations, 1990, 201 Fn. 108 und 290.

[251] Siehe nur *Specht-Riemenschneider/Schneider*, MMR 2019, 503 (504).

[252] VGH München, NVwZ 2019, 171 Rn. 16 (zu § 11 Abs. 1 BDSG aF).

[253] Zum Weisungsrecht als maßgeblichem Indiz für das Vorliegen von Auftragsverarbei-

der nur der Auftraggeber Verantwortlicher, der Auftragnehmer hingegen Auftragsverarbeiter ist (vgl. Art. 28 DS-GVO).

Zudem muss jedenfalls grundsätzlich kumulativ über die Mittel *und* den Zweck der Verarbeitung gemeinsam entschieden werden.[254] Eine gemeinsame Bestimmung der Mittel der Verarbeitung impliziert, dass eine signifikante Mitentscheidungsgewalt jedes Beteiligten hinsichtlich der konkreten Art und Weise der Verarbeitung besteht.[255] Bezüglich der Gemeinsamkeit des Zwecks wird vertreten, dass es für einen gemeinsamen Zweck auch ausreichen könne, wenn sich die einzelnen Zwecke jeweils im Sinne eines wechselseitig positiven Nutzens ergänzten.[256] Dies erscheint jedoch zu weit gefasst, da dies typischerweise bei jedem freiwilligen Austauschverhältnis der Fall ist.[257] Vorzugswürdig ist es,[258] im Wesentlichen dieselben Kriterien anzuwenden wie diejenigen, die aus dem Gesellschaftsrecht für die Frage bekannt sind, ob ein gemeinsamer Gesellschaftszweck verfolgt wird oder lediglich gleichgerichtete Partikularinteressen.[259] Dies ist in der Sache sinnvoll, da eine gemeinsame Verantwortung nur bei einer gemeinsamen Organisations- oder Entscheidungsstruktur greifen sollte. Zwar müssen die gemeinsam Verantwortlichen keinesfalls (konkludent) eine Gesellschaft zu Zwecken der gemeinsamen Datenverarbeitung gegründet haben.[260] Dennoch ist der Abgleich mit dem Gesellschaftsrecht instruktiv: Auch hier tritt eine gleichartige, volle Außenhaftung der Gesellschafter nach § 128 S. 1 HGB (analog) nur ein, wenn eine hinreichende Gemeinsamkeit des verfolgten Zwecks angenommen werden kann. Sonst verbleibt es bei partikularen Ansprüchen gegen die einzelnen an einem Projekt beteiligten Personen.

Genau dieser Mechanismus obwaltet auch im Datenschutzrecht. Bei Vorliegen gemeinsamer Verantwortlichkeit greift Art. 26 DS-GVO. Nach seinem ersten Absatz müssen die gemeinsam Verantwortlichen eine Vereinbarung abschließen, in der sie eine interne Aufteilung der nach der DS-GVO zu erfüllenden Pflichten vornehmen.[261] Diese Vereinbarung, die Betroffenen gemäß Art. 26 Abs. 2 DS-GVO in den wesentlichen Teilen zur Verfügung gestellt

tung *B. Wagner*, ZD 2018, 307 (310); zum alten Recht (§ 11 BDSG Abs. 1 aF) *Knopp*, DuD 2010, 783 (784).

254 Dies entspricht der wohl hM, siehe *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 26 DS-GVO Rn. 12; zweifelnd *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 26 DS-GVO Rn. 13.

255 *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 7 DS-GVO Rn. 20.

256 GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 104.

257 Vgl. *Hanloser*, ZD 2019, 122 (123).

258 *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", 2010, 24.

259 Siehe dazu etwa *Schäfer*, in: MüKo, BGB, 7. Aufl. 2017, § 705 Rn. 17–19; *Windbichler*, Gesellschaftsrecht, 24. Aufl. 2017, 49.

260 Insbesondere an der Beitragsleistung mit Blick auf ein verselbstständigtes Vermögen wird es häufig fehlen; vgl. auch *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 26 DS-GVO Rn. 30.

261 Dazu *Härting*, ITRB 2018, 167 (169 f.).

werden muss, entfaltet jedoch keine Außenwirkung. Vielmehr gilt nach Art. 26 Abs. 3 DS-GVO, dass Betroffene ihre Rechte vollumfänglich gegenüber jedem Einzelnen der gemeinsam Verantwortlichen geltend machen können. Die Regelung ähnelt damit dem im Grundsatz unbeschränkten Forderungsrecht gegenüber Gesamtschuldnern nach § 421 Abs. 1 S. 1 BGB.[262]

cc) Zwischenstufen: Die Rechtssache *Wirtschaftsakademie Schleswig-Holstein*

Die dichotome Unterscheidung zwischen alleiniger Verantwortung einerseits und vollkommen gleichrangiger gemeinsamer Verantwortung andererseits stieß bereits unter der Geltung der DSRL auf Kritik, da sie den vielfältigen, technologisch und rechtlich abgestuften Formen der Kooperation in gegenwärtigen Informationsanbieterverhältnissen nicht gerecht wurde. Die Artikel-29-Datenschutzgruppe schlug daher vor,[263] die beiden Verantwortungstypen lediglich als die Pole eines Spektrums anzusehen, innerhalb dessen verschiedene Formen von Verantwortungsaufteilung als „pluralistische Kontrolle" stattfinden können. In der Literatur wird zudem eine getrennte, aber parallele Verantwortung mehrerer Verantwortlicher vorgeschlagen.[264]

Der EuGH schloss sich der Betrachtungsweise der Artikel-29-Datenschutzgruppe in der Rechtssache *Wirtschaftsakademie Schleswig-Holstein* im Ergebnis an. In der Sache ging es darum, ob neben Facebook auch die Betreiber von Facebook Fanpages gemeinsam Verantwortliche für jene Datenverarbeitungen sind, die sich an jenen Daten vollziehen, die von Besuchern der Fanpages über von Facebook installierte Cookies gesammelt werden. Der EuGH entschied in einem ersten Schritt, dass die Betreiber von Fanpages gemeinsam mit Facebook Verantwortliche sind (dazu sogleich im Einzelnen unten, § 4 A.III.1.b)dd)(1)).

In einem zweiten Schritt betonte der EuGH jedoch unter Rekurs auf die Schlussanträge des Generalanwalts, dass eine gemeinsame Verantwortung „nicht zwangsläufig eine gleichwertige Verantwortlichkeit der verschiedenen Akteure zur Folge hat, die von einer Verarbeitung personenbezogener Daten betroffen sind. Vielmehr können diese Akteure in die Verarbeitung personenbezogener Daten in verschiedenen Phasen und in unterschiedlichem Ausmaß in der Weise einbezogen sein, dass der Grad der Verantwortlichkeit eines jeden von ihnen unter Berücksichtigung aller maßgeblichen Umstände des Einzel-

---

[262] So auch GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 96; *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 26 DS-GVO Rn. 28; *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 26 DS-GVO Rn. 29. Ähnliches regelt Art. 82 Abs. 4 DS-GVO für den Schadensersatz.

[263] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", 2010, 22; dem folgend etwa *Moos/Rothkegel*, MMR 2018, 596 (597).

[264] *Lee/Cross*, MMR 2019, 559 (562); *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 126 ff.; *Petri*, ZD 2015, 103 (106); *Jandt/Roßnagel*, ZD 2011, 160 (161).

falls zu beurteilen ist."[265] Generalanwalt *Bot* wiederum hatte sich zur Herleitung dieser Schlussfolgerung maßgeblich auf die Ausführungen der Artikel-29-Datenschutzgruppe gestützt.[266] Diese Ausdifferenzierung bestätigte der EuGH in der Rechtssache *Zeugen Jehovas* nochmals;[267] die dogmatische Umsetzung und Konsequenz dieser flexiblen Verantwortungsaufteilung blieb jedoch im Dunkeln.

dd) Anwendung auf die drei Leitfälle

Diese Kriterien lassen sich wiederum spezifisch auf die drei Leitfälle anwenden. Angesichts der einschlägigen Rechtsprechung wird mit dem zweiten Leitfall begonnen.

(1) Datenerhebung durch Drittanbieter (*third-party tracking*)

Besondere Aufmerksamkeit haben auch in der Rechtsprechung Fälle erregt, bei denen es um *third-party tracking* geht, etwa durch Cookies und durch Social Plug-Ins.

(a) Die Rechtsprechung des EuGH

Der EuGH hat sich in zwei größeren Entscheidungen zur Frage der Verantwortlichkeit geäußert. Den Anfang machte die soeben erwähnte Rechtssache *Wirtschaftsakademie Schleswig-Holstein* zu Facebook Fanpages. Hinzu kam dann die Rechtssache *Fashion ID* zu Social Plug-Ins.

(aa) Kriterien

Der EuGH benennt in den Urteilen eine Reihe von Kriterien, nach denen sich bemisst, ob eine gemeinsame Verantwortung vorliegt.

α. Cookies: Nochmals *Wirtschaftsakademie Schleswig-Holstein*

In der Rechtssache *Wirtschaftsakademie Schleswig-Holstein* entschied der EuGH in einem zumindest hinsichtlich der Urteilsgründe kritikwürdigen Urteil, dass eine gemeinsame Verantwortlichkeit von Facebook und den Betreibern von Facebook Fanpages vorläge, weil die Betreiber von Facebook Fanpages über das von Facebook zwingend zur Verfügung gestellte Analyseinstrument *Facebook Insights* anonymisierte statistische Auswertungen über die Besucher der jeweiligen Fanpage erhielten. Die Analyseparameter dieser

[265] EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 43; ebenso EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 70.

[266] GA *Bot*, Schlussanträge v. 24.10.2017 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 75 f.

[267] EuGH, Urt. v. 10.7.2018 – Rs. C-25/17 (*Zeugen Jehovas*) – Rn. 66.

Auswertung können die Betreiber der Fanpage in gewissem Rahmen selbst bestimmen („Parametrierung").[268] Insofern bestimmen die Inhaber der Fanpage, auch wenn die Analyse der Daten selbst lediglich durch Facebook vorgenommen wird, nach Auffassung des EuGH in hinreichender Weise über die Mittel und Zwecke der Verarbeitung mit.[269] Die DSRL verlange nicht, „dass bei einer gemeinsamen Verantwortlichkeit mehrerer Betreiber für dieselbe Verarbeitung jeder Zugang zu den betreffenden personenbezogenen Daten hat."[270]

Der EuGH bemühte hierfür drei Argumente. Erstens setzten die Betreiber der Fanpage eine notwendige Voraussetzung für die Verarbeitung der Daten von Besuchern der Fanpage durch Facebook.[271] Dieses Kriterium ist jedoch überinklusiv, da daran gemessen auch die Betreiber sonstiger notwendiger Infrastruktur (zum Beispiel Stromanbieter oder Access Provider) gemeinsam Verantwortliche sein müssten, was niemand vertritt.[272] Zweitens bestimmt der Betreiber der Fanpage die durch Facebook vorgenommene Datenanalyse infolge der Parametrierung entscheidend mit.[273] Drittens steuert er auch die Zwecke der Datenverarbeitung, da die Analyseinformationen den Fanpagebetreibern die Optimierung ihres Auftritts und Produkts ermöglichen.[274] Auch dieses dritte Kriterium leidet jedoch an mangelnder Selektionskraft, da nicht jeder, der anonymisierte Daten zur Ausrichtung der eigenen Unternehmensstrategie nutzt, Verantwortlicher für die Verarbeitung der den anonymisierten Statistiken zu Grunde liegenden personenbezogenen Daten sein kann.[275]

Entscheidend ist nach hier vertretener Auffassung das zweite vom EuGH vorgebrachte Kriterium:[276] Der gemeinsam Verantwortliche muss über die konkreten Mittel und Zwecke der Verarbeitung signifikante Mitentscheidungsgewalt haben. Nur dies entspricht dem Wortlaut, aber auch dem Sinn und Zweck der Vorschriften über gemeinsame Verantwortung im Sinne der

---

[268] EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 36 f.

[269] EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 39.

[270] EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 38; bestätigt in EuGH, Urt. v. 10.7.2018 – Rs. C-25/17 (*Zeugen Jehovas*) – Rn. 69; Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 69.

[271] EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 35; zustimmend *Bergt*, ITRB 2018, 151 (152).

[272] *Hacker*, MMR 2018, 779 (779 f.); *Marosi/Matthé*, ZD 2018, 361 (362); GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 74 f.; *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 124.

[273] EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 39.

[274] EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 37.

[275] *Hacker*, MMR 2018, 779 (780).

[276] *Hacker*, MMR 2018, 779 (780); *Härting*, ITRB 2018, 167 (168); *ders.*, Internetrecht, 6. Aufl. 2017, Rn. 236 f.; *Marosi/Matthé*, ZD 2018, 361 (362); *Schulz*, ZD 2018, 363 (364); aA *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 125: Maßgeblichkeit des Zwecks.

Korrespondenz von Kontrolle und Verantwortung. Die beiden anderen Kriterien sind für sich genommen nicht hinreichend und können lediglich stützende Hilfserwägungen darstellen, die im Rahmen einer allfälligen Gesamtwürdigung zu beachten sind. Da tatsächlich relevante Entscheidungsparameter durch den Fanpagebetreiber mitgestaltet werden können, lässt sich auch in der hier vertretenen Interpretation eine Mitverantwortung an der Datenanalyse letztlich begründen.

Damit ist jedoch zugleich klar, dass die für Facebook Fanpages angenommene gemeinsame Verantwortung nicht für jegliche Form von Cookies, die durch Drittanbieter auf Webseiten gesetzt werden, gelten kann. Entscheidend war für den EuGH, dass gerade der Webseitenbetreiber die Parameter der Datenanalyse mitbestimmen konnte. Dies ist jedoch eine Besonderheit der Funktionsweise von *Facebook Insights*, die für andere Cookies und Tracking-Tools nicht in der gleichen Weise gilt. Mithin muss jeweils im Einzelfall überprüft werden, inwieweit der Webseitenbetreiber die relevanten Entscheidungsparameter selbst (mit) auswählt. Der Webseitenbetreiber entscheidet bei Tracking-Tools, diese über einen Code im HTML-Text der Webseite einzubinden.[277] Die Daten werden dann durch den jeweiligen Drittanbieter direkt, ohne weiteres Zutun des Webseitenbetreibers, erhoben.[278] Der reine Kausalbeitrag der Ermöglichung der Setzung von Drittanbietercookies kann, entgegen einer verbreiteten Literaturansicht[279] und wohl auch der früheren Tendenz des EuGH,[280] jedoch nicht für die Verantwortung für die gesamte Kette der dadurch ermöglichten Datenverarbeitungen genügen.[281] Hinter der Literaturansicht steht zwar das verständliche rechtspolitische Ziel, über eine Mitverantwortung der Webseitenanbieter deren Anreize für die Einbindung von Drittanbietercookies zu reduzieren.[282] Mit Wortlaut und Zweck von Art. 4 Nr. 7 DS-GVO ist dies jedoch nach hier vertretener Ansicht nicht in Einklang zu bringen. Es müssen konkrete Möglichkeiten hinzukommen, die Datenverarbeitung selbst oder jedenfalls ihre relevanten Parameter mitzugestalten.[283] Bei Google Analytics z. B. ist eine derartige „Parametrierung" durch die Webseiteninhaber, soweit aus den Nut-

[277] *Knopp*, DuD 2010, 783 (784).
[278] *Knopp*, DuD 2010, 783 (784).
[279] *Weichert*, ZD 2014, 605 (609); *Meyer*, MMR 2017, 254 (257); *Föhlisch/Pilous*, MMR 2015, 631 (633); *Ernst*, NJOZ 2010, 1917 (1918); *KG* MMR 2011, 464 (465).
[280] Siehe nochmals EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 41; ferner Urt. v. 13.5.2014 – Rs. C-131/12 (*Google Spain*) – Rn. 34–41; dazu *Karg*, ZD 2014, 359 (360); jetzt jedoch aufgegeben in EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 76.
[281] So auch *Härting*, ITRB 2012, 109 (110); *Schulz*, ZD 2018, 357 (364); *Piltz*, ZD 2017, 336 (337); *Voigt/Alich*, NJW 2011, 3541 (3543).
[282] Vgl. GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 72; *Weichert*, ZD 2014, 605 (608).
[283] Ebenso noch BVerwG, ZD 2016, 393 Rn. 26; wohl auch OLG Düsseldorf, MMR 2017, 254 Rn. 13 f.; *Martini/Fritzsche*, NVwZ 2015, 1497 (1498).

zungsbedingungen ersichtlich, nicht vorgesehen.[284] Konsequenterweise liegt dann nach der hier vertretenen Auffassung auch keine datenschutzrechtliche (Mit-) Verantwortlichkeit des Webseitenbetreibers, der Google Analytics einbindet, für die von Google vorgenommene Datenanalyse vor. Lediglich hinsichtlich der initialen Erhebung der Daten kann eine solche angenommen werden.[285]

β. Social Plug-Ins: Die Rechtssache *Fashion ID*

Die identischen drei Kriterien aus der Rechtssache *Wirtschaftsakademie Schleswig-Holstein* nutzte der EuGH auch in der Rechtssache *Fashion ID*, um die Frage der gemeinsamen Verantwortlichkeit im Fall von Social Plug-Ins zu beantworten. Auch hier ermöglicht der Webseitenbetreiber durch die Einbindung eines iframes in seine Webseite die direkte Datenübertragung an Facebook,[286] und auch hier steht dem Webseitenbetreiber das Analyseinstrument *Facebook Insights* zur Verfügung.[287] Angesichts der starken Parallelen zu der Konstellation von Facebook Fanpages überraschte der EuGH daher kaum, als er den Webseitenbetreiber auch hier als gemeinsam mit Facebook Verantwortlichen bezeichnete.[288] Allerdings beschränkte der EuGH nun erstmals die gemeinsame Verantwortung auf bestimmte Verarbeitungsschritte, konkret die Erhebung der Daten und ihre Übermittlung an Facebook. Auch hier begegnet das Argument, dass die Einbindung des Social Plug-Ins in den Code der Webseite eine notwendige Bedingung setzt, die eine Kausalkette in Gang bringt, ohne welche Datenübertragungen an Facebook nicht geschehen würden.[289] Ferner kommt auch hier zum Tragen, dass die *Facebook Insights* zur Optimierung des Websiteauftritts und des Produkts genutzt werden können,[290] was der EuGH jedoch unerwähnt lässt.[291] Vielmehr ist für ihn relevant, dass der Social Plug-In, wenn er betätigt wird, die Sichtbarkeit der Webseite in sozialen Netzwerken erhöht.[292]

---

[284] *Google*, Nutzungsbedingungen für Google Analytics, https://www.google.com/analytics/terms/de.html (zuletzt abgerufen am 14.6.2019), unter 4.

[285] Siehe genauer unten, § 4 A.III.1.b)dd)(1)(b).

[286] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 75.

[287] *Marosi/Matthé*, ZD 2018, 361 (363); vgl. EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 80.

[288] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 76, 85.

[289] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 75, 78; so bereits GA *Bot*, Schlussanträge v. 24.10.2017 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 69–72; *Bergt*, ITRB 2018, 151 (152).

[290] GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 68.

[291] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 80 (ohne Nennung von *Facebook Insights*).

[292] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 80; GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 104; siehe dazu kritisch *Sattler*, GRUR 2019, 1023 (1024 f.).

Die Kritik der Entscheidung fällt genauso aus wie jene der Rechtssache *Wirtschaftsakademie Schleswig-Holstein*: Der EuGH hätte sich in seiner Argumentation auf das zweite Kriterium, die konkrete Mitentscheidungsgewalt infolge der Parametrierung, fokussieren müssen. Hier liegt nun auch der entscheidende Unterschied zur Konstellation der Facebook Fanpages: Webseitenbetreiber, welche ein Social Plug-In von Facebook einbinden, können offenbar gerade nicht die relevanten Analyseparameter mitbestimmen.[293] Dies wird vom EuGH denn auch gar nicht erwähnt. In der Sache schließt er sich jedoch einer Fokussierung auf das zweite Kriterium an. Denn mangels Parametrierung kann hinsichtlich der sich an die Erhebung anschließenden Datenanalyse[294] durch Facebook, wie auch soeben für Google Analytics diskutiert, gerade nicht von einer sachlich hinreichenden Mitentscheidungsgewalt der Webseiteninhaber gesprochen werden – ein Ergebnis, zu dem auch der EuGH kommt.[295]

(bb) Rechtsfolgen

Hinsichtlich der Rechtsfolgen der gemeinsamen Verantwortung ist richtigerweise zwischen den nach der DSRL entschiedenen Fällen und der DS-GVO zu unterscheiden.

α. Geltung der DSRL (Altfälle)

Wie bereits erwähnt, nahm der EuGH bereits in der Rechtssache *Wirtschaftsakademie Schleswig-Holstein* an, dass eine gemeinsame Verantwortung nach der DSRL nicht notwendig gleichrangig gedacht sein muss, sondern unterschiedliche Abstufungen hinsichtlich der Rechte und Pflichten der einzelnen Verantwortlichen aufweisen kann.[296] Entscheidend seien jeweils die Umstände des Einzelfalles. Dies konnte der EuGH so formulieren, da in der DSRL keine spezifische Regelung für die Rechtsfolgen der gemeinsamen Verantwortung enthalten war.[297]

β. Art. 26 Abs. 3 DS-GVO

Genau eine solche Rechtsfolgenregelung wurde jedoch mit Art. 26 DS-GVO eingeführt. Jedenfalls dem Wortlaut nach erlaubt sie ein abgestuftes Verantwortungsspektrum allerdings gerade nicht, da Art. 26 Abs. 3 DS-GVO für das Außenverhältnis eine strikt gleichrangige Verantwortung installiert, die dem deutschen Verständnis einer Gesamtschuld nach § 421 BGB entspricht.[298]

---

[293] GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 68.
[294] Zur Frage der Daten*erhebung* sogleich, § 4 A.III.1.b.dd)(1)(b).
[295] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 85.
[296] Siehe oben, Text bei § 4, Fn. 265.
[297] Kritisch aber *Piltz*, ZD 2017, 336 (337).
[298] Siehe bereits oben, § 4, Fn. 262.

Damit ist eigentlich kein Raum mehr dafür,[299] den „Grad der Verantwortlichkeit eines jeden [der gemeinsam Verantwortlichen] unter Berücksichtigung aller maßgeblichen Umstände des Einzelfalls zu beurteilen."[300]

Sinn und Zweck von Art. 26 Abs. 3 DS-GVO dürfte die Verhinderung von Nachteilen aus einer Informationsasymmetrie sein:[301] Die gemeinsam Verantwortlichen selbst wissen regelmäßig besser, wer welche Aspekte der Datenverarbeitung kontrollieren kann. Diese Asymmetrie wird auch durch die nach Art. 26 Abs. 2 DS-GVO zu veröffentlichenden wesentlichen Teile der internen Verantwortlichen nur abgemildert, nicht jedoch in jedem Fall gänzlich aufgehoben. Die betroffene Person soll daher davor geschützt werden, bei mehreren Verarbeitern nicht zuverlässig denjenigen auszuwählen zu können, der nach der internen Zuständigkeitsverteilung für das konkrete Betroffenenrecht verantwortlich ist.[302] Abstufungen der Verantwortung sind mit Blick auf dieses informationelle Schutzprinzip eigentlich nicht vorgesehen. Lediglich im Rahmen der Schadensersatzhaftung kann nach Art. 82 Abs. 5 DS-GVO Regress genommen werden und ausnahmsweise eine Außenhaftung nach Art. 82 Abs. 3 DS-GVO mangels Verschulden ausgeschlossen sein. Ferner kann bei der Gewichtung von Sanktionen nach Art. 83 DS-GVO ebenfalls auf die tatsächliche Entscheidungsgewalt abgehoben werden.[303]

(b) Plädoyer für eine abgestufte Verantwortung im Rahmen der DS-GVO

Demgegenüber lässt sich jedoch auch für die DS-GVO ein funktionaler Ansatz vertreten, der in teleologischer Auslegung dem Prinzip der Korrespondenz von Kontrolle und Verantwortung gerecht wird.

(aa) Kriterien

Vorzugswürdig erscheint demnach, auch für die DS-GVO in zweifacher Weise zu differenzieren: nach (i) Verarbeitungsschritten und den hier jeweils sich bietenden (ii) Steuerungsmöglichkeiten.[304] Zunächst ist mithin scharf zwischen

---

[299] *Moos/Rothkegel*, MMR 2019, 584 (586).

[300] EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 43.

[301] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", 2010, 27; *Hacker*, MMR 2018, 779 (780).

[302] Vgl. *Marosi/Matthé*, ZD 2018, 361 (363): Schutz vor unklaren Verantwortlichkeiten; *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 26 DS-GVO Rn. 28; *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 26 Rn. 36.

[303] *Bergt*, ITRB 2018, 151 (152).

[304] So auch *Marosi/Matthé*, ZD 2018, 361 (363); *Moos/Rothkegel*, MMR 2019, 584 (585); *Hanloser*, ZD 2019, 458 (459); zu Abgrenzungsschwierigkeiten *Sattler*, GRUR 2019, 1023 (1025); aA *Globocnik*, 50 ICC 2019, 1033 (1037): Gesamtbetrachtung aller Datenverarbeitungsprozesse; *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 128 f.; siehe ferner für eine parallele, getrennte Verantwortlichkeit die Nachweise in § 4, Fn. 264.

den einzelnen Verarbeitungen zu unterscheiden.[305] Der EuGH führt dies in der Rechtssache *Wirtschaftsakademie Schleswig-Holstein* noch nicht konsequent durch. Er betont zwar, dass der Grad der Verantwortlichkeit in „verschiedenen Phasen" der Verarbeitung unterschiedlich ausfallen kann,[306] spricht aber dennoch dem Webseitenbetreiber einer Fanpage jedenfalls grundsätzlich eine gemeinsame Verantwortung für alle Verarbeitungen von Daten der Fanpagebesucher zu.[307] Demgegenüber muss richtigerweise bereits im Grundsatz die Erhebung der Daten streng getrennt werden von der späteren Analyse und weiteren Übermittlung an etwaige Drittunternehmen.[308] Dieser Auffassung hat sich der EuGH für die DSRL nun in der Rechtssache *Fashion ID* auch angeschlossen.[309] Dafür spricht insbesondere auch Art. 4 Nr. 2 DS-GVO, der ganz verschiedene Verarbeitungsmöglichkeiten jeweils separat nennt.[310] Innerhalb dieser einzelnen Verarbeitungsschritte muss dann zweitens entschieden werden, inwiefern tatsächlich eine Steuerungsmöglichkeit im Sinne einer konkreten Mitentscheidungsgewalt hinsichtlich der Zwecke und Mittel der Datenverarbeitung in dem spezifischen Verarbeitungsschritt vorliegt.

Dies impliziert, dass bei Tracking-Tools zunächst die Erhebung der Nutzerdaten (Browserinformationen, IT-Adresse, besuchte Webseite, Verweildauer etc.[311]) separat betrachtet werden muss.[312] Hier lässt sich in der Tat nicht in Abrede stellen, dass dem Webseiteninhaber signifikante Entscheidungsgewalt zukommt: Ohne die Einbindung des Tracking-Instruments kommt es nicht zu einer Datenerhebung. Zugleich erhebt jedoch der Inhaber des Tracking-Tools, nicht der Webseitenbetreiber, die Daten unmittelbar. Daher sind beide Entitäten gleichrangig an der Erhebung beteiligt und insofern auch gemeinsam

---

[305] Vgl. *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 7 DS-GVO Rn. 22.

[306] EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 43; Urt. v. 10.7.2018 – Rs. C-25/17 (*Zeugen Jehovas*) – Rn. 66.

[307] EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 39 und 41.

[308] So auch GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 97 ff., besonderes Rn. 101.

[309] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 70.

[310] Art. 4 Nr. 2 DS-GVO unterscheidet „das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen [und] die Vernichtung"; siehe daher auch EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 71 f.; GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 98 f.

[311] Siehe etwa mit Blick auf die von Google Analytics erhobenen Daten *Steidle/Pordesch*, DuD 2008, 324 (325).

[312] Der EuGH erstreckt die gemeinsame Verantwortung auf die Erhebung und die (initiale) Übermittlung an den Anbieter des Plug-Ins. Allerdings ist dies ein und derselbe Vorgang, da die Daten direkt an den Anbieter des Plug-Ins fließen, eine Übermittlung seitens des Webseitenbetreibers also nicht stattfindet, siehe *Hanloser*, ZD 2019, 458 (459).

Verantwortliche.[313] Anders wiederum liegt es hinsichtlich der sich daran anschließenden Analyse der Daten. Sofern keine Mitbestimmung über die Analyseparameter durch den Webseitenbetreiber erfolgt, scheidet nach hier vertretener, der Rechtsprechung des EuGH zur DSRL entsprechender Ansicht eine Mitverantwortung aus.[314] Gleiches gilt für eine etwaige weitere Übermittlung der Daten durch den Anbieter des Plug-Ins an Dritte.

Ein besonderes Folgeproblem der hier vertretenen Ansicht stellt sich dann, wenn eine Entscheidungsmöglichkeit für den untergeordneten Anbieter zwar eingeräumt, diese aber nicht genutzt wird (etwa, indem einfach die Voreinstellung der Parameter belassen wird). In der Tat wird z. B. die Analysemöglichkeit Fanpagebetreibern von Facebook unabdingbar aufgedrängt.[315] Einige Stimmen der Literatur wollen nun die bloße Einwirkungs*möglichkeit* für die Begründung von Verantwortung genügen lassen.[316] Aus der Perspektive der Korrespondenz von Kontrolle und Verantwortung erscheint dies zwar einerseits zweifelhaft, da ein Belassen der Voreinstellungen häufig gerade keine bewusste, reflektiert-kontrollierende Entscheidung, sondern eine einfache Folge von Unaufmerksamkeit, Trägheit oder mangelnder Informationsverarbeitungskapazität sein dürfte (*status quo bias*).[317] Nichtsdestoweniger muss andererseits letztlich entscheidend sein, dass Kontrolle ausgeübt werden *könnte*; die (beschränkt rationale oder bewusste) diesbezügliche Zurückhaltung kann nicht zu einer Entlastung führen, wenn eine Mitentscheidung technisch möglich wäre.

(bb) Rechtsfolgen

Sofern für einen bestimmten Verarbeitungsabschnitt eine gemeinsame Verantwortung angenommen werden kann, gilt an sich Art. 26 Abs. 3 DS-GVO mit der uneingeschränkten Außenhaftung jedes gemeinsam Verantwortlichen für alle Betroffenenrechte.[318] In Ansehung des Prinzips der Korrespondenz von Kontrolle und Verantwortung, das den Begriff datenschutzrechtlicher Verantwortlichkeit prägt, ist jedoch Art. 26 Abs. 3 DS-GVO in bestimmten Fällen teleologisch zu reduzieren:[319] Jeder Verantwortliche haftet im Rahmen der Betroffenenrechte grundsätzlich nur soweit, wie ihm eine Kontroll- und Einflussnahmemöglichkeit hinsichtlich der Erfüllung der Ansprüche gegeben ist. Dies

[313] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 85; GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 106.

[314] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 85; GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 107; zu Google Analytics siehe bereits oben, Text bei § 4, Fn. 284.

[315] *Weichert*, ZD 2014, 605 (608).

[316] *Föhlisch/Pilous*, MMR 2015, 631 (633); ähnlich GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 107: Einflusssphäre.

[317] *Samuelson/Zeckhauser*, 1 Journal of Risk and Uncertainty 1988, 7.

[318] Vgl. auch EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 103–106; *Moos/Rothkegel*, MMR 2019, 584 (586).

[319] Dazu bereits *Hacker*, MMR 2018, 779 (780).

verwirklicht den Grundsatz *ultra posse nemo tenetur* auf unionsrechtlicher Ebene.[320] Allerdings muss der Verantwortliche richtigerweise alle zumutbaren Anstrengungen unternehmen, um Betroffenenrechte zu erfüllen. Anlehnen kann sich eine solche Interpretation an die Reichweite der Störerhaftung, die ebenfalls in derartiger Weise beschränkt ist.[321]

Eine Grenze findet diese teleologische Reduktion wiederum in dem Art. 26 Abs. 3 DS-GVO konturierenden Prinzip des Schutzes vor Informationsasymmetrie (informationelles Schutzprinzip). Art. 26 Abs. 3 DS-GVO liegt die Wertung zu Grunde, dass Unklarheiten hinsichtlich der internen Verantwortungsaufteilung nicht zulasten des Betroffenen gehen dürfen. Eine teleologische Reduktion kann daher nur insoweit vorgenommen werden, als die beschränkten Einfluss- und Kontrollmöglichkeiten, zum Beispiel durch die Veröffentlichung wesentlicher Teile der internen Vereinbarung nach Art. 26 Abs. 2 DS-GVO, der Öffentlichkeit und damit dem einzelnen Betroffenen jedenfalls potenziell bekannt sein konnten.

α. Notwendigkeit einer teleologischen Reduktion

Die Notwendigkeit einer derartigen teleologischen Reduktion ergibt sich daher vor allem dann, wenn entgegen den, nach der hier vertretenen Ansicht zu Grunde zu legenden, Kriterien nicht nach einzelnen Verarbeitungsschritten und den diesbezüglichen Kontrollmöglichkeiten differenziert wird, sondern einem technisch untergeordneten Verarbeiter die volle Verantwortung aufgebürdet wird für alle Datenverarbeitungen im Zusammenhang mit der Auswertung von Daten, an deren Erhebung dieser Verarbeiter initial beteiligt ist. Diese nicht zwischen Verarbeitungsschritten differenzierende Lesart entspricht, wie dargestellt, den Ausführungen des EuGH in den Rechtssachen *Wirtschaftsakademie Schleswig-Holstein* und *Zeugen Jehovas*,[322] wurde jedoch in der Rechtssache *Fashion ID* aufgegeben.[323]

Wird hingegen nach den einzelnen Verarbeitungsschritten differenziert, so ergibt sich eine Disjunktion von Kontrollmöglichkeit und Verantwortung nur in deutlich weniger Fällen, da jeweils gesondert festgestellt werden muss, dass jedenfalls grundsätzlich eine Kontrollmöglichkeit auch für den konkreten Verarbeitungsschritt vorliegt.

β. Subsidiäre Anwendung von § 275 Abs. 1 oder 2 BGB

Denkbar wäre ferner, wenn eine derartige Disjunktion von Kontrollmöglichkeit und Verantwortung auftritt, die Betroffenenrechte nach § 275 Abs. 1 oder 2 BGB zu beschränken, wenn der technisch untergeordnete Verarbeiter (etwa

[320] Vgl. auch *Hanloser*, ZD 2019, 122 (123).
[321] Vgl. BGH MMR 2016, 210 Rdnr. 39 f. – recht§billig.
[322] Siehe oben, Text bei § 4, Fn. 307.
[323] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 85.

der Webseiteninhaber) technisch nicht in der Lage ist, die Betroffenenrechte zu erfüllen. Zum Beispiel kann das der Fall sein bei der Löschung von Daten, die lediglich beim übergeordneten Verarbeiter (etwa Facebook) gespeichert sind. Dies wirft die später noch eingehender zu behandelnde Frage der Anwendbarkeit nationalen Rechts neben der DS-GVO auf.[324]

Bereits hier ist jedoch festzustellen, dass Risiken der Unmöglichkeit und des groben Missverhältnisses zwischen Leistungsinteresse und Schuldneraufwand, die in § 275 Abs. 1 und 2 BGB geregelt werden, zwar grundsätzlich in der DS-GVO keine allgemeine, sondern lediglich eine punktuelle Regelung erfahren haben.[325] Allerdings ist im hier zu entscheidenden Fall davon auszugehen, dass in Art. 4 Nr. 7 DS-GVO durchaus eine Beschränkung auf das Mögliche und Zumutbare durchaus angelegt ist. Dies entspricht, wie ausgeführt, nicht nur dem Prinzip der Korrespondenz von Kontrolle und Verantwortung, sondern findet letztlich auch im Wortlaut der Vorschrift insoweit eine Stütze, als dort von der *Entscheidung* über Zwecke und Mittel der Verarbeitung die Rede ist. Entscheidungsgewalt impliziert aber Kontrollmöglichkeiten.

Insofern lässt sich die hier in Rede stehende Beschränkung der Betroffenenrechte nach hier vertretener Auffassung bereits aus dem europäischen Recht selbst ableiten. Dies ist gegenüber einem Rückgriff auf nationales Recht in der Tat insoweit vorzugswürdig, als dadurch die Harmonisierungswirkung des Unionsrechts gewährleistet bleibt.[326] Ein Rückgriff auf § 275 Abs. 1 oder 2 BGB ist daher in den hier zu Grunde liegenden Konstellationen grundsätzlich nicht notwendig.

Anders kann es lediglich dann einmal liegen, wenn eine teleologische Reduktion am informationellen Schutzprinzip von Art. 26 Abs. 3 DS-GVO scheitert, eine Erfüllung der Betroffenenrechte (zum Beispiel von Löschungsansprüchen aus Art. 17 DS-GVO) dem untergeordneten Verarbeiter jedoch tatsächlich technisch unmöglich ist (§ 275 Abs. 1 BGB[327]) oder der Tatbestand von

[324] Siehe unten, § 5 A.

[325] Für den Fall der Pflichtinformationen, die bei Erhebung der personenbezogenen Daten bei einer anderen als der betroffenen Person erbracht werden müssen, findet sich in Art. 14 Abs. 5 lit. b DS-GVO eine § 275 Abs. 1 und 2 BGB vergleichbare Regelung; für die Mitteilung der Berichtigung, Löschung oder Einschränkung der Verarbeitung an Empfänger, denen die Daten offengelegt wurden, in Art. 19 S. 1 DS-GVO; für die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person in Art. 35 Abs. 3 lit. c DS-GVO. Unter Zugrundlegung der unter § 5 A. noch im Einzelnen zu etablierenden Kriterien ergibt sich damit folgendes Bild: § 275 BGB ist jedenfalls grundsätzlich auf die Betroffenenrechte anwendbar, da ein beredtes Schweigen des DS-GVO (gerade bei Unmöglichkeit) abwegig erscheint und eine Begrenzung von Ansprüchen auf ein mögliches und zumutbares Maß auch mit der Verwirklichung des Binnenmarktes nicht kollidiert, diesen vielmehr durch einen nachvollziehbaren Interessenausgleich und das Erlöschen von Ansprüchen, deren Durchsetzung hochgradig ineffizient wäre, tendenziell fördert.

[326] Siehe dazu ausführlich unten, § 5 A.

[327] Ob technische Unmöglichkeit zugleich immer eine rechtlich relevante Unmöglichkeit nach § 275 Abs. 1 BGB darstellt, darf zwar bezweifelt, muss hier aber nicht weiter verfolgt werden.

§ 275 Abs. 2 BGB erfüllt ist. Das informationelle Schutzprinzip gebietet dann jedoch richtigerweise, dass dem Betroffenen keine Kosten (z. B. Gerichtskosten infolge Anspruchsabweisung) für die Geltendmachung des Betroffenenrechts entstehen dürfen, da die Unmöglichkeit oder Unzumutbarkeit dem Betroffenen nicht bekannt war. Eine Überwälzung von Kosten auf den Betroffenen würde in diesen Fällen dem Effektivitätsgrundsatz des Unionsrechts zuwiderlaufen, da ihn dies von der Geltendmachung seiner Rechte abhalten könnte.[328]

γ. Konsequenzen für einzelne Betroffenenrechte

Wenn man dem folgt, sollte der Webseitenanbieter (oder allgemeiner: der technisch untergeordnete Anbieter, der lediglich eine Infrastruktur oder ein Instrument des übergeordneten Anbieters nutzt), soweit er selbst auch (gemeinsamer) Verantwortlichen ist, jedenfalls zur Erfüllung der Informationspflicht aus Art. 13 f. DS-GVO verpflichtet sein, da die formelle Informationsmöglichkeit keine materielle Entscheidungsgewalt voraussetzt.[329] Diese Verpflichtung ist insbesondere auch deshalb wichtig, weil die Datenverarbeitung auch solche Besucher der Seite betrifft, die nicht bei dem übergeordneten Anbieter (etwa Facebook) registriert sind.[330] Hingegen dürften die Verpflichtungen aus Art. 16–20 und Art. 22 sowie Art. 25 und 32 DS-GVO wohl eher nur den übergeordneten Anbieter treffen, sofern für den Betroffenen klar ersichtlich ist, dass dieser die eigentliche Datenanalyse steuert. Mit Ausnahme von Art. 25 und 32 DS-GVO stellt sich dieses Problem jedoch nur, wenn nicht nach einzelnen Verarbeitungsschritten differenziert wird, da eine Speicherung der Daten und eine automatisierte Entscheidung im Einzelfall allenfalls im Rahmen der durch den übergeordneten Anbieter durchgeführten Datenanalyse durchgeführt wird. Auskunftsansprüche aus Art. 15 DS-GVO können gegenüber dem untergeordneten Anbieter geltend gemacht werden, soweit nicht Informationen objektiv erkennbar nur dem übergeordneten Anbieter zugänglich sind. Auch dieses Problem wird bei Differenzierung zwischen den Verarbeitungsschritten deutlich reduziert, da der Auskunftsanspruch dann gegenüber dem untergeordneten Verarbeiter nur hinsichtlich der Datenerhebung besteht, für die eine Auskunftserteilung jedenfalls grundsätzlich auch möglich sein sollte. Insgesamt lassen sich so die Fälle der zweiten Fallgruppe (*third-party tracking*) interessengerecht lösen.

(2) Datenübermittlung an Drittunternehmen (personalisierte Werbung)

Eine weitere Fallgruppe an Leitfällen betrifft die Übermittlung von Daten an Drittunternehmen und hier insbesondere einerseits den Einsatz von Daten zu

[328] Vgl. EuGH, Urt. v. 17.4.2008 – Rs. C-404/06 (*Quelle*) – Rn. 34 f.; EuGH, Urt. v. 23.5.2019 – Rs. C-52/18 (*Fülla*) – Rn. 40.

[329] So auch EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 102–106.

[330] So auch *Petri*, EuZW 2018, 540 (541).

Zwecken personalisierter Werbung (*ad exchanges*) und andererseits die Datenweiterleitung im Internet der Dinge.

(a) Werbenetzwerke (*ad exchanges*)

Im Fall der Werbenetzwerke (*ad exchanges*) geht es, wie oben ausgeführt,[331] um die Durchführung von Auktionen in Realzeit, mit denen bestimmt wird, welche Werbung für individuelle Nutzer auf einer bestimmten Webseite geschaltet wird. Auch hier bestehen abgrenzbare Verantwortungsbereiche, die nach den einzelnen Verarbeitungsschritten (vgl. Art. 4 Nr. 2 DS-GVO) unterschieden werden können. Die einzelnen Akteure (Anbieter der Content-Webseite; *ad exchange*; Werbetreibender) dürften im Regelfall jedenfalls größtenteils als separate, alleinige Verantwortliche für die jeweils durch sie durchgeführten Verarbeitungsschritte gelten, da sie keine gemeinsamen Zwecke verfolgen oder gemeinsame Mittel verwenden, sondern lediglich jeweils eigene Zwecke im Rahmen ihrer eigenen informationstechnischen Infrastruktur vornehmen.[332] Auch der Umstand, dass die *ad exchange* eine Plattform darstellt, auf der die Akteure suchkostenminimierend zusammengebracht werden können, ändert daran nichts, da es sich nicht um eine Infrastruktur handelt, welche die Akteure gemeinsam aufgebaut haben.[333]

Demnach zeichnet die *ad exchange* allein verantwortlich für die Übermittlung der Profilinformation an Werbetreibende sowie die Durchführung der Auktion und den Zuschlag mit Bezug auf das konkrete Kundenprofil. Die Verarbeitung des Profils zur Bestimmung des Höchstgebots bei der Auktion liegt wiederum im alleinigen Verantwortungsbereich des jeweiligen Werbetreibenden. Schwieriger zu bestimmen ist die Verantwortung des Inhabers der Webseite hinsichtlich der Übermittlung des Kundenprofils an die *ad exchange*. Dieses wird automatisiert von der *ad exchange* abgefragt durch Cookies oder andere Tracking-Technologien. Der Webseiteninhaber ermöglicht lediglich in technischer Weise diese automatisierte Übermittlung insofern, als er seine Webseite so konfiguriert, dass die Tracking-Instrumente wirksam eingebunden werden können.[334] Die Situation ist mithin derjenigen von Webseiten, die Social Plug-Ins verwenden, unmittelbar vergleichbar. Die Artikel-29-Datenschutzgruppe weist dem Webseiteninhaber und der *ad exchange* für die initiale Erhebung der Daten daher richtigerweise eine gemeinsame Verantwortung zu.[335]

---

[331] Siehe Text bei § 4, Fn. 156.

[332] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", 2010, 24.

[333] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", 2010, 24.

[334] *Artikel-29-Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, WP 171, 2010, 14.

[335] *Artikel-29-Datenschutzgruppe*, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, WP 171, 2010, 14; *Artikel-29-Datenschutzgruppe*, Stellungnahme

(b) Weiterleitung im Internet der Dinge

Im Internet der Dinge ist der Anbieter des jeweiligen IoT-Geräts jedenfalls insofern alleiniger Verantwortlicher, als er allein über eine Datenweiterleitung und -analyse zum Beispiel zu Werbezwecken oder zur Produktoptimierung entscheidet.[336] Bindet er externe Werbeunternehmen ein, so gilt dasselbe wie zu *ad exchanges* Gesagte; hier ist zwischen verschiedenen Akteuren im Ökosystem des Internets der Dinge streng zu unterscheiden.[337]

Ist jedoch der Nutzer selbst an der Datenverarbeitung dergestalt beteiligt, dass er über die Verarbeitung aktiv selbst entscheidet (zum Beispiel durch das Posten von Nutzerdaten eines Fitness-Wearables in sozialen Netzwerken über einen absolvierten Lauf), so ist der Nutzer selbst insofern Verantwortlicher. Teilweise wird hier eine gemeinsame Verantwortung angenommen.[338] In der Tat ist das erste der vom EuGH im Fall *Wirtschaftsakademie Schleswig-Holstein* verwendete Kriterium erfüllt (notwendige Bedingung der Verwendung des vom Anbieter in Verkehr gebrachten Produkts). Naheliegender dürfte es jedoch auch hier sein, zwischen verschiedenen Verarbeitungsschritten zu unterscheiden, etwa zwischen der im Gerät bzw. beim Anbieter oder in einer Cloud ablaufenden Datenanalyse und der davon vollkommen getrennten und damit auch nicht notwendig verbundenen Veröffentlichung von Informationen durch den Nutzer in sozialen Netzwerken. Ob und inwieweit Daten durch Nutzer derartig veröffentlicht werden, wird vom Anbieter der jeweiligen IoT-Geräte typischerweise nicht kontrolliert.[339] Anders liegt es jedoch, wenn sich die Veröffentlichung der Daten automatisiert aufgrund von Voreinstellungen vollzieht, welche der Geräteanbieter in das Gerät eingebunden hat. Dann ist von einer gemeinsamen Verantwortung von Anbieter und Nutzer auszugehen.[340]

(3) Datenerhebung bei Dritten

Von der gerade geschilderten Situation der Datenweiterleitung von Daten des Eigentümers oder jedenfalls unmittelbaren Nutzers eines IoT-Produkts zu unterscheiden sind die Fälle der dritten Fallgruppe, bei denen Daten durch ein IoT-Gerät erhoben werden, mit dem der Anbieter nicht in einem unmittelbaren

1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", 2010, 28.

[336] *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 13; *B. Wagner*, ZD 2018, 307 (309).

[337] *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 13 f.

[338] *B. Wagner*, ZD 2018, 307 (310 f.).

[339] Der Anbieter mag zwar Anreize dafür setzen und auch die Informationsumgebung auf derartige Veröffentlichungen ausrichten. Letztlich liegt aber die alleinige Letztentscheidungsgewalt typischerweise beim Endnutzer.

[340] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 13.

Nutzungsverhältnis steht. Dies kann etwa der Fall sein, wenn Daten von Besuchern oder Familienmitgliedern des unmittelbar Nutzungsberechtigten (versehentlich) verarbeitet werden.[341] Auch hier wird wieder zwischen den verschiedenen Verarbeitungsschritten zu differenzieren sein.

Eine gemeinsame Verantwortung des Eigentümers oder primär Nutzungsberechtigten einerseits und des Geräteanbieters andererseits kommt wiederum nur für die initiale Erhebung der Daten in Betracht. Eine notwendige Bedingung hat der primär Nutzungsberechtigte durch den Erwerb des Geräts jedenfalls erfüllt.[342] Eine hinreichende Kontrollmöglichkeit über die konkrete Erhebung dürfte seinerseits jedenfalls dann bestehen, wenn er entweder auf die Erhebung aktiv hingewirkt hat (zum Beispiel durch Überlassung des Geräts an Besucher oder Familienangehörige) oder er es unterlassen hat, das Gerät gegen Nutzung durch Dritte zu sichern, obwohl dies technisch (zum Beispiel durch eine PIN) möglich war. In beiden Fällen verhält es sich ähnlich wie bei der Einbindung eines Social Plug-Ins auf der eigenen Webseite: Indem das (ungesicherte) IoT-Gerät in die unmittelbare Lebensumgebung der Dritten eingeführt wird, leistet der Geräteinhaber einen signifikanten Beitrag zur Datenerhebung, über deren „Ob" er grundsätzlich Kontrollmöglichkeiten hat. Dies impliziert, dass Geräteinhaber jedenfalls hinsichtlich der Erhebung für datenschutzrechtswidrige Verarbeitung Adressat von Betroffenenrechten Dritter sein können.[343] Die davon ausgehende Anreizwirkung zum sorgsamen Umgang mit derartigen Geräten ist jedoch durchaus zu begrüßen, da die Geräteinhaber, gerade auch gegenüber dem Anbieter, typischerweise *least cost avoider* hinsichtlich der Vermeidung einer datenschutzrechtswidrigen Datenerhebung sein dürften.

c) Datenschutzrechtliche Störerhaftung als dritte Kategorie?

Diskutiert wird neben der aus Art. 4 Nr. 7 DS-GVO folgenden Verantwortlichkeit auch immer wieder eine davon unabhängige Verantwortung nach den Grundsätzen der Störerhaftung.[344] Demnach könnte eine natürliche oder juristische Person, auch wenn sie nicht Verantwortlicher nach Art. 4 Nr. 7 DS-GVO ist, Adressat von Betroffenenrechten sein, wenn sie Handlungs- oder Zustandsstörer ist (und die übrigen Voraussetzungen der Störerhaftung vorliegen), etwa wenn sie die Möglichkeit einer Verarbeitung durch Dritte lediglich kausal ermöglicht (und dies für die Annahme von Verantwortung nach Art. 4 Nr. 7 DS-GVO nicht hinreicht). Störer ist nach ständi-

[341] Siehe dazu oben, Text bei § 3, Fn. 191.

[342] Dies als ausreichend betrachtend *B. Wagner*, ZD 2018, 307 (309).

[343] Zu prüfen ist dann jeweils noch, ob die Haushaltsausnahme des Art. 2 Abs. 2 lit. c DS-GVO erfüllt ist, was bei Weiterleitung an IoT-Geräteanbieter jedoch regelmäßig zu verneinen ist, siehe *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 15; *B. Wagner*, ZD 2018, 307 (311); ferner bereits oben, Text bei § 4, Fn. 241.

[344] Siehe auch noch unten, § 5 C.III.1.

ger Rechtsprechung, wer – ohne Täter oder Teilnehmer zu sein – in irgendeiner Weise willentlich und adäquat-kausal zur Verletzung des geschützten Rechtsguts beiträgt.[345] Sowohl die EuGH-Vorlage des Bundesverwaltungsgerichts in Sachen *Wirtschaftsakademie Schleswig-Holstein* als auch jene des OLG Düsseldorf im *Fashion ID*-Verfahren beinhalteten explizit eine Frage zur Statthaftigkeit der Erstreckung zivilrechtlicher Haftung auf Akteure, die selbst nicht datenschutzrechtlich Verantwortliche sind.[346] Der EuGH ist in beiden Verfahren eine Antwort schuldig geblieben. GA *Bobek* hingegen hat in seinen Schlussanträgen zur Rechtssache *Fashion ID* der Störerhaftung wegen Ermöglichung der Verletzung datenschutzrechtlicher Pflichten (wohl) eine Absage erteilt.[347]

Eine derartige Ausweitung der Verantwortlichkeit lässt sich in der Tat mit der DS-GVO nicht vereinbaren.[348] Zwar hat der EuGH in einem *obiter dictum* eine zivilrechtliche Haftung von nicht datenschutzrechtlich Verantwortlichen grundsätzlich zugelassen.[349] Die Regelung in Art. 4 Nr. 7 DS-GVO ist jedoch nach hier vertretener Auffassung als abschließend zu betrachten,[350] sodass eine darüberhinausgehende Annahme von Verantwortlichkeit nach den Prinzipien der (öffentlich-rechtlichen oder zivilrechtlichen) Störerhaftung als direkter Verstoß gegen die DS-GVO zu werten wäre. Bei Grundlage der Störerhaftung im nationalen Recht stünde ihr mithin der Anwendungsvorrang des Unionsrechts entgegen; wollte man sie aus dem Unionsrecht selbst entwickeln, so widerspräche dies dem Vorrang der DS-GVO im Rahmen der im ersten Teil entwickelten Sachintegration, da mit der Frage der Verantwortlichkeit für den Verstoß gegen datenschutzrechtliche Pflichten eindeutig primär von der DS-GVO geregelte Risiken in Bezug genommen werden. In Betracht kommt eine zivilrechtliche Haftung daher nur insoweit, als sie an Rechtsverstöße anknüpft, die nicht in der DS-GVO abschließend geregelt sind. Der Hinweis des EuGH lässt sich denn auch in diesem Sinne verstehen.[351]

---

345 Siehe nur BGH MMR 2015, 674 – Rn. 49.

346 OLG Düsseldorf, ZD 2017, 334 Rn. 16; BVerwG, ZD 2016, 393 Rn. 31–36; siehe auch VG Schleswig, ZD 2014, 51 (54).

347 GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (Fashion ID) – Rn. 109 f.

348 So auch *Hanloser*, ZD 2019, 122 (123); *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 133; *B. Wagner*, ZD 2018, 307 (309); *Martini/Fritzsche*, NVwZ 2015, 1497 (1498), die jedoch eine Auswahlverantwortung annehmen; aA (Bejahung der Störerhaftung) *Petri*, ZD 2015, 103 (105); *Mantz*, ZD 2014, 62 (65).

349 EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 74.

350 So zur DSRL-Regelung VG Schleswig, ZD 2014, 51 (54); OVG Schleswig, ZD 2014, 643 (645); *Voigt/Alich*, NJW 2011, 3541 (3543).

351 EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 74: „unbeschadet einer etwaigen insoweit im nationalen Recht vorgesehenen zivilrechtlichen Haftung". Dies impliziert nicht, dass eine zivilrechtliche Haftung gerade für datenschutzrechtliche Verstöße zulässig ist, da sich „insoweit" richtigerweise lediglich auf den Umstand bezieht, dass der Passivlegitimierte nicht datenschutzrechtlich Verantwortlicher ist.

d) Ergebnis zur Verantwortlichkeit

Nach hier vertretener Ansicht ist somit streng zwischen einzelnen Verarbeitungsschritten zu differenzieren und hinsichtlich dieser jeweils zu fragen, ob hinreichende Kontrollmöglichkeiten für die Annahme gemeinsamer Verantwortung nach Art. 4 Nr. 7 DS-GVO bestehen. Kommt es dennoch zu einer Disjunktion von Kontrollmöglichkeiten und Verantwortung, insbesondere zu einer technischen Unmöglichkeit oder Unzumutbarkeit der Erfüllung von Betroffenenrechten, so ist Art. 26 Abs. 3 DS-GVO insoweit teleologisch zu reduzieren.

Zu betonen ist jedoch, dass diese teleologische Reduktion ihre Grenze im informationellen Schutzprinzip des Art. 26 Abs. 3 DS-GVO findet. Sie kann daher nur dann vollzogen werden, wenn für den Betroffenen objektiv erkennbar war, dass keine Kontroll- oder Erfüllungsmöglichkeiten bestanden. Ist unklar, ob dies objektiv erkennbar war, streitet im Zweifel der Betroffenenschutz gegen eine teleologische Reduktion von Art. 26 Abs. 3 DS-GVO: Diese Zielsetzung eines hohen Schutzniveaus wird schließlich auch vom EuGH betont.[352] Sofern dann subsidiär §275 Abs. 1 oder 2 BGB zur Anwendung kommen, dürfen dem Betroffenen daraus keine Kosten (etwa infolge der gerichtlichen Abweisung des Anspruches) entstehen. Insgesamt sollte eine einschränkende Auslegung von Art. 26 Abs. 3 DS-GVO jedoch darum bemüht sein, unterschiedlichen Rollenverteilungen und Einwirkungsmöglichkeiten in mehrstufigen Verhältnissen insoweit Rechnung zu tragen, wie dies mit einem effektiven Betroffenenschutz noch vereinbar ist. Eine Ausdehnung der Verantwortlichkeit über Art. 4 Nr. 7 DS-GVO hinaus im Wege der Störerhaftung schließlich ist abzulehnen.

2. Grundsätze der Datenverarbeitung

Neben der Frage der Verantwortlichkeit stellen die Grundsätze der Datenverarbeitung ein weiteres Basiskonzept des Datenschutzrechts dar, das als „Rückgrat des Datenschutzrechts“[353] nicht nur für die Auslegung der spezifischen datenschutzrechtlichen Pflichten, sondern auch für die hier interessierenden drei Leitfälle erhebliche Bedeutung hat.

a) Rechtscharakter der Grundsätze

Die Grundsätze der Datenverarbeitung, festgehalten in Art. 5 Abs. 1 DS-GVO, sind keine wohlfeile Aufzählung hehrer Prinzipien, sondern stellen echte, unmittelbar geltende Rechtspflichten dar.[354] Ein Verstoß gegen sie macht die Ver-

[352] EuGH, Urt. v. 5.6.2018 – Rs. C-210/16 (*Wirtschaftsakademie Schleswig-Holstein*) – Rn. 26.

[353] *Lynskey*, The Foundations of EU Data Protection Law, 2015, 35: „backbone“; siehe auch *Roßnagel*, ZD 2018, 339 (342): „wesentliche Zielsetzungen“.

[354] *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 1;

arbeitung rechtswidrig.[355] Adressat der Pflichten ist, nach Art. 5 Abs. 2 DS-GVO, jedenfalls[356] der im vorangegangenen Abschnitt ausführlich behandelte Verantwortliche. Dabei liegt ihr praktischer Schwerpunkt vor allem in der Anleitung der Interpretation spezifischer datenschutzrechtlicher Vorschriften,[357] welche die Prinzipien für bestimmte Fragestellungen konkretisieren und operationalisieren.[358]

Die Grundsätze selbst stellen damit eine mittlere Konkretisierungsebene zwischen der primärrechtlichen Gewährleistung des Datenschutzgrundrechts (Art. 8 GRCh, Art. 16 AEUV) und den spezifischen datenschutzrechtlichen Pflichten dar.[359] Dabei ist jedoch unbestreitbar, dass die Grundsätze selbst aufgrund ihres Abstraktionsgehalts von erheblicher Unschärfe gekennzeichnet sind.[360] Der Graubereich derjenigen Verarbeitungspraktiken, von welchen sich nicht unmittelbar und klar sagen lässt, ob sie gegen die Grundsätze verstoßen oder diese gerade noch einhalten, dürfte im Vergleich mit vielen spezifischen datenschutzrechtlichen Pflichten besonders hoch sein.[361]

Nichtsdestoweniger ist die Verletzung der Grundsätze der Datenverarbeitung als solche bußgeldbewehrt: Nach Art. 83 Abs. 5 lit. a DS-GVO kann als Geldbuße bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs eines Unternehmens verhängt werden. Die DS-GVO kennt ferner neben den in Art. 5 Abs. 1 DS-GVO festgehaltenen Grundsätzen noch weitere Prinzipien, die in anderen Normen ihren Niederschlag gefunden haben.[362] Sie mögen nicht in jedem Fall mit den Grundsätzen nach Art. 5 Abs. 1 DS-GVO auf einer Stufe stehen, haben aber dennoch insofern eine herausgehobene Stellung, als ihnen möglicherweise Leitbildcharakter im Rahmen von § 307 Abs. 2 Nr. 1 BGB zukommen kann.[363] Im hiesigen Kon-

---

Reimer, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 2; *Schantz*, in: BeckOK DatenschutzR, 28. Ed. 1.2.2019, Art. 5 DS-GVO Rn. 2; weitergehend *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 21: Optimierungsgebote; ebenso *Roßnagel*, ZD 2018, 339 (342).

355 *Roßnagel*, ZD 2018, 339 (343).

356 Ob Auftragsverarbeiter auch erfasst sind, ist umstritten, siehe etwa *Schantz*, in: BeckOK DatenschutzR, 28. Ed. 1.2.2019, Art. 5 DS-GVO Rn. 2.

357 Vgl. EuGH, Urt. v. 7.5.2009 – Rs. C-553/07 (*Rijkeboer*) – Rn. 65; *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (682 ff.); *Schantz*, in: BeckOK DatenschutzR, 28. Ed. 1.2.2019, Art. 5 DS-GVO Rn. 2; *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 15, 26.

358 *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 1.

359 Vgl. *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 20.

360 *Reimer*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 2; *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 21 f., 25.

361 Siehe dazu auch noch unten, § 5 C.II.1.e)bb)(1)(b).

362 *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 29.

363 Dazu unten, § 5 C.II.1.e)bb)(1)(b).

text ist insbesondere einerseits das Marktortprinzip (Art. 3 Abs. 2 DS-GVO) und andererseits das Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO) zu nennen. Diese wurden[364] bzw. werden[365] jedoch in dieser Arbeit separat behandelt. Die Verletzung insbesondere von Art. 25 DS-GVO ist ebenfalls bußgeldbewehrt nach Art. 83 Abs. 4 lit. a DS-GVO. In methodischer Hinsicht ist damit festzuhalten, dass einerseits die Grundsätze der Datenverarbeitung die Auslegung der sie konkretisierenden Normen prägen;[366] andererseits können diese Grundsätze, wenn der Wortlaut der Konkretisierung abschließend ist, für die durch die speziellere Norm geregelten Sachverhalte kein vom Geltungsinhalt dieser Norm abweichendes Ergebnis begründen. Ist eine Verarbeitung daher nach einer spezifischen Rechtsgrundlage, die einen Grundsatz abschließend konkretisiert, zulässig, so kann sie nicht unter Berufung auf eben diesen Grundsatz als rechtswidrig ausgewiesen werden.[367]

b) Die Grundsätze des Art. 5 Abs. 1 DS-GVO im Einzelnen

Im Folgenden sollen die einzelnen Grundsätze, in aller gebotenen Kürze, im Einzelnen vorgestellt und bereits in einem ersten Zugriff auf ihre Relevanz für die drei Leitfälle befragt werden.

aa) Art. 5 Abs. 1 lit. a Var. 1 DS-GVO: Legalität

Nach Art. 5 Abs. 1 lit. a Var. 1 DS-GVO müssen Daten rechtmäßig verarbeitet werden. Diesem Legalitätsprinzip kommt jedoch gegenüber Art. 6 DS-GVO sowie dem unmittelbaren Geltungsanspruch der sonstigen datenschutzrechtlichen Pflichten[368] kein eigenständiger funktionaler Gehalt zu abseits einer rein appellativen Verstärkung der Bedeutung des Vorbehalts des Gesetzes.[369] Er kann daher im Folgenden vernachlässigt werden.

bb) Art. 5 Abs. 1 lit. a Var. 2 DS-GVO: Treu und Glauben (*fairness*)

Von ungleich größerer Relevanz ist hingegen der in Art. 5 Abs. 1 lit. a Var. 2 DS-GVO verankerte Grundsatz der Datenverarbeitung nach Treu und Glauben (englisch: *fair data processing*). Vorab ist festzuhalten, dass der Begriff auf unionaler Ebene autonom, und nicht in unmittelbarer Übernahme etwa des

364 Siehe oben, § 4 A.II.1.b) zum Marktortprinzip.
365 Siehe unten, § 4 C.III. zu Art. 25 DS-GVO.
366 Siehe etwa EuGH, Urt. v. 1.10.2015 – Rs. C-201/14 (*Bara*) – Rn. 30 ff.
367 So auch *Roßnagel*, ZD 2018, 339 (342 f.).
368 Ob diese von Art. 5 Abs. 1 lit. a Var. 1 DS-GVO umfasst werden, ist umstritten, hier aber irrelevant; siehe zum Streit *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 8 ff.
369 *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 388–390; *Roßnagel*, ZD 2018, 339 (340).

Begriffs von Treu und Glauben aus § 242 BGB, bestimmt werden muss.[370] Insgesamt hätte sich, um Missverständnisse zu vermeiden, eine Übersetzung als Grundsatz „fairer" oder „angemessener" Datenverarbeitung, unter Verzicht auf die bürgerlich-rechtlich konnotierte Begrifflichkeit von „Treu und Glauben", angeboten.[371]

(1) Rechtsbereichsübergreifende Fairness jenseits von Transparenz

Hier besteht erheblicher Koordinierungsbedarf mit den übrigen, im positiven EU-Privatrecht verwurzelten Fairnessgeboten, nicht nur der Klauselrichtlinie,[372] sondern etwa auch der UGP-Richtlinie,[373] aber auch dem unional geprägten Antidiskriminierungsrecht. Zwar kann dies in der vorliegenden Studie nicht umfassend geleistet werden,[374] die konzeptuelle Abstimmung mit dem Verbot missbräuchlicher Klauseln wird allerdings einen Schwerpunkt des zivilrechtlichen Teils der Arbeit darstellen.[375] Bereits an dieser Stelle lässt sich jedoch vorzeichnen, dass gerade aufgrund der begrifflichen Übereinstimmung mit bzw. Nähe zu weiteren Fairnessbegriffen des Unionsrechts der datenschutzrechtliche Begriff seine inhaltliche Ausfüllung – zumindest auch – unter Rekurs auf diese weiteren Begriffe erhalten muss. Er wird nach diesem Verständnis zu einem potenziellen (und im Einzelfall immer zu spezifisch zu öffnenden) Einfallstor für Wertungen, die außerhalb des Datenschutzrechts im engeren Sinne liegen.[376]

---

[370] *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 13; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 20; *Roßnagel*, ZD 2018, 339 (340).

[371] *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 18; *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 14; siehe zur Varianz des Begriffs in den verschiedenen Sprachfassungen aber *Malgieri*, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 154 (160 ff.).

[372] Richtlinie 93/13/EWG des Rates vom 5. April 1993 über mißbräuchliche Klauseln in Verbraucherverträgen, ABl. 1993 L 95/29.

[373] Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates vom 11. Mai 2005 über unlautere Geschäftspraktiken im binnenmarktinternen Geschäftsverkehr zwischen Unternehmen und Verbrauchern und zur Änderung der Richtlinie 84/450/EWG des Rates, der Richtlinien 97/7/EG, 98/27/EG und 2002/65/EG des Europäischen Parlaments und des Rates sowie der Verordnung (EG) Nr. 2006/2004 des Europäischen Parlaments und des Rates (Richtlinie über unlautere Geschäftspraktiken), ABl. 2005 L 149/22.

[374] Siehe aber zum Verhältnis von datenschutzrechtlichem Fairnessgebot und Antidiskriminierungsrecht *Hacker*, 55 Common Market Law Review 2018, 1143 (1172 f.); *Zehlike/Hacker/Wiedemann*, 34 Data Mining and Knowledge Discovery 2020, 163 (188); *Zuiderveen Borgesius*, Strengthening legal protection against discrimination by algorithms and artificial intelligence, The International Journal of Human Rights 2020, DOI: 10.1080/13642987.2020.1743976, 1 (7 ff.); die Klärung des Verhältnisses von UGP-Richtlinie und datenschutzrechtlichem Fairnessgebot muss einer gesonderten Abhandlung vorbehalten bleiben; siehe aber zum methodischen Zusammenhang noch unten, § 5 A.II.; ferner auch knapp *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (719).

[375] Siehe unten, § 5 C.II.1.a), d), e) und besonders g).

[376] In diesem Sinne auch *Maxwell*, 5 International Data Privacy Law 2015, 205 (210);

Der Grundsatz der Verarbeitung nach Treu und Glauben war bereits in Art. 6 Abs. 1 lit. a Var. 1 DSRL enthalten. Er wurde, den Ausführungen im 38. Erwägungsgrund der DSRL folgend, vielfach in der Literatur[377] und auch vom EuGH interpretiert als formale Verpflichtung, die Transparenz der Datenverarbeitung sicherzustellen.[378] Nachdem die DS-GVO nunmehr aber mit Art. 5 Abs. 1 lit. a Var. 3 DS-GVO einen eigenständigen Transparenzgrundsatz erhalten hat, stellt sich mit besonderer Dringlichkeit die Frage der Neuinterpretation des Fairnessgebots. Fairness kann unter der DS-GVO nicht mehr auf Transparenz reduziert werden, da der Begriff sonst neben dem eigenständigen Transparenzgebot redundant wäre.[379] Dafür spricht in systematischer Hinsicht auch der Abgleich mit der JI-Richtlinie, in welcher der Grundsatz der Datenverarbeitung nach Treu und Glauben auch nicht mehr als Transparenz zu verstehen sein dürfte.[380]

(2) Inhaltliche Ausfüllung

Grundsätzlich kann Treu und Glauben bzw. Fairness eine prozedurale und eine substantielle Dimension annehmen.[381] In der Tat dürften viele der prozeduralen Normen der DS-GVO, so etwa die Informationspflichten, zumindest auch als Konkretisierung des Fairnessgebots angesehen werden.[382] Besonders fraglich erscheint demgegenüber, inwiefern dem Grundsatz von Treu und Glauben eine substantielle Dimension eignet, die über die spezifischen, in der DS-GVO

Hacker, 7 International Data Privacy Law 2017, 266 (277); *Hacker*, 55 Common Market Law Review 2018, 1143 (1172); *Malgieri*, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 154 (156); unentschieden *Butterworth*, 34 Computer Law & Security Review 2018, 257, (265 f.).

[377] Siehe nur die Übersicht bei *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (138–140).

[378] EuGH, Urt. v. 1.10.2015 – Rs. C-201/14 (*Bara*) – Rn. 34; in diesem Sinne auch für die DS-GVO noch *Wissenschaftliche Dienste – Deutscher Bundestag*, Zulässigkeit der Transkribierung und Auswertung von Mitschnitten der Sprachsoftware „Alexa" durch Amazon, WD 10 – 3000 – 032/19, Sachstand, 2019, 8 f.

[379] *Maxwell*, 5 International Data Privacy Law 2015, 205 (208); *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (159); *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 14 f.; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 20.

[380] Die JI-Richtlinie kennt weiterhin nur den Grundsatz von Treu und Glauben, nicht aber den der Transparenz. Ihr 26. Erwägungsgrund weist jedoch darauf hin, dass eine heimliche Datenerhebung insofern gerade möglich sein soll; siehe etwa *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 16.

[381] Siehe, zu Fairness als Begriff der politischen Philosphie, *Hooker*, in: Honderich (Hrsg.), The Oxford Companion to Philosophy, 2005, 287; *Rawls*, A Theory of Justice, 1999, 11; engeres, rein prozedurales Verständnis bei *Dworkin*, Law's Empire, 1986, 164 f.; zu Fairness als Rechtsbegriff der DS-GVO, *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (178 f.); vgl. auch *Fikentscher/Hacker/Podszun*, FairEconomy, 2013, 72–74; *Hacker*, Verhaltensökonomik und Normativität, 2017, 377–379.

[382] *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (139 f., 163); *Malgieri*, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 154 (157).

aufgestellten Pflichten hinausreicht. Richtigerweise dürfte es sich dabei letztlich um einen Auffangtatbestand für Formen der unangemessenen Datenverarbeitung handeln, die nicht (oder nicht notwendig) zugleich eine Verletzung spezifischer datenschutzrechtlicher Pflichten darstellen.[383] Besonders eine ungerechtfertigte, auf Datenverarbeitung basierende Diskriminierung indiziert dabei die Verletzung des Fairnessgrundsatzes.[384] Dabei ist jedoch, zur Bestimmung der Unangemessenheit, jeweils eine umfassende Interessenabwägung notwendig, die wiederum insbesondere die spezifischen datenschutzrechtlichen Pflichten, und deren im Einzelfall möglicherweise abschließenden Charakter, in den Blick nimmt.[385] Ein derartiges abwägungsbasiertes Verständnis offenbart auch eine durch das britische Data Protection Tribunal ergangene Entscheidung zum Fairnessgrundsatz unter der DSRL.[386]

Allerdings ist ein solcher Abwägungstatbestand für rein datenschutzrechtlich radizierte Fälle in systematischer Hinsicht von reduzierter Relevanz, da z. B. Art. 6 Abs. 1 lit. f, Art. 7 Abs. 4 und Art. 22 Abs. 3 DS-GVO ebenfalls Abwägungsvorgänge hinsichtlich der Frage der materiellen Rechtmäßigkeit der Datenverarbeitung erfordern. Zwar ist nicht auszuschließen, dass Konstellationen auftreten können, die nicht nach den genannten Normen zu entscheiden sind (etwa, wenn die Verarbeitung ausschließlich auf Art. 6 Abs. 1 lit. b DS-GVO gestützt wird). Sie dürften jedoch selten sein. Daraus erhellt, dass der Grundsatz von Treu und Glauben insbesondere aus der Verschränkung mit den übrigen, im europäischen Marktordnungsrecht enthaltenen Fairnessgeboten seine inhaltliche Konturierung erfahren dürfte.[387] Bei einem solchen Verständnis erweist sich der Grundsatz von Treu und Glauben als eine Scharniernorm, über welche Wertungen anderer Rechtsgebiete, sofern diese in einem konkreten Kontext in einem unmittelbaren Zusammenhang mit Datenverarbeitungsvorgängen stehen, gleichsam in die DS-GVO transplantiert werden können.

---

[383] *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, 145; *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 17; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 20; *Reimer*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 14; *Roßnagel*, ZD 2018, 339 (340); *Indenhuck/Britz*, BB 2019, 1091 (1093); *Buchner*, in: *Tinnefeld* et al. (Hrsg.), Einführung in das Datenschutzrecht, 7. Aufl., 2020, 22 (243).

[384] *Hacker*, 55 Common Market Law Review 2018, 1143 (1172 f.) m. w. N.; *Artikel-29-Datenschutzgruppe*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, WP 251 rev. 1, 2018, 11; *Malgieri*, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 154 (158 f.); siehe auch *CNIL*, How Can Humans Keep the Upper Hand? 2017, 49.

[385] Ähnlich abwägungsbasierte Interpretation bei *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (141); *Bygrave*, Data Protection Law, 2002, 58.

[386] *British Gas Trading v Data Protection Registrar*, Data Protection Tribunal (1998) DA98 3/49/2, 11, http://webarchive.nationalarchives.gov.uk/+/http:/www.dca.gov.uk/foi/bgtdec.pdf.

[387] Ähnliche Ansätze bei *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (170); *Indenhuck/Britz*, BB 2019, 1091 (1093); *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (690).

Letztlich hat der Grundsatz der Datenverarbeitung nach Treu und Glauben nach diesem Verständnis zwei unterschiedliche Dimensionen, eine datenschutzrechtsexterne und eine datenschutzrechtsinterne. Einerseits geht es um die Erfassung unangemessener Datenverarbeitung, die durch den Verstoß gegen „Fairnessgebote" anderer Rechtsgebiete indiziert werden. Andererseits kann ein Verstoß gegen Treu und Glauben auch dann angenommen werden, wenn aus datenschutzrechtsimmanenter Perspektive eine Unangemessenheit festgestellt wird, die jedoch nicht zugleich einen Verstoß gegen *spezifische* Pflichten des Datenschutzrechts darstellt.

cc) Art. 5 Abs. 1 lit. a Var. 3 DS-GVO: Transparenz

Der Transparenzgrundsatz aus Art. 5 Abs. 1 lit. a Var. 3 DS-GVO wurde im Zuge der Novellierung des unionalen Datenschutzrechts neu hinzugefügt; er fand sich noch nicht als eigenständiger Gesichtspunkt in der DSRL. Für das Datenschutzprivatrecht ist er in doppelter Hinsicht von Bedeutung. Zum einen belegt seine Existenz, dass sich, wie soeben gesehen, der Grundsatz der Datenverarbeitung von Treu und Glauben nicht mehr in der Herstellung von Transparenz erschöpfen kann. Zum anderen ist der Transparenzgrundsatz Signum des Versuchs, Datensouveränität vor allem durch die Ermöglichung einer informierten Entscheidung seitens der betroffenen Personen herzustellen.[388] So hat auch das Bundesverfassungsgericht eindringlich auf die Verknüpfung von Wissen hinsichtlich der Datenverarbeitung und Verhaltensfreiheit hingewiesen.[389] Transparenz bezieht sich dabei sowohl auf das „Ob" als auch das „Wie" der Datenverarbeitung.[390] Dadurch soll insbesondere die Rechtewahrnehmung ermöglicht werden; heimlichen Verarbeitungen wird eine Absage erteilt.[391] Insofern wird der Grundsatz durch die Informationspflichten und Auskunftsrechte, die sich aus Art. 4 Nr. 11 und Art. 12–15 DS-GVO ergeben, ganz maßgeblich konkretisiert.[392] Auch Zertifizierungen und Siegel, Art. 42 DS-GVO, können und sollen der Herstellung von Transparenz dienen (siehe 100. Erwägungsgrund der DS-GVO).

Hinsichtlich der drei Leitfälle ist Transparenz immer dann besonders problematisch, wenn Daten durch Dritte oder von Dritten erhoben werden.[393] Bei der Datenerhebung durch Dritte ist den betroffenen Personen häufig nicht be-

[388] Vgl. den 39. Erwägungsgrund der DS-GVO: „Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können."

[389] BVerfG NJW 1984, 419 (422) – Volkszählung; siehe auch bereits oben, § 3 B.II.2.a).

[390] Siehe nochmals den 39. Erwägungsgrund der DS-GVO.

[391] *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 18.

[392] Siehe nur, statt vieler, *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 52 ff.

[393] Siehe auch *Wissenschaftliche Dienste – Deutscher Bundestag*, Zulässigkeit der Tran-

wusst, dass neben derjenigen Entität, mit der ihr primäres Nutzungsverhältnis besteht, noch weitere Verarbeiter Daten erheben und analysieren. Hinsichtlich der Datenerhebung bei Dritten, etwa durch Audiomitschnitte von Nichteigentümern durch IoT-Geräte, ergeben sich ähnliche Problemstellungen. Insbesondere ist hier kritisch, wie überhaupt eine hinreichende Information und die Möglichkeit zu einer Einwilligung in solchen Konstellationen bewerkstelligt werden kann. Dies kann jedoch jeweils erst mit Bezug auf die konkreten, speziellen Informationspflichten der DS-GVO in den folgenden Abschnitten dieser Arbeit diskutiert werden. Insgesamt zeigt sich damit, dass nicht nur Informationsüberlastung und Komplexität,[394] sondern auch die Natur der vernetzten Datenerhebung in der digitalen Wirtschaft den Transparenzgrundsatz an seine Grenzen bringen.

dd) Art. 5 Abs. 1 lit. b DS-GVO: Zweckbindung

Ganz ähnlich stellt sich die Ausgangslage hinsichtlich des Zweckbindungsgrundsatzes dar, der in Art. 5 Abs. 1 lit. b DS-GVO verankert ist. Demnach müssen personenbezogene Daten für „festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden". Die Verzahnung mit dem Transparenzgrundsatz ist evident: Über die konkreten Zwecke muss informiert werden (Art. 13 Abs. 1 lit. c, Art. 14 Abs. 1 lit. c DS-GVO).

Auch hier ergeben sich einerseits Reibungspunkte mit den Möglichkeiten maschinellen Lernens, bestimmte, ursprünglich zu einem spezifischen Zweck erhobene Daten zu weiteren Zwecken zu nutzen, die zum Zeitpunkt der Datenerhebung noch nicht klar definiert sind (*secondary use*[395]).[396] Auch der Grundsatz der Zweckbindung ist jedoch andererseits in besonderer Weise konkretisiert durch die Verpflichtung, nach Art. 4 Nr. 11 DS-GVO eine Einwilligung jeweils nur beschränkt auf einen konkreten Fall und gem. Art. 6 Abs. 1 lit. a DS-GVO nur für bestimmte Zwecke einzuholen. Ferner ergibt sich eine enge Verbindung zu Art. 6 Abs. 4 DS-GVO, der die Verarbeitung zu neuen Zwecken in besonderer Weise regelt. Diese ist nicht etwa generell unzulässig, aber bestimmten Anforderungen unterworfen, vor allem der Vereinbarkeit des neuen mit (mithin der wertenden Nähe zu) dem ursprünglichen Zweck.[397] Ähnlich

skribierung und Auswertung von Mitschnitten der Sprachsoftware „Alexa" durch Amazon, WD 10 – 3000 – 032/19, Sachstand, 2019, 8 f.

[394] Dazu umfassend, mit Bezug auf vertragliche Pflichtinformationen, *Hacker*, Verhaltensökonomik und Normativität, 2017, besonders §§ 4, 9 und 10.

[395] Zu *secondary use* etwa *Mayer-Schönberger/Cukier*, Big Data: A revolution that will transform how we live, work, and think, 2013, Kapitel 6.

[396] *Roßnagel*, ZD 2013, 562 (564); *von Grafenstein*, DuD 2015, 789; *Buchner*, DuD 2016, 155 (156 f.); *Culik/Döpke*, ZD 2017, 226.

[397] *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 24; *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 97.

wie beim Transparenzgrundsatz lassen sich auch die in Verbindung mit dem Zweckbindungsgrundsatz auftretenden Probleme daher am besten an den konkreten Normen, welche den Grundsatz verwirklichen, lösen.

ee) Art. 5 Abs. 1 lit. c DS-GVO: Datenminimierung

Mit dem Zweckbindungsgrundsatz wiederum eng verbunden ist der Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO.[398] Er statuiert letztlich, was bislang wenig Beachtung gefunden hat,[399] einen abgeschwächten Verhältnismäßigkeitsgrundsatz, bei dem der jeweilige Verarbeitungszweck als legitimer Zweck die Richtschnur abgibt. Personenbezogene Daten müssen, mit Blick auf diesen Zweck, (i) erheblich sein, (ii) auf das notwendige Maß beschränkt und (iii) angemessen (engl.: *adequate*).

Dies zeigt zugleich, dass nicht jede besonders weitgehende Datenerhebung und Verarbeitung einen Verstoß gegen den Grundsatz der Datenminimierung darstellt.[400] Minimierung bedeutet daher nicht, die Sammlung personenbezogener Daten gegen null konvergieren zu lassen.[401] Zwar ist mit Blick auf diesen Grundsatz die besonders umfangreiche Sammlung, Verbreitung oder Analyse von personenbezogenen Daten in der Tat kritisch; dies betrifft insbesondere, wenngleich nicht nur, die erste Fallgruppe der Leitfälle. Allerdings muss in jedem Einzelfall letztlich abgewogen werden, inwiefern der Verarbeitungszweck die jeweilige Datenanalyse trägt. Minimierung kann also nur statthaben unter der Randbedingung, dass der jeweilige Zweck (gerade noch) erreicht werden kann. Insbesondere müssen alle Möglichkeiten ausgeschöpft werden, die Analyse mithilfe nicht personenbezogener Daten durchzuführen.[402] Damit ergibt sich auch unter Geltung der DS-GVO eine rechtliche Präferenz für die

---

[398] Zu diesem Grundsatz ausführlich *von Grafenstein*, DuD 2015, 789.

[399] Für eine Verhältnismäßigkeitsprüfung auch *Schantz*, in: BeckOK DatenschutzR, 28. Ed. 1.2.2019, Art. 5 DS-GVO Rn. 24; zurückgenommener *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 58: zusammengefasst als „zur Erreichung des festgelegten Verarbeitungszwecks erforderlich"; ablehnend *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 5 Rn. 22; Anklänge bei *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 116: Beschränkung der Eingriffstiefe in das Datenschutzgrundrecht.

[400] Vgl. *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, 2014, 584f.

[401] *Roßnagel et al.*, Datensparsamkeit oder Datenreichtum? Zur neuen politischen Diskussion über den datenschutzrechtlichen Grundsatz der Datensparsamkeit, Policy Paper des Forums „Privatheit und selbstbestimmtes Leben in der digitalen Welt", 2017, 3; *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 128.

[402] *Roßnagel et al.*, Datensparsamkeit oder Datenreichtum? Zur neuen politischen Diskussion über den datenschutzrechtlichen Grundsatz der Datensparsamkeit, Policy Paper des Forums „Privatheit und selbstbestimmtes Leben in der digitalen Welt", 2017, 4; *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 125; *Schantz*, in: BeckOK DatenschutzR, 28. Ed. 1.2.2019, Art. 5 DS-GVO Rn. 25.1; *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, 2014, 585.

Pseudo- oder, wo möglich, gar Anonymisierung.[403] Die Daten bzw. die Verarbeitung müssen dabei zunächst, wie dies von der Prüfung der Verhältnismäßigkeit bekannt ist, grundsätzlich geeignet sein, diesen Zweck überhaupt zu fördern („erheblich").[404] Ferner dürfen sie nicht über das zur Erreichung dieses Zwecks erforderliche Maß hinausgehen („das […] notwendige Maß", Art. 5 Abs. 1 lit. c DS-GVO). Art. 6 Abs. 1 lit. c DSRL hatte demgegenüber lediglich verlangt, dass die Verarbeitung nicht exzessiv sein darf (besonders deutlich in der englischen Fassung: „not excessive in relation to the purposes for which they are collected and/or further processed").[405]

Schließlich müssen die Daten bzw. Verarbeitungsweisen im engeren Sinne mit den Interessen der betroffenen Personen und den Wertungen des Datenschutzrechts im Einklang stehen, was einen Ausgleich mit den grundsätzlich auf Verarbeitung dringenden Interessen und Chartagrundrechten der jeweiligen Verantwortlichen bedingt („angemessen"). Zwar hat sich der Rat bei den Verhandlungen zur DS-GVO mit seinem Vorschlag, ausdrücklich einen zweckbezogenen Verhältnismäßigkeitsgrundsatz aufzustellen, nicht durchsetzen können.[406] Daher wird man „angemessen" nicht als synonym zu „verhältnismäßig im engeren Sinne" interpretieren können. Auch die englische Sprachfassung spricht lediglich von „adequate", nicht von „proportionate". Allerdings bedingt nach hiesigem Verständnis die Erwähnung der Angemessenheit durchaus, dass, über die reine Erforderlichkeit hinaus, letztlich eine Abwägung stattfinden muss, die danach fragt, ob die Daten für den Zweck, unter Berücksichtigung entgegenstehender Belange des Betroffenen oder Dritter, sachgerecht sind.[407] Schlussendlich wird dies der EuGH zu entscheiden haben.

Die Datenverarbeitung auch durch Private wird damit zwar nicht einem generellen,[408] wohl aber einem auf den Zweck bezogenen, Abwägungsgebot unterworfen. Aufgrund der offenen Form des Abwägungsprozesses lässt sich nicht in jedem Fall mit Sicherheit ex ante sagen, ob der Grundsatz der Datenminimierung eingehalten wurde oder nicht.[409] Der Zweck kann aber jedenfalls

[403] *Schantz*, NJW 2016, 1841 (1841 f.); *Schantz*, in: BeckOK DatenschutzR, 28. Ed. 1.2.2019, Art. 5 DS-GVO Rn. 25.1.; für die DSRL bereits *Caspar*, ZRP 2015, 233 (234); *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, 2014, 585.

[404] So auch *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 58.

[405] *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 5 Rn. 22; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 37.

[406] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 117.

[407] Ähnlich *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 119: „sachgerecht"; *Schantz*, in: BeckOK DatenschutzR, 28. Ed. 1.2.2019, Art. 5 DS-GVO Rn. 26: „wertende Betrachtung"; enger *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 35: „Zuordnung zu den Zwecken [kann] nicht beanstandet werden".

[408] Siehe aber zur unmittelbaren Adressierung Privater durch Art. 8 GRCh noch unten, § 5 C.III.4.a)aa).

[409] Vgl. *Roßnagel*, ZD 2018, 339 (342).

nach hier vertretener Auffassung auch in der Personalisierung der Funktionsweise eines Produkts mithilfe von Techniken maschinellen Lernens liegen, so dass darauf ausgerichteten (Big Data) Analysen nicht von vornherein ein Riegel vorgeschoben ist.[410]

Der Grundsatz der Datenminimierung wird schließlich, zumindest partiell, operationalisiert durch die Verpflichtung auf *privacy by design and by default*, Art. 25 DS-GVO. Ferner lassen sich auch die Löschungspflichten nach Art. 17 DS-GVO sowie das Recht auf die Beschränkung der Datenverarbeitung nach Art. 18 DS-GVO als Ausflüsse des Grundsatzes der Datenminimierung lesen.[411] Auch diese Normen werden in den folgenden Abschnitten genauer beleuchtet. Schließlich fällt die strukturelle Verwandtschaft zum Erlaubnistatbestand in Art. 6 Abs. 1 lit. f DS-GVO auf. Sofern hiernach bereits eine Abwägung der jeweiligen Interessen und Grundrechte notwendig ist, entfaltet der Grundsatz der Datenminimierung, jedenfalls grundsätzlich, keine darüberhinausgehende Wirkung. Ihm kommt jedoch eine eigenständige Bedeutung zu, wenn die Datenverarbeitung auf andere Erlaubnistatbestände gestützt wird.[412]

ff) Art. 5 Abs. 1 lit. d-f DS-GVO: Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit

Die verbleibenden Grundsätze nach Art. 5 Abs. 1 lit. d-f DS-GVO (Richtigkeit; Speicherbegrenzung; Integrität und Vertraulichkeit) sind allesamt für die Leitfragen dieses Teils weniger relevant. Der Grundsatz der Richtigkeit personenbezogener Daten ist besonders als technische Vorfrage für mögliche Diskriminierungen, die aus systematisch fehlerhaft erhobenen Daten folgen können, von Bedeutung.[413] Ferner lassen sich daraus Anforderungen für Datenqualität ableiten, was für maschinelles Lernen bedeutsam ist, hier jedoch nicht weiter verfolgt werden kann.[414] Der Grundsatz der Speicherbegrenzung behandelt ebenfalls eine eher hinsichtlich der technischen Umsetzung relevante Frage. Schließlich ist der Grundsatz der Sicherheit der Datenverarbeitung, wie bereits bei den Risiken der vernetzten Datenerhebung angesprochen, ein zentrales Problem gerade im Bereich des Internets der Dinge. Damit befasst sich

---

[410] aA offenbar *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 135.

[411] Für Art. 18 DS-GVO auch *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 38.

[412] Explizit auch für die Einwilligung *Schantz*, in: BeckOK DatenschutzR, 28. Ed. 1.2.2019, Art. 5 DS-GVO Rn. 26.

[413] Grundsätzlich zur Auslegung dieses Grundsatzes, gerade auch im Bereich maschinellen Lernens, *Hoeren*, ZD 2016, 459.

[414] Dazu *Hoeren*, ZD 2016, 459; *Hoeren*, MMR 2016, 8; *Hacker*, A Legal Framework for AI Training Data, 13 Law, Innovation and Technology (im Erscheinen), https://ssrn.com/abstract=3556598.

das eigenständige Gebiet der IT-Sicherheit, dass hier jedoch aus Platzgründen ebenfalls außen vor bleiben muss.[415]

c) Zusammenfassung zu den Grundsätzen der Datenverarbeitung

Zusammenfassend lässt sich damit festhalten, dass insbesondere zwei Grundsätze der Datenverarbeitung für die Leitfragen dieses zweiten Teils der Arbeit besondere Relevanz besitzen. Einerseits kann der Grundsatz der Datenverarbeitung nach Treu und Glauben als eine Scharniernorm interpretiert werden, durch die fairnessrelevante Wertungen anderer Rechtsbereiche für das Datenschutzrecht fruchtbar gemacht werden können. Andererseits inkorporiert der Grundsatz der Datenminimierung einen Verhältnismäßigkeitsgrundsatz, bei dem bezogen auf den spezifischen Zweck der Datenverarbeitung jeweils, sofern nicht nach den jeweiligen sonstigen Normen ohnehin notwendig, Abwägungen zwischen den Interessen und Grundrechten der Datenverarbeiter und jenen der Betroffenen durchzuführen sind.

Darüber hinaus sind die hier interessierenden Grundsätze der Datenverarbeitung im Wesentlichen durch spezielle Vorschriften in den übrigen Teilen der DS-GVO umgesetzt. Bei der Besprechung dieser jeweiligen Normen werden sie im Folgenden auch behandelt.

B. Ermöglichende Strukturen im Datenschutzrecht

Normen des Privatrechts lassen sich in mannigfacher Weise einteilen. Für die Zwecke der Marktregulierung ist, wie oben ausgeführt, die Unterscheidung zwischen Vorschriften mit primär ermöglichender Funktion und solchen mit primär regulatorischer Funktion essenziell.[416] Das Datenschutzrecht ist gekennzeichnet durch ein vor allem in Art. 6 Abs. 1 DS-GVO verortetes Verbot mit Erlaubnisvorbehalt.[417] Ihm eignet daher primär eine regulatorische Dimension. Allerdings beinhaltet es auch Ermöglichungsstrukturen, die Räume zur privatautonomen Rechtsgestaltung vorhalten, ja diese zum Teil auch explizit fördern und unterstützen sollen. Darin liegt der Kern eines, im Folgenden noch weiter zu entwickelnden, Datenermöglichungsrechts.

Diese Regelungen finden sich primär in den Erlaubnistatbeständen von Art. 6 Abs. 1 lit. a und b DS-GVO, welche Datenverarbeitungen auf Grundlage einer

[415] Siehe dazu etwa den Überblick bei *Djeffal*, MMR 2019, 289.

[416] Siehe oben, § 1 C. und § 1 D.I.

[417] Siehe nur *Ziegenhorn/von Heckel*, NVwZ 2016, 1585 (1586); *von Grafenstein*, DuD 2015, 789 (795); *Buchner*, DuD 2016, 155 (157); *Langhanke*, Daten als Leistung, 2018, 31; *Veil*, NVwZ 2018, 686 (688); *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 184 f.; gegen diese Begrifflichkeit nunmehr *Roßnagel*, NJW 2019, 1 (4 f.) („Erlaubnisprinzip"); von dieser terminologischen Nuance hängt in dieser Arbeit indes nichts ab.

Einwilligung oder eines Vertrags legitimieren.[418] Die verschiedenen Voraussetzungen der Einwilligung – ihre Unmissverständlichkeit und Bestimmtheit, besonders aber ihre Informiertheit und Freiwilligkeit – verfolgen zumindest auch das Ziel, die privatautonome Ausübung von Kontrolle über die Verarbeitung personenbezogener Daten zu stärken.[419] Sie sind damit zum einen Zulässigkeitsvoraussetzungen für die Datenverarbeitung, andererseits aber eben auch, zumindest partiell, auf die Ermöglichung bewusster (Unmissverständlichkeit, Bestimmtheit), auf einem eigenen Willensentschluss basierender (Freiwilligkeit) und informierter Entscheidungen (Informiertheit) ausgerichtet. Lediglich Art. 6 Abs. 1 lit. b DS-GVO ist eher permissiv und importiert gewissermaßen die autonomiefördernden Ermöglichungsstrukturen des allgemeinen Privatrechts.[420] Die Entscheidung über den Vertragsschluss wird aber zugleich auch noch von den Informationspflichten der Art. 12 ff. DS-GVO gestützt, die ja auch hinsichtlich der vertragserforderlichen Datenverarbeitung erfüllt werden müssen. Auch wenn die genuin ermöglichenden Strukturen im allgemeinen Privatrecht, schon aufgrund der dortigen Umkehrung des Verbots mit Erlaubnisvorbehalt in eine Erlaubnis privatautonomer Gestaltung mit Verbotsvorbehalt,[421] stärker ausgeprägt sind als im Datenschutzrecht, so lassen sich doch auch Art. 6 Abs. 1 lit. a und b DS-GVO als Einfallstore für Privatautonomie verstehen.

Jedenfalls ihrer Zielsetzung nach sind ferner auch die Informationspflichten der Art. 12–15 DS-GVO schwerpunktmäßig unter die Normen mit Ermöglichungsfunktion zu zählen. Informationspflichten nehmen bekanntermaßen eine Zwitterstellung zwischen ermöglichenden und regulatorischen Normen ein.[422] Einerseits korrigieren sie Informationsasymmetrien und sind daher hinsichtlich Suchgütern notwendig für die wirksame Inanspruchnahme von Privatautonomie. Andererseits legen sie einen zwingenden regulatorischen Rahmen fest, welche die Handlungsfreiheit des Verpflichteten einengt. Hier werden sie im Rahmen der Diskussion der Einwilligung, die ja nach Art. 4 Nr. 11 DS-GVO in informierter Weise abgegeben werden muss, soweit notwendig behandelt. Eine besondere Bestimmung, welche die privatautonome Gestaltung von Datenaustauschvorgängen gerade durch Nutzer ins Werk setzen soll, findet sich schließlich in Art. 20 DS-GVO mit dem Recht auf Datenübertragung. Dadurch wird Wahlfreiheit aktiv gefördert.

---

[418] *Albrecht*, CR 2016, 88 (92).

[419] Vgl. nur den zweiten Satz des siebten Erwägungsgrunds der DS-GVO; die Einwilligung als Kern privatautonomer Gestaltung im Datenschutzrecht betrachtend auch *Sattler*, JZ 2017, 1036 (1039); *Sattler*, in: Ochs et al. (Hrsg.), Die Zukunft der Datenökonomie, 2019, 1 (16 ff.); siehe auch noch unten, § 4 B.I.1.

[420] Siehe unten, § 4 B.II.1.

[421] *Sattler*, JZ 2017, 1036 (1038); siehe auch *Emmerich*, in: MüKo, BGB, 8. Aufl. 2019, § 311 Rn. 1.

[422] Dazu ausführlich *Hacker*, Verhaltensökonomik und Normativität, 2017, 277 f., 404 ff.

Die nähere Untersuchung wird jedoch erweisen, dass auch diese Normen mit Ordnungselementen wertender Natur durchsetzt sind, welche der Ausübung von Privatautonomie bereits aus genuin datenschutzrechtlicher Sicht Grenzen setzen. Dies gilt sowohl für die Einwilligung (I.) wie auch die vertragserforderliche Datenverarbeitung (II.), in geringerem Umfang jedoch auch für das Recht auf Datenübertragung (III.).

I. Die Einwilligung und ihre Schranken: Reibungspunkte zwischen Privatautonomie und Regulierung

Dreh- und Angelpunkt der Diskussion um Nutzen und Nachteil des Datenschutzrechts gerade in Situationen des Marktaustauschs ist traditionellerweise die Einwilligung. Aus rechtspolitischer und empirischer Sicht ist die Einwilligung stark kritisiert worden, vielfach auch zu Recht. Diese Kritik wird unten aufgenommen[423] und muss in der Tat für die Konzeption eines Marktordnungsrechts für die Datenwirtschaft entscheidend beherzigt werden. Zunächst jedoch soll, nach einem kurzen Blick auf den Ermöglichungscharakter der Einwilligung (1.) und ihr Verhältnis zum Vertrag (2.), der Frage nachgegangen werden, inwieweit der Grundtatbestand der Einwilligung in der DS-GVO (3.) sowie die Regelung der Cookie-Einwilligung (4.) eigenständige Mechanismen beinhalten, um den in § 3 genannten Gründen des Marktversagens in datengetriebenen Austauschprozessen, besonders in den drei Leitfällen, entgegenzuwirken. Dies legt die Grundlage für die Behandlung der dogmatischen Verzahnungen zwischen den Einwilligungstatbeständen des Datenschutzrechts und dem BGB in einem späteren Kapitel der Arbeit (§ 5 B.II.).

1. Ermöglichungscharakter

Der Ermöglichungscharakter der Einwilligung ist durchaus zu bejahen.[424] Nicht nur gibt sie den Nutzern als permissive Regelung grundsätzlich die Möglichkeit, frei und autonom zu entscheiden, ob eine Verarbeitung erlaubt werden soll; sondern die einzelnen Voraussetzungen der Einwilligung können, wenngleich auch in unterschiedlichem Umfang, jeweils wie gesehen auch als aktive Förderung einer freien, bewussten und informierten Entscheidung verstanden werden.[425] Dabei können die betroffenen Personen in Rechnung stellen, inwiefern die im Gegenzug angebotenen Leistungen ihnen die Datenverarbeitung zu rechtfertigen erscheinen.

Während die Einwilligung im öffentlich-rechtlichen Bereich eher selten ist (vgl. 43. Erwägungsgrund DS-GVO), stellt sie jedenfalls nach der gesetzgeberischen Konzeption das zentrale Instrument der Kontrolle und Souveränität der

[423] Siehe unten, § 4 B.I.5. und § 6 C.
[424] Siehe etwa *Lynskey*, The Foundations of EU Data Protection Law, 2015, 185 ff.
[425] Siehe oben, Einleitung zu § 4 B.

Datenverarbeitung durch den Nutzer in privatrechtlichen Kontexten dar.[426] Allerdings ist zu beachten, dass die Einwilligung, selbst wenn sie optimal genutzt wird, privatautonome Rechtsgestaltung zu fördern, jedoch nicht zu verbürgen vermag. Denn die Ablehnung der Einwilligung in die Verarbeitung führt grundsätzlich nicht zu einem Verbot der Verarbeitung, da ein anderer Erlaubnistatbestand des Art. 6 Abs. 1 DS-GVO greifen kann.[427]

Hinzu kommt, dass der Ermöglichungscharakter der Einwilligung durch die bereits angesprochenen (verhaltens-)ökonomischen Effekte erheblich limitiert wird.[428] Einwilligungen werden ubiquitär erteilt und sind häufig in Nutzungsbedingungen versteckt. Diese Praktiken seitens der datenschutzrechtlich Verantwortlichen sind jedoch, wie die folgenden Ausführungen erweisen, nicht in allen Fällen rechtskonform. Die folgenden Abschnitte gehen daher der Frage nach, inwiefern die Einwilligung ihr Versprechen von Kontrolle und Souveränität entfalten kann, wenn ihre Voraussetzungen konsequent durchgesetzt werden.

2. Zum Verhältnis von Einwilligung und Vertrag

Bevor jedoch die einzelnen Voraussetzungen der datenschutzrechtlichen Einwilligung beleuchtet werden können, muss geklärt werden, in welchem Verhältnis sie zu einem etwaigen Vertrag zwischen betroffener Person und Verantwortlichem steht. Dies ist insbesondere relevant, wenn im Rahmen des Geschäftsmodells des Verantwortlichen Daten als Gegenleistung fungieren oder die Parteien über einen Nutzungsvertrag hinsichtlich eines IoT-Geräts verbunden sind.

In der Literatur wird von einigen Stimmen eine Integration von Einwilligung und schuldrechtlichem Vertrag befürwortet.[429] So sei zwischen einer einseitigen Einwilligung, die außerhalb eines Vertragskontextes abgegeben wird, und einer „schuldvertraglichen“[430] bzw. „schuldrechtlichen Einwilligung“[431] zu unterscheiden, die im Kontext eines Vertragsschlusses erklärt wird. Auch wenn die dogmatischen Konsequenzen nicht immer klar aufgezeigt werden, liegt dem die Auffassung zugrunde, dass die Einwilligung in letzterem Fall mit dem Vertrag untrennbar verbunden ist und eine echte rechtsgeschäftliche Willenserklärung darstellt. Die Einwilligung werde dann „Bestandteil

---

[426] Vgl. *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 18–20; *Engeler*, ZD 2018, 55 (56).

[427] Inwiefern ein Rückgriff auf andere Tatbestände gesperrt ist, wird allerdings in der Literatur unterschiedlich beurteilt, siehe Text bei § 4, Fn. 637 ff.

[428] Siehe unten, § 4 B.I.5.

[429] *Bräutigam*, MMR 2012, 635 (636); *Helle*, AfP 1985, 93 (99) für die kunsturheberrechtliche Einwilligung; wohl auch *Frömming/Peters*, NJW 1996, 958 (958) für die medienrechtliche Einwilligung; Übersicht über das Meinungsspektrum vor Geltungsbeginn der DS-GVO bei *Langhanke*, Daten als Leistung, 2018, 148 ff.

[430] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 232, 237, 253.

[431] *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 44.

eines umfassenderen schuldvertraglichen Rechtsverhältnisses" und sei daher „als schuldvertragliche Einwilligung einzuordnen".[432]

Dies kann jedoch aus verschiedenen Gründen nicht überzeugen. Vielmehr ist zwischen der Einwilligung einerseits und dem Vertragsschluss andererseits in dogmatischer Hinsicht scharf zu unterscheiden, auch wenn beide selbstverständlich in zeitlicher und sachlicher Hinsicht eng verknüpft und auch in derselben Urkunde enthalten sein können – aber nicht müssen. Dies ist bereits ein erstes Indiz für die notwendige Trennung zwischen beiden Instrumenten.[433] Die grundsätzliche Trennung und Abstraktheit[434] der Einwilligung von dem mit dem Verantwortlichem abgeschlossenen Vertrag ist ferner schon deshalb zwingend, weil für den Abschluss und die Wirksamkeit der beiden Instrumente jeweils gänzlich unterschiedliche Rechtsregime gelten. Die Einwilligung beurteilt sich, jedenfalls primär, nach verschiedenen Vorschriften der DS-GVO (dazu sogleich unter 3.). Der Vertragsschluss jedoch ist durch die DS-GVO (und im Übrigen auch die DIDD-Richtlinie[435] und die Warenkauf-Richtlinie[436]) gar nicht geregelt. Für ihn gilt daher nationales Vertragsrecht (dazu unten, § 5 B.III.). Wollte man die Einwilligung in den Vertrag selbst dogmatisch integrieren, so müsste diese Aufspaltung zwischen den verschiedenen Regelungsebenen überwunden werden.

Ferner unterscheidet auch die DS-GVO selbst in Art. 6 Abs. 1 lit. a und b klar zwischen Einwilligung einerseits und einem auf Datenverarbeitung abzielenden Vertrag andererseits. Schließlich ist nicht ersichtlich, weshalb die Rechtsnatur und die sonstige dogmatische Ausprägung der Einwilligung davon abhängen sollte, in welchem Kontext sie abgegeben wird.[437] Nach hier vertretener Auffassung ist die Einwilligung lediglich geschäftsähnliche Handlung und kein einseitiges Rechtsgeschäft, da ihre Rechtsfolgen kraft Gesetzes (Art. 6 Abs. 1 lit. a DS-GVO) eintreten und nicht, weil sie gewollt sind.[438] Der Vertrag, sei er auch für die Datenverarbeitung relevant, ist jedoch zweifellos Rechtsgeschäft.

Dies bedeutet freilich nicht, dass keine Verbindungen zwischen Einwilligung und Vertrag bestehen könnten. Ganz im Gegenteil kann vertraglich die

---

[432] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 237.

[433] *Langhanke*, Daten als Leistung, 2018, 150.

[434] Zur Geltung des Abstraktionsprinzips zwischen datenschutzrechtlicher Einwilligung und Vertrag *Metzger*, AcP 216 (2016), 817 (831 f.); *Specht*, JZ 2017, 763 (765 f.); *Langhanke*, Daten als Leistung, 2018, 163 ff.; *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.4.; differenzierend zwischen Einwilligungstypen, aber ohne Rekurs auf die datenschutzrechtliche Einwilligung, *Ohly*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, 2002, 448 ff.

[435] Art. 3 Abs. 10 der DIDD-Richtlinie.

[436] Art. 3 Abs. 6 der Richtlinie (EU) 2019/771 des Europäischen Parlaments und des Rates vom 20. Mai 2019 über bestimmte vertragsrechtliche Aspekte des Warenkaufs, ABl. L 136/28.

[437] *Riesenhuber*, RdA 2011, 257 (258).

[438] Dazu unten, § 5 B.II.1.a).

Abgabe einer Einwilligung versprochen und diese Abgabe auch (ebenso wie die Überlassung von personenbezogenen Daten) in den Rang einer Gegenleistung erhoben werden (siehe unten, § 5 B.I.).[439] Allein diese Verknüpfung zeigt jedoch, dass eine Trennung und Abstraktion zwischen Vertrag und Einwilligung vorzugswürdig ist: die Einwilligung ist in diesem Fall Erfüllung des vertraglichen Leistungsversprechens (oder der vertraglichen Bedingung) und mit diesem (oder dieser) gerade nicht identisch.[440]

3. Grundtatbestand: Art. 6 Abs. 1 lit. a DS-GVO

Um nachzuvollziehen, inwiefern die Einwilligung ihrem theoretischen Ermöglichungscharakter auch praktisch gerecht werden kann, müssen zunächst die dogmatischen Strukturen der Einwilligung geklärt und diese auf die drei Leitfälle angewendet werden. Die Dringlichkeit solcher Klärung erwächst nicht zuletzt aus dem ersten durch die französische Datenschutzbehörde wegen eines Verstoßes gegen die DS-GVO verhängten Bußgeld: Google wurde mit einem Bußgeld in Höhe von € 50 Mio. belegt wegen verschiedener Verstöße gegen Kriterien des Einwilligungstatbestands, vor allem im Kontext personalisierter Werbung (dazu unten, S. 170 ff.). Auf diese Entscheidung wird daher im Rahmen des ersten Leitfalls immer wieder zurückzukommen sein.

Die Vorschriften zur Einwilligung sind auf verschiedene Normen der DS-GVO, des BDSG und auch des UWG verteilt. Die zentrale Konsequenz – die Rechtmäßigkeit der von der Einwilligung umfassten Datenverarbeitung – findet sich in Art. 6 Abs. 1 lit. a DS-GVO. Die eigentliche Legaldefinition des Grundtatbestands der Einwilligung jedoch ist in Art. 4 Nr. 11 DS-GVO verortet (a)). Hinzu kommen weitere Wirksamkeitsvoraussetzungen für spezifische Verarbeitungssituationen, die vor allem in den Art. 7–9 DS-GVO zu finden sind (b)). Inwieweit darüber hinaus auf allgemeine Wirksamkeitsvoraussetzungen für Rechtsgeschäfte nach dem BGB zurückgegriffen werden kann und muss, ist umstritten (c)). Auf weitere Kriterien der Einwilligung in Sonderrechtsbereichen, aufgestellt etwa in § 26 BDSG für die Arbeitnehmereinwilligung[441] oder in § 7 Abs. 2 UWG für Direktwerbung durch E-Mail und Telefon,[442] wird an geeigneter Stelle kurz eingegangen. Insgesamt wird sich jedoch zeigen, dass eine konsequente Anwendung der Wirksamkeitsvoraussetzungen

---

[439] KG BeckRS 2019, 8570 Rn. 43; siehe auch BGH NJW 2017, 2119 Rn. 22 – Robinson Liste; BT-Drucks. 17/13951, 72; *Hacker*, ZfPW 2019, 148 (159); *Specht*, JZ 2017, 763 (764); vgl. auch LG Berlin MMR 2018, 328 Rn. 51; EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 80.

[440] *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.4.; *Langhanke*, Daten als Leistung, 2018, 124 f.; *Specht*, JZ 2017, 763 (765); *Metzger*, AcP 216 (2016), 817 (832); *Ohly*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, 2002, 168 f. und 448.

[441] Siehe unten, § 4 B.I.13.a)dd)(4)(b).

[442] Siehe unten, Text bei § 4, Fn. 448 und 964 und § 5, Fn. 713.

der Einwilligung durchaus eine Handhabe bietet, zumindest ein Stück weit die regulatorischen Risiken vernetzter Datenerhebung einzuhegen.

a) Allgemeiner Begriff der Einwilligung, Art. 4 Nr. 11 DS-GVO

Eine wirksame datenschutzrechtliche Einwilligung führt gemäß Art. 6 Abs. 1 lit. a DS-GVO zur Rechtmäßigkeit der von ihr umfassten Datenverarbeitung. In begrifflicher Hinsicht jedoch ist Art. 4 Nr. 11 DS-GVO die zentrale Norm, in welcher die Einwilligung legaldefiniert wird als „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist". Sie stellt damit eine qualifizierte Form des Einverständnisses dar. Im Zusammenspiel mit Art. 6 Abs. 1 lit. a DS-GVO ergeben sich fünf Kriterien für eine wirksame Einwilligung: Unmissverständlichkeit, Bestimmtheit, Informiertheit, Freiwilligkeit und Abgabe vor der Datenverarbeitung. Während die Unmissverständlichkeit das „Ob" der Einwilligung betrifft und die Bestimmtheit deren Inhalt, beziehen sich die übrigen drei Kriterien auf die Umstände einer möglichst präferenzkonformen Einwilligung.

aa) Unmissverständlichkeit

Neu eingeführt im Zuge der europäischen Datenschutzreform, die im Erlass der DS-GVO gipfelte, wurde das erste Kriterium der wirksamen Einwilligung: das der Unmissverständlichkeit. In der Tat wird sich zeigen, dass dies gerade gegenüber der in Deutschland auch seitens des BGH in der Vergangenheit vertretenen Auslegung der DSRL erhebliche Neuerungen mit sich bringt.

(1) Grundsatz: Ausdrücklich oder konkludent

Grundsätzlich kann jedoch nach dem Wortlaut von Art. 4 Nr. 11 DS-GVO auch eine unmissverständliche Einwilligung sowohl ausdrücklich als auch konkludent erteilt werden. Ferner besteht, anders als noch unter § 4a Abs. 1 S. 3 BDSG aF, kein Schriftformerfordernis mehr.

(a) Dimensionen der Unmissverständlichkeit

Dem 32. Erwägungsgrund der DS-GVO lassen sich vielmehr zwei Dimensionen der Unmissverständlichkeit entnehmen: aktives Tun und Absonderung der Einwilligung gegenüber dem sonstigen Austauschvorgang.

(aa) Aktives Tun

Zunächst impliziert Unmissverständlichkeit, dass die Einwilligung, ob nun ausdrücklich oder konkludent, jedenfalls durch aktives Tun erklärt werden

muss.[443] Denn der 32. Erwägungsgrund der DS-GVO erläutert explizit, dass dafür das „Anklicken eines Kästchens beim Besuch einer Internetseite [oder] die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft" ausreichen soll. Entscheidend ist jedoch, was nach demselben Erwägungsgrund nicht zureichend für eine eindeutige Erklärung ist: „Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person". Erforderlich ist mithin immer ein aktiver Opt-In; die bloße Möglichkeit zu einem Opt-Out kann das Kriterium der Unmissverständlichkeit nicht erfüllen. Angesichts von verhaltensökonomisch gut belegten *default*-Effekten[444] ist es auch sinnvoll, aktives Tun zu fordern, wenn die Einwilligung tatsächlich Souveränität der Nutzer über ihre Daten und bewussten Umgang mit ihnen ermöglichen soll.

Die Insistenz auf aktivem Opt-In ist insbesondere deshalb relevant, weil der BGH für die Zeit vor Geltung der DS-GVO in den beiden Entscheidungen *Payback* und *HappyDigits* zunächst gerade anders geurteilt hatte.[445] In der Rechtssache *Payback* hielt er eine Klausel für datenschutzrechtlich gem. § 4a BDSG aF unbedenklich, in der eine Einwilligung durch AGB erteilt wurde, wobei sich unmittelbar im Anschluss an die betreffende Formulierung ein Kästchen befand, das angekreuzt werden konnte, falls die Einwilligung nicht erteilt werden sollte.[446] Weder BDSG noch DSRL beinhalteten nach dem BGH ein Erfordernis zur aktiven Erteilung der Einwilligung;[447] ein solches ergebe sich nur aus § 7 Abs. 2 UWG.[448] In der Rechtssache *HappyDigits* bestätigte der BGH diese Einschätzung und befand, dass es datenschutzrechtlich auch ausreichend sei, wenn die Klausel, welche die Einwilligung beinhaltet, aktiv durchgestrichen werden muss, soll die Einwilligung verweigert werden.[449]

Diese eigenwillige Interpretation des Einwilligungserfordernisses nach der DSRL stieß schnell auf Widerstand im Schrifttum.[450] In der Sache wenig überraschend hat der EuGH diese Rechtsprechung, auf die verspätete Vorlage des BGH hin, in der Rechtssache *Plant49* auch für die DSRL noch korrigiert.[451]

---

[443] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 54, 62 f. (dazu sogleich genauer); siehe zuvor auch bereits GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 73; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 57; *Buchner*, WRP 2018, 1283 (1285).

[444] Dazu etwa *Hacker*, Verhaltensökonomik und Normativität, 2017, 85 f.; *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 264 ff.; *Baumgartner/Gausling*, ZD 2017, 308 (312); *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (9).

[445] Dazu *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 116; *Langhanke*, Daten als Leistung, 2018, 66 ff.

[446] BGH NJW 2008, 3055 Rn. 22 f. – Payback.

[447] BGH NJW 2008, 3055 Rn. 23 – Payback.

[448] BGH NJW 2008, 3055 Rn. 27 – Payback.

[449] BGH NJW 2010, 864 Rn. 22 f. – HappyDigits.

[450] Siehe etwa *Brisch/Laue*, CR 2008, 724; *Buchner*, DuD 2010, 39 (43); *Langhanke*, Daten als Leistung, 2018, 67.

[451] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 54–59.

Für Altfälle ist daher ebenfalls eine aktive Einwilligung zu fordern. Der BGH musste sich dem notgedrungen anschließen.[452]

Diese Wende zur aktiven Einwilligung gilt nach der Entscheidung des EuGH in *Planet49* umso mehr unter Geltung der DS-GVO.[453] Denn der 32. Erwägungsgrund der DS-GVO stellt seinerseits unmissverständlich klar, dass Untätigkeit oder bestimmte Voreinstellungen dem Gebot der Unmissverständlichkeit nicht genügen. Dies folgt im Übrigen hinsichtlich Voreinstellungen auch aus Art. 25 Abs. 2 DS-GVO.[454] Daher ist es irrelevant, ob der „mündige Verbraucher" diese Kästchen wahrgenommen hätte oder nicht.[455]

Dieser Auslegung des EuGH stehen auch nicht die Interessen oder Grundrechte der Verantwortlichen entgegen. Denn sie ist technisch nicht schwer umzusetzen und verursacht gegenüber einer Variante, bei der etwa ein Kästchen für den Opt-Out angekreuzt werden muss, keinerlei Mehraufwand. Vielmehr geht es allein um die Steuerungswirkung von Voreinstellungen und den mit einer Einwilligung *by default* verbundenen Kontrollverlust. Wenn die Einwilligung tatsächlich ein Instrument sein soll, den Nutzern Souveränität und Kontrolle über ihre Daten zu vermitteln, um auch materiell privatautonom über diese disponieren zu können, so darf sie nicht unter Hinweis auf eine Opt-Out-Möglichkeit in jenen Nutzungsbedingungen versteckt werden, die in fast allen Fällen zu Recht mit rationaler Ignoranz gestraft werden. Die Zulässigkeit der Opt-Out Einwilligung ist daher mit der Entscheidung in *Planet49* zu Recht Rechtsgeschichte geworden sein.

(bb) Gesonderte Einwilligung

Auch der Umstand, dass die betroffene Person selbst bei Opt-Out Einwilligungen zumeist eine zumindest mittelbar mit der Einwilligung zusammenhängende aktive Betätigung ausübt (Unterschrift eines Vertrages,[456] Anklicken eines Bestellkästchens auf einer Webseite[457]), kann nicht genügen. Denn das aktive Tun muss gerade unmittelbar spezifisch auf die Einwilligung bezogen sein. Dies ist Gegenstand der zweiten Dimension der Unmissverständlichkeit: der gesonderten Einwilligung.[458]

---

[452] BGH GRUR 2020, 891 Rn. 51 ff. – Cookie-Einwilligung II (dazu auch unten, § 4 B.I.4.a)bb)(1)(c)); siehe zuvor bereits KG MMR 2020, 239 Rn. 41 f.; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 58; *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 494; *Stemmer*, in: BeckOK DatenschutzR, 27. Ed. 1.5.2019, Art. 7 DS-GVO Rn. 83; *Schantz*, NJW 2016, 1841 (1844).

[453] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 54, 62 f.

[454] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 56.

[455] Dies ist ein zentrales Argument des BGH in NJW 2008, 3055 Rn. 24 f. – Payback.

[456] Dies war ein Argument des BGH in NJW 2008, 3055 Rn. 24 f. – Payback.

[457] Dies erwägend *Krohm*, ZD 2016, 368 (372); dagegen *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 58.

[458] EuGH, Urt. v. 1.10.2019 – R. C-673/17 (*Planet49*) – Rn. 58 f.; GA *Szpunar*, Schluss-

Nach den Ausführungen von GA *Szpunar* in der Rechtssache *Planet49* muss die Einwilligung von der eigentlichen Austauschaktivität zwischen den Parteien getrennt sein, also zum Beispiel von dem Herunterladen eines Programms oder dem Ausfüllen eines Anmeldeformulars.[459] Dem hat sich der EuGH in seinem Urteil angeschlossen.[460] Dies ist insoweit richtig, als aus der vom Betroffenen zur Erreichung des eigentlichen Austauschziels ausgeführten Handlung gerade nicht unmissverständlich geschlossen werden kann, dass diese auch den Charakter einer Einwilligung haben soll. Vielmehr bliebe eine derartige Handlung, selbst wenn man ihr zugleich den Aussagegehalt der Abgabe einer Einwilligung beilegen wollte, doch immer ambivalent.[461] Nach dem 32. Erwägungsgrund bedeutet Unmissverständlichkeit aber Eindeutigkeit.

Es muss jedoch genügen, wenn eine eigenständige vorbereitende Handlung mit unmittelbarem und spezifischem Bezug auf die Einwilligung vorgenommen wird, die Abgabe der Einwilligung jedoch mit der Abgabe einer anderen Willenserklärung zusammenfällt,[462] sofern die Einwilligung weiterhin unter den konkreten Umständen unmissverständlich ist.[463] Dies ist etwa der Fall, wenn Betroffene ein eigenes Kästchen für die Einwilligung ankreuzen oder sonst separat aktiv zum Ausdruck bringen, dass sie eine Einwilligung erteilen wollen. *Diese* vorbereitende Handlung muss von der eigentlichen Austauschhandlung, bzw. der Abgabe der Willenserklärung zur rechtlichen Verpflichtung auf diese

anträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 63–66, 74 f., 89. Allerdings wird das Kriterium der gesonderten Einwilligung von GA *Szpunar* systematisch nicht überzeugend als Ausfluss der Informiertheit und Freiwilligkeit der Einwilligung eingeordnet. Dies folgt aus seiner Annahme, zwei Willenserklärungen könnten „nicht beide derselben Schaltfläche für die Teilnahme [an einem Gewinnspiel] zugeordnet werden" (ebd., Rn. 89). Dass mit einer Handlung aber nicht zwei Willenserklärungen abgegeben werden können, vermag bereits logisch nicht einzuleuchten: Wenn nur klargestellt ist, dass eine Person mit dem Heben ihres Armes sowohl einen Kaufvertrag über eine Flasche Wein abschließen als auch zugleich seinen alten Weinöffner verkaufen möchte, so können unproblematisch diese beiden Willenserklärungen im Rahmen der Vertragsfreiheit in einer Handlung zusammengefasst werden (ebenso *Moos/Rothkegel*, MMR 2019, 736 [738]). Nach deutschem Verständnis fallen sogar häufig die Abgabe einer schuldrechtlichen und einer sachenrechtlichen Willenserklärung in einer Handlung zusammen. Entscheidend ist dabei jeweils, dass aus dem Kontext eindeutig hervorgeht, dass gerade zwei unterschiedliche Willenserklärungen mit derselben Handlung abgegeben werden sollen. Darauf zielt das Kriterium der Unmissverständlichkeit in Art. 4 Nr. 11 DS-GVO.

[459] GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 89.

[460] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 58–60. Der EuGH verortet dieses Erfordernis (wohl) in dem Kriterium, dass die Einwilligung für den bestimmten Fall abgegeben werden muss. Auch dies erscheint jedoch nicht schlüssig, da die Frage, welche Fälle vom Inhalt einer Einwilligung umfasst sind, von der hier zu beurteilenden nach der klaren Separierung der Abgabe der Einwilligung von einer „Willensbekundung mit anderem Gegenstand" (ebd., Rn. 58) völlig unabhängig ist.

[461] *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 20.

[462] Für die Möglichkeit einer Verbindung von Einwilligung und anderweitiger Willenserklärung auch *Hanloser*, ZD 2019, 264 (265); *Taeger/Schweda*, ZD 2020, 124 (126).

[463] *Taeger/Schweda*, ZD 2020, 124 (126 f.).

Handlungen, verschieden sein. Sie ist jedoch typischerweise noch nicht mit der Abgabe der Einwilligung verbunden: Man stelle sich vor, ein Nutzer setzt im Rahmen eines Bestellvorgangs ein Häkchen bei einem Hinweistext hinsichtlich der Kontaktierung mit Werbebotschaften, schließt den Bestellvorgang jedoch nicht ab. In diesem Fall ermangelt es einer Abgabe nicht nur hinsichtlich der Willenserklärung, mit der die Bestellung vorgenommen wird, sondern richtigerweise auch hinsichtlich der Einwilligung. Das reine Ankreuzen selbst ist mithin lediglich eine Vorbereitungshandlung für diese Abgabe,[464] ähnlich dem Aufsetzen eines Schriftstücks vor dessen Absendung. Es muss jedoch genügen, dass die vorbereitende Handlung separat erfolgt.

Dafür spricht in systematischer Hinsicht auch der Abgleich mit Art. 7 Abs. 2 S. 1 DS-GVO,[465] der das Hervorhebungsgebot beinhaltet und lautet: „Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist." Auch hier ist lediglich das separate Ersuchen (englische Version: *request*), nicht aber die separate Abgabe der eigentlichen Erklärung, vorgesehen.[466]

Es würde daher auch in systematischer Hinsicht zu weit führen, mit GA *Szpunar* zu verlangen, dass auch die Abgabe der Einwilligung selbst von der Abgabe der in dem Austauschverhältnis primär relevanten Willenserklärung (typischerweise der auf Abschluss eines Verpflichtungsgeschäfts gerichteten) verschieden sein müsste.[467] Andernfalls müsste künftig bei jedem Online-Bestellvorgang für jede Einwilligung eine eigene Schaltfläche zur Verfügung gestellt werden, mit der diese Einwilligung abgesandt wird. Der Nutzer müsste mithin sowohl einen Haken setzen als auch die Einwilligung absenden, zusätzlich zur Betätigung der Schaltfläche für die Absendung der primären, transaktionsbezogenen Willenserklärung. Dies ist jedoch für eine Unmissverständlichkeit der Abgabe nicht erforderlich, würde vielmehr zugleich unnötige Verwirrung stiften, da die Nutzer dann regelmäßig, aus ihrer Perspektive, „doppelt" einwilligen müssten. Der Informiertheit des Einwilligungsprozesses wäre dies eher abträglich; zugleich wäre dieser weitere Eingriff in die unternehmerische Freiheit für die Unmissverständlichkeit der Einwilligung nicht erforderlich und damit nicht gerechtfertigt.

---

464 GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 89.

465 *Taeger/Schweda*, ZD 2020, 124 (126).

466 Vgl. auch *Hanloser*, ZD 2019, 264 (265).

467 So aber GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 96; ebenfalls wohl *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 19; aA und insoweit zutreffend, allerdings bezüglich § 4a Abs. 1 S. 4 BDSG aF, BGH NJW 2008, 3055 Rn. 23 – Payback.

(b) Anwendung auf die drei Leitfälle

Im Sinne des eben Gesagten ausgelegt, entfaltet das Kriterium der Unmissverständlichkeit durchaus signifikante Unterscheidungskraft für die Frage, ob eine Einwilligung rechtlich wirksam ist oder nicht. Dies zeigt sich besonders an der Anwendung des Kriteriums auf die drei Leitfälle.

(aa) Datenweiterleitung an Dritte (personalisierte Werbung)

Einwilligungen werden vor allem auch eingeholt, um personalisierte Werbung und die damit verbundenen Datenverarbeitungsvorgänge, etwa Datenweiterleitungen an Dritte, zu legitimieren. Hintergrund ist, dass äußerst unklar ist, ob Datenverarbeitung zu Zwecken der personalisierten Werbung nach Art. 6 Abs. 1 lit. f DS-GVO zulässig ist. Daher soll die Einwilligung ein höheres Maß an Rechtssicherheit bieten. Dies kann sie aber naturgemäß nur, wenn sie rechtlich wirksam ist.

Für besondere Aufmerksamkeit hat das Verfahren der französischen Datenschutzbehörde CNIL gegen Google gesorgt, das oben bereits kurz angesprochen wurde.[468] Das wegen Verstoßes gegen die DS-GVO verhängte Bußgeld in Höhe von € 50 Millionen gründete vor allem auf der Unwirksamkeit der Einwilligung hinsichtlich der Datenverarbeitung für personalisierte Werbung. Die Datenschutzbehörde hob besonders hervor, dass Google vorangekreuzte Kästchen verwendet, was eine unmissverständliche Erklärung der betroffenen Person ausschließt.[469]

Gleiches muss gelten, wenn eine Einwilligung allein dadurch erteilt werden soll, dass ein Service (weiter) genutzt wird.[470] Skype etwa gestaltet so seine Cookie-Einwilligung,[471] die bis zum Geltungsbeginn der ePrivacy-VO nach hier vertretener Auffassung auch an der DS-GVO zu messen ist (zu deren Wirksamkeitsvoraussetzungen unten, §4 B.I.4.). Denn auch die fortgesetzte Nutzung eines Produkts stellt kein aktives Tun dar, das sich spezifisch und gesondert auf eine Einwilligung bezöge. Dies gilt auch dann, wenn der Verantwortliche einen Hinweis eingeblendet, wonach die fortgesetzte Nutzung einer Einwilligung gleichkommt;[472] denn dem weiteren Besuch einer Webseite

[468] Zu diesem Verfahren *Moerel*, CNIL's Decision Fining Google Violates One-Stop-Shop, Working Paper, 2019, https://ssrn.com/abstract=3337478 (hinsichtlich der Zuständigkeitsfragen); *Tambou*, 5 European Data Protection Law Review 2019, 80.

[469] *CNIL*, Deliberation of the Restricted Committee SAN-2019–001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, 2019, Rn. 153 ff.

[470] *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 19; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 58.

[471] https://www.skype.com/de/ (zuletzt abgerufen am 22.7.2019): „Diese Website verwendet Cookies für Analysen, personalisierte Inhalte und Werbung. Indem Sie diese Website nutzen, erklären Sie sich mit dieser Verwendung einverstanden."

[472] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 58; *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 494.

oder der Nutzung einer App kommt typischerweise lediglich der Erklärungsgehalt zu, dass die betroffene Person die Funktionen dieses Produkts in bestimmungsgemäßer Weise nutzen möchte. Die Auslegung, dass neben diesem Nutzungswillen noch ein Erklärungswille hinsichtlich der Einwilligung vorläge, ist zwar nicht undenkbar, aber eben nicht, wie von der DS-GVO gefordert, eindeutig. So ist auch anerkannt, dass das Anbringen eines Schildes „Eltern haften für ihre Kinder" am Eingang eines Ladengeschäfts nicht zu einer vertraglichen Garantiehaftung der Eltern für die Kinder führt, sondern rechtlich, mangels objektiver Anhaltspunkte für einen elterlichen Rechtsbindungswillen, in der Regel wirkungslos ist. Hinreichend für eine unmissverständliche Einwilligung ist vielmehr ein Button, der sich auf die Einwilligung bezieht.[473]

(bb) Datenerhebung durch Dritte (*third-party tracking*)

Dieselben Kriterien gelten auch für Tracking-Instrumente, die durch Drittanbieter genutzt werden. Hier ist den Nutzern häufig die automatisierte Datenübertragung mit Aufruf der Webseite oder Nutzung der App schon gar nicht bewusst, sodass eine unmissverständliche Einwilligung durch die fortgesetzte Nutzung a fortiori ausscheidet. Um diese Problematik einzuhegen, wurden verschiedene Software-Lösungen entwickelt, die zum Beispiel Social Plug-Ins so konfigurieren, dass diese erst nach einer aktiven Bestätigung durch den Nutzer Daten zu sammeln beginnen (sog. Shariff-Lösung und 2-Klick-Lösung).[474] Diese genügen den Anforderungen an eine unmissverständliche Einwilligung; sie sind aber auch erforderlich, um derartige Tracking-Instrumente auf der Basis einer Einwilligung datenschutzkonform einsetzen zu können. Das Hauptproblem bei derartigen Instrumenten ist jedoch, dass die Betroffenen typischerweise gar keine Kenntnis von den einzelnen Datenverarbeitungsvorgängen haben. Dies ist im Rahmen der Informiertheit der Einwilligung von Belang.

(cc) Datenerhebung bei Dritten

Als besonders problematisch erweist sich die Unmissverständlichkeit der Einwilligung bei der Datenerhebung bei Dritten, etwa bei Personen, mit denen nicht das primäre Nutzungsverhältnis bei IoT-Geräten besteht. Soll hier konkludent eine Einwilligung in dem Einstieg in ein vernetztes Fahrzeug, dem Betreten eines Smart Home oder dem Besuch einer Smart City liegen?

Eine derartige Einwilligung dürfte unter dem Regime der DS-GVO jeweils am Kriterium der Unmissverständlichkeit scheitern. Denn sie wäre von den Handlungen, mit denen das jeweilige Produkt in bestimmungsgemäßer Weise

[473] *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 494.
[474] *Föhlisch/Pilous*, MMR 2015, 631 (635 f.); *Schleipfer*, DuD 2014, 318 (324); *Globocnik*, 50 ICC 2019, 1033 (1041).

genutzt wird, nicht zu unterscheiden. Damit ist die zweite Dimension der Unmissverständlichkeit verletzt: Die Handlung ist hinsichtlich der Abgabe einer Einwilligung gerade ambivalent, nicht eindeutig. Eine Einwilligung müsste daher eigens vor der Nutzung des Geräts oder der Umgebung eingeholt werden.

Dies stellt mit zunehmender Verbreitung von vernetzten Gegenständen ein erhebliches Umsetzungsproblem dar.[475] Will man nicht die Betroffenen ständig mit neuen Einwilligungen für Geräte, mit denen sie in Kontakt kommen, behelligen,[476] so müssen neue Wege bei der Bereitstellung und Abgabe der Einwilligung in stark vernetzten Umgebungen gefunden werden.[477]

(2) Ausnahme: Nur ausdrücklich

In drei Fällen kann die unmissverständliche Einwilligung schließlich nur ausdrücklich, mithin also nicht konkludent,[478] erklärt werden: nach Art. 9 Abs. 2 lit. a DS-GVO bei sensitiven Daten; nach Art. 22 Abs. 2 lit. c DS-GVO bei automatisierter Entscheidungsfindung; und nach Art. 49 Abs. 1 lit. a DS-GVO bei der Datenübermittlung ins EU-Ausland. All diese Sachverhalte zeichnen sich durch erhöhte Datenschutzrisiken aus.[479] Der Unterschied zum Kriterium der Unmissverständlichkeit in allen anderen Fällen ist jedoch marginal, wenn man dieses Kriterium, wie hier, im Sinne der zwei Dimensionen von aktivem Tun und Absonderung der Einwilligung versteht. Lediglich die Frage, ob bestimmte Handlungsformen als konkludente, aber unmissverständliche Einwilligung gedeutet werden können, ist dann obsolet.

bb) Bestimmtheit

Das zweite zentrale Kriterium für die Wirksamkeit der datenschutzrechtlichen Einwilligung ist ihre Bestimmtheit. Damit wird vor allem der Zweckbindungsgrundsatz des Art. 5 Abs. 1 lit. b DS-GVO operationalisiert. Art. 4 Nr. 11 DS-GVO fordert, dass eine Einwilligung „für den bestimmten Fall" erteilt werden muss; und Art. 6 Abs. 1 lit. a DS-GVO setzt hinzu, dass sie „für einen oder mehrere bestimmte Zwecke" abzugeben ist. Der 32. Erwägungsgrund der DS-GVO schließlich spezifiziert, dass, wenn „die Verarbeitung mehreren Zwecken dient, […] für alle diese Verarbeitungszwecke eine Einwilligung gegeben werden [sollte]."

---

[475] *Ziegler/Menon/Annichino*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 149 (165); *Steege*, MMR 2019, 509 (511).

[476] Kritisch daher *Roßnagel*, MMR 2005, 71 (72); *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 168 f.

[477] Siehe unten, § 6 C.I.3.c).

[478] Statt vieler: *Stemmer*, in: BeckOK DatenschutzR, 27. Ed. 1.5.2019, Art. 7 DS-GVO Rn. 82.

[479] Allenfalls bei Art. 22 DS-GVO kann man dies im Einzelfall anders sehen.

Während die Unmissverständlichkeit mithin das „Ob" der Einwilligung betrifft, regelt die Bestimmtheit ihren Inhalt.[480] Dies bedeutet, dass es für eine wirksame Einwilligung notwendig ist, dass die Zwecke und Kontexte, in welchen die Datenverarbeitung(en) erfolgen soll(en), ex ante spezifisch angegeben werden müssen. Eine pauschale Einwilligung in unbestimmte Verarbeitungskontexte und -zwecke ist daher nach allgemeiner Ansicht unwirksam.[481] Vorbehaltlich einer Lösung über Art. 6 Abs. 4 DS-GVO stellt dies ein zentrales Problem für Anwendungen maschinellen Lernens dar, bei denen typischerweise die Daten für neue Zwecke (die Ermittlung bislang unbekannter Korrelationen) eingesetzt werden, die im Zeitpunkt der Datenerhebung noch nicht bekannt oder absehbar waren (dazu unten, § 4 C.II.). Dies ist gerade auch bei Daten, die im Rahmen des Internets der Dinge generiert werden, akut.[482]

Das Problem des *secondary use*, das in der Tat mit den herkömmlichen Instrumenten der Einwilligung kaum zu bewältigen ist (und daher über Art. 6 Abs. 4 DS-GVO oder – vorzugswürdig – über Art. 6 Abs. 1 lit. f DS-GVO gelöst werden muss), muss streng getrennt werden von jenen Fällen, in denen die Verarbeitungskontexte und -zwecke bereits bei der Erhebung feststehen, über diese aber nicht hinreichend informiert wird. Letztlich erweist sich damit das Bestimmtheitskriterium als eng verknüpft mit dem Merkmal der Informiertheit der Einwilligung:[483] Über Kontexte und Zwecke muss informiert werden, sodass die Einwilligung mit Bezug auf diese abgegeben werden kann.

Das Bestimmtheitskriterium ist dabei durchaus ein scharfes Schwert. Bereits im Jahr 2016 stellte das OVG Hamburg fest, dass die anlässlich eines WhatsApp-Updates eingeholte Einwilligung der Nutzer in den Datenaustausch zwischen WhatsApp und Facebook mangels Bestimmtheit des Zwecks unwirksam war.[484] Auch das Bußgeld der französischen Datenschutzbehörde CNIL gegen Google, von dem bereits die Rede war, gründete unter anderem

---

[480] *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 67.

[481] Statt vieler: *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 62; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 69.

[482] *Bolognini/Balboni*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 71 (77); *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 8.

[483] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 63.

[484] OVG Hamburg, Beschl. v. 1.3.2018, BeckRS 2018, 2175, Rn. 35 f. (pauschale Einwilligung für die Zwecke „Network/Security", „Business Intelligence Analytics" und „Facebook Ads/Products"); ähnlich die italienische Wettbewerbsbehörde *AGCM*, WhatsApp Fined for 3 Million Euro for Having Forced Its Users to Share Their Personal Data with Facebook, Pressemitteilung (12.7.2017), http://www.AGCM.it/en/newsroom/press-releases/2380-whatsapp-fined-for-3-millioneuro-for-having-forced-its-users-to-share-their-personal-data-with-facebook.html; zu diesem Update auch *Zingales*, 33 Computer Law & Security Review 2017, 553.

auf mangelnder Bestimmtheit der Einwilligung.[485] Gerade für die Fallgruppen der ersten und zweiten Leitfälle, die Datenweiterleitung an Dritte und die Datenerhebung durch Dritte, ist das Bestimmtheitsgebot daher außerordentlich relevant.

cc) Informiertheit

Die verbliebenen drei Kriterien der Informiertheit, Freiwilligkeit und Abgabe vor der Datenverarbeitung sollen die materiellen Grundlagen der Inanspruchnahme von Privatautonomie sichern. Dass die Einwilligung in informierter Weise abgegeben werden muss, soll die Informationsasymmetrie zwischen Verantwortlichen und Betroffenen hinsichtlich der genauen Umstände der Verarbeitung abmildern.[486] Insbesondere muss für die Nutzer erkennbar sein, wer die Daten wie verarbeitet.[487] Die Verarbeitungsprozesse müssen daher transparent gemacht werden. Dies geschieht primär über die in Art. 12 ff. DS-GVO verankerten Informationspflichten.[488]

Das Informationsregime des europäischen Privatrechts hat sich, inspiriert vom Informationsmodell des US-amerikanischen Kapitalmarktrechts, nicht nur im europäischen Kapitalmarktrecht, sondern vor allem auch im Verbraucherrecht herausgebildet und gefestigt.[489] Wenn die Abmilderung von Informationsasymmetrie Zielpunkt der Informiertheit der Einwilligung ist, so nimmt es nicht Wunder, wenn in jüngster Zeit eine Engführung des Verbraucherleitbilds des unionalen Verbraucherrechts mit dem Nutzerleitbild des europäischen Datenschutzrechts propagiert wird, prominent etwa von GA *Szpunar*.[490] Dieses Leitbild, das auch vom BGH unter Geltung der DSRL angewendet wurde,[491]

---

[485] *CNIL*, Deliberation of the Restricted Committee SAN-2019–001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, 2019, Rn. 156 f.

[486] Zur Informationsasymmetrie bereits oben, § 3 B.II.1.a).

[487] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 59.

[488] Siehe dazu auch *Taeger/Schweda*, ZD 2020, 124 (128); Ob die Anforderungen aus Art. 4 Nr. 11 und Art. 12 ff. DS-GVO hinsichtlich der Informiertheit exakt deckungsgleich sind, ist umstritten, hier aber nicht weiter von Belang, siehe etwa *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 73 (für Differenzierung); *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 35 (für Synchronisierung). Der EuGH scheint keinen Unterschied zwischen dem Erfordernis der informierten Einwilligung und den Pflichten nach Art. 12 ff. DS-GVO zu machen, siehe EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 76, 79 f.

[489] *Hacker*, Verhaltensökonomik und Normativität, 2017, § 9; knapper *Grundmann*, in: Festschrift Canaris, 2017, 907 (928 ff.).

[490] GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 113; für einen durchschnittlichen Nutzer als Referenzrezipienten auch *Bäcker*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 12 DS-GVO Rn. 11; *Quaas*, in: BeckOK Datenschutzrecht, 29. Ed. 2019, Art. 12 DS-GVO Rn. 15; *Pohle/Spittka*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 12 DS-GVO Rn. 10.

[491] BGH NJW 2008, 3055 Rn. 24; BGH NJW 2010, 864 Rn. 30.

bestimmt ganz erheblich die Art und das Maß der Information, welche übermittelt werden müssen: Sie ist so zu bemessen, dass ein durchschnittlich informierter, situationsadäquat aufmerksamer und verständiger Nutzer in der Lage ist, informiert zu entscheiden.[492] Angesichts der technischen Komplexität der Verarbeitungsvorgänge kann dies jedoch nur heißen, dass die Konsequenzen der Einwilligung ermessen und die Auswirkungen der Handlungen des Nutzers für ihn erkennbar werden.[493] In der Umsetzung hat dies zwei Komponenten: Einerseits muss der Verantwortliche Transparenz herstellen, andererseits muss der Nutzer zumindest die Möglichkeit der Erkenntnis der wesentlichen Umstände der Verarbeitung haben.

(1) Transparenz

Hinsichtlich der Transparenz der wesentlichen Verarbeitungsprozesse ist zunächst zu bemerken, dass die mangelnde Information über den Umstand, dass überhaupt eine Einwilligung eingeholt wird, gar zum Wegfall des Erklärungsbewusstseins und damit zur Unwirksamkeit der Einwilligung führen kann.[494] So führt das OVG Hamburg, in Wiedergabe der Vorgängerentscheidung des VG Hamburg, zum Versuch der Einholung einer Einwilligung in den Datenaustausch zwischen WhatsApp und Facebook anlässlich des WhatsApp-Updates vom 25.8.2016 aus:

„Es fehlt an einer bewussten Einwilligung der betroffenen Nutzer. Denn für einen durchschnittlichen Nutzer ist nicht erkennbar, dass die Betätigung des obigen Buttons ‚Zustimmen' eine Einwilligung in Datenvorgänge nach § 4 Abs. 1 BDSG darstellen soll. Es fehlt nämlich jeglicher Hinweis darauf, dass es in der Sache um die Einholung einer Einwilligung in Datenverarbeitungen geht. Dies kann dem Nutzer auch gar nicht bewusst sein. Der dem Hyperlink ‚Zustimmen' vor- bzw. nachfolgende Text erwähnt dies mit keinem Wort. Die Wortwahl, die Datenschutzrichtlinie werde aktualisiert, suggeriert vielmehr, die Daten des Nutzers würden geschützt."[495]

In ähnlicher Weise hatte bereits das AG Elmshorn entschieden, dass eine klauselartige Einwilligung unter der Überschrift „Datenschutz" keine informierte Einwilligung darstellen könne, da die Wortwahl „Daten*schutz*" gerade suggeriere, dass die Privatsphäre des Nutzers durch die darin enthaltenen Angaben in besonderer Weise protegiert werde.[496] Empirische Untersuchungen stützen

[492] Ähnlich für das Kriterium der klaren und verständlichen Information nach Art. 6 Abs. 1 S. 1 VRRL GA *Saugmandsgaard Øe*, Schlussanträge v. 19.12.2018 – Rs. C-681/17 (*slewo*) – Rn. 55.

[493] GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 115.

[494] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 56.

[495] OVG Hamburg, Beschl. v. 1.3.2018, BeckRS 2018, 2175, Rn. 37; siehe zudem auch Rn. 43.

[496] AG Elmshorn, MMR 2005, 870 (871); zustimmend *Nord/Manzel*, NJW 2010, 3756 (3758).

diese Sichtweise: Nutzer glauben häufig, dass eine Datenschutzerklärung (*privacy policy*) ein Anzeichen für den Schutz ihrer Daten ist.[497]

Informationsasymmetrie wurde im ersten Teil dieser Arbeit als einer von vier Typen von Marktversagen im Bereich der digitalen Wirtschaft ausgemacht.[498] Daher pocht die Rechtsprechung zu Recht darauf, dass Transparenz zunächst einmal bedeutet, dass überhaupt verständlich gemacht wird, dass eine Einwilligung in bestimmte Datenverarbeitungsvorgänge erteilt wird. Diese Rechtsprechung kann sich zudem auf eine noch konkretere empirische Basis stützen: 62 % der Teilnehmer einer Studie glaubten irrtümlich, dass die Existenz einer *privacy policy* impliziere, dass eine Webseite ihre persönlichen Informationen nicht ohne ihre Erlaubnis weiterverarbeiten darf.[499]

Weiterhin müssen die wesentlichen Umstände der Datenverarbeitung so dargestellt werden, dass der Nutzer die Konsequenzen der Einwilligung leicht ermitteln kann. Wo technische Komplexität auf kognitive Limitationen von Nutzern trifft, müssen neue Wege beschritten werden, um dem Gebot aus Art. 12 DS-GVO, Informationen leicht und verständlich darzulegen, gerecht zu werden.[500] Dies ist zum Teil bereits in der DS-GVO angelegt und kann durch Icons, gestufte Informationserteilung, sprachliche Verständlichkeit sowie andere Mechanismen gefördert werden (siehe im Einzelnen unten, § 6 C.I.).

(2) Erkenntnismöglichkeit

Der Nutzer muss andererseits durch die vom Verantwortlichen bereitgestellten Informationen in die Lage versetzt werden, eine präferenzkonforme Entscheidung über die Einwilligung zu treffen. Dabei würde es jedoch zu weit führen, mit dem LG Berlin zu fordern, dass der (typische) Nutzer auch tatsächlich die Informationen zur Kenntnis nimmt.[501] Vielmehr muss es mit der zumutbaren Erkenntnismöglichkeit sein Bewenden haben.[502] Dafür spricht in teleologischer Hinsicht, dass die Verantwortung des Verarbeiters dort endet, wo die Selbstverantwortung des Nutzers beginnt. Wer trotz verständlicher Informationen und zumutbarer, dem Kontext des Austausches entsprechender[503] Mög-

---

[497] *Turow et al.*, 3 I/S: A Journal of Law and Policy for the Information Society 2008, 723 (731 f.); siehe auch *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 33.

[498] Siehe oben, § 3 B.II.1.a).

[499] *Acquisti/Brandimarte/Loewenstein*, 347 Science 2015, 509 (512).

[500] Siehe etwa *Hacker*, Verhaltensökonomik und Normativität, 2017, 444 ff.

[501] LG Berlin, MMR 2018, 328 Rn. 47 (zu § 4a Abs. 1 BDSG aF). Das LG geht sogar davon aus, dass der Nutzer „in jedem Fall" die Informationen zur Kenntnis nehmen müsste, also wohl (praktisch) jeder Nutzer die Informationen kognitiv verarbeiten könnte. Dass dies illusorisch ist und eine informierte Einwilligung effektiv unmöglich machen würde, liegt auf der Hand, siehe unten, § 4 B.I.5.

[502] So auch OLG Frankfurt a. M. MMR 2016, 245 (246); *Hanloser*, ZD 2019, 264 (265); *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 23 und 72; *Lang/Peintinger*, ELR 2013, 206 (207); *Ernst*, ZD 2017, 110 (113).

[503] Zu diesbezüglichen Differenzierungen *Buchner/Kühling*, in: Kühling/Buchner, DS-

lichkeit deren Kenntnisnahme verweigert, kann später nicht redlich behaupten, die Einwilligung sei mangels Informiertheit unwirksam.[504]

In systematischer Hinsicht streitet dafür auch der Blick auf das AGB-Recht. Auch hier genügt nach § 305 Abs. 2 Nr. 2 BGB bekanntlich die zumutbare Möglichkeit der Kenntnisnahme. Diese Regelung hat mit dem 20. Erwägungsgrund immerhin einen Anknüpfungspunkt in der Klauselrichtlinie und ist Ausdruck eines umfassenderen Leitbildes des im Rahmen seiner Möglichkeiten immer noch souveränen und selbstverantwortlichen Verbrauchers.[505] Sollen Nutzer- und Verbraucherleitbild einander angenähert werden, so muss dies auch dies auch den Umstand betreffen, dass die bloße Erkenntnismöglichkeit genügt. So hat denn auch das OVG Hamburg richtigerweise (implizit) entschieden, dass die Möglichkeit der Kenntnisnahme der Informationen ausreicht, sofern dem Nutzer explizit in dem Hinweis auf weiterführende Informationen bewusst gemacht wird, dass es gerade um die Einholung einer Einwilligung, und nicht die „Aktualisierung der Datenschutzrichtlinie", geht.[506]

(3) Anwendung auf die drei Leitfälle

Die Vorgaben für eine informierte Einwilligung sind einmal mehr für die drei Leitfälle besonders bedeutsam.

(a) Datenweiterleitung an Dritte

Eine Einwilligung in die Datenweiterleitung an Dritte scheitert besonders häufig vor Gericht an der Informiertheit der Einwilligung. Denn der Verantwortliche muss den Kreis der Dritten genau benennen und dortige Verarbeitungsformen transparent machen; zudem muss, als Ausfluss des Bestimmtheitsgebot, der Zweck der Verarbeitung deutlich gemacht werden. Angesichts der im dritten Kapitel beschriebenen Multirelationalität personenbezogener Daten[507] ist dies kein einfaches, aber ein dringliches Unterfangen.

Das LG Berlin und ihm folgend das KG entschieden daher zu Recht, dass eine von Facebook verwendete Klausel, wonach pauschal das Einverständnis mit der Weiterleitung persönlicher Daten in die USA und einer weiteren Verarbeitung dort erteilt wurde, keine bestimmte und informierte Einwilligung darstellt.[508] Weiterhin urteilte es, dass auch die Verwendung für personalisier-

GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 60; LG Frankfurt a. M. ZD 2016, 494 (497) (zu § 4a BDSG aF).

[504] OLG Frankfurt a. M. MMR 2016, 245 (246).

[505] Ausführlich dazu *Drexl*, Die wirtschaftliche Selbstbestimmung des Verbrauchers, 1998, etwa 7 ff.

[506] So auch OVG Hamburg, Beschl. v. 1.3.2018, BeckRS 2018, 2175, Rn. 38 (zu § 4a Abs. 1 BDSG aF).

[507] Siehe oben, § 3 A.III.

[508] LG Berlin, MMR 2018, 328 Rn. 65; KG MMR 2020, 239 Rn. 49.

te Werbung hinreichend spezifiziert werden muss. So reicht es nicht aus, eine Einwilligung zu erteilen für die Nutzung von Profilinformationen „für kommerzielle, gesponserte oder verwandte Inhalte".[509] Auch die Entscheidung der französischen Datenschutzbehörde CNIL zur Verwendung personenbezogener Daten für personalisierte Werbung durch Google stützte sich auf die mangelnde Informiertheit der Einwilligung als einen zentralen Gesichtspunkt.[510] Wichtig ist dabei, dass die Informationen einfach zugänglich sein müssen und nicht über verschiedene Dokumente, Webseiten oder Links verstreut sein dürfen. Genau dies war jedoch bei den von Google zur Verfügung gestellten Informationen der Fall. Manche Inhalte ließen sich nur nach vier Klicks durch verschiedene Zwischenwebseiten erreichen, andere waren gar nicht verlinkt.[511] Vergleichbare Opazität herrscht auch bei vielen anderen Verarbeitungsinformationen großer Internetfirmen.[512]

Nicht nur, aber insbesondere auch für Daten, die bei IoT-Geräten anfallen, muss daher klar und nachvollziehbar angegeben werden, welche Verantwortlichen diese Daten wie zu welchen Zwecken verarbeiten. Besonders bedeutsam ist dabei, ob die Verarbeitung für die Funktionalität des Geräts essenziell ist oder damit weitere Motive, etwa Werbezwecke, verfolgt werden.

(b) Datenerhebung durch Dritte

Ein zentrales Problem bei der Datenerhebung durch Dritte (*third-party tracking*) ist, zunächst einmal überhaupt Transparenz hinsichtlich dieser Datenverarbeitungsvorgänge herzustellen. Dass grundsätzlich über die Verwendung von Tracking-Instrumenten, die personenbezogene Daten sammeln, informiert werden muss, ist unstreitig.[513] Umstritten ist allerdings einerseits, welche Informationen genau zu erteilen sind, und andererseits, wer diese zur Verfügung stellen muss.

Hinsichtlich des Inhalts der Informationen ist hier die Differenz zwischen technischer Komplexität und Aufmerksamkeit bzw. Verarbeitungskapazität der Nutzer besonders hoch. Daher muss etwa bei Cookies zwar neben den Typen der gesammelten Daten auch über die Funktionsdauer der Cookies als auch die Frage, ob Dritte auf die Cookies Zugriff erhalten, informiert wer-

[509] LG Berlin, MMR 2018, 328 Rn. 66; KG MMR 2020, 239 Rn. 50.

[510] *CNIL*, Deliberation of the Restricted Committee SAN-2019–001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, 2019, Rn. 142 ff.

[511] *CNIL*, Deliberation of the Restricted Committee SAN-2019–001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, 2019, Rn. 102, 147.

[512] *Forbrukerrådet*, Deceived by Design, Bericht, 2018, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf; *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (4).

[513] Siehe Art. 5 Abs. 3 der (revidierten) ePrivacy-Richtlinie sowie Art. 4 Nr. 11, Art. 13 DS-GVO.

den.[514] Die Verständlichkeit muss jedoch etwa durch gestaffelte Informationen oder Icons erhöht werden (dazu unten, § 6 C.I.1.).

Adressat der Informationspflichten nach Art. 12 ff. DS-GVO ist der Verantwortliche.[515] Letztlich hängt die Antwort auf die Frage, wer die Informationen erteilen muss, daher davon ab, inwiefern man den Drittanbieter, der über ein Tracking-Tool Daten sammelt, und den Anbieter der Webseite oder App, in welche das Instrument eingebunden wird, als gemeinsame Verantwortliche betrachtet.[516] Nimmt man jedenfalls für die initiale Erhebung der Daten eine gemeinsame Verantwortlichkeit an,[517] so müssen die Verarbeiter nach Art. 26 Abs. 1 S. 2 DS-GVO eine interne Aufteilung vornehmen, welche eine effektive Informationsvermittlung gewährleistet. Dies wird typischerweise zur Folge haben, dass der Anbieter der Webseite oder App die notwendigen Informationen bereithält, da sein Produkt der primäre Anlaufpunkt für die Nutzer ist und nur so die Informationen vor der Datenverarbeitung an den Nutzer gelangen können.[518]

(c) Datenerhebung bei Dritten

Besonders schwierig ist es, eine sachgerechte Informationsvermittlung in den Fällen der Datenerhebung bei Dritten, etwa bei Nicht-Primärnutzern von IoT-Geräten, sicherzustellen.[519] Dritte kommen mit diesen Geräten zunehmend häufiger, oft jedoch rein zufällig oder ungeplant in Berührung. Oftmals wird dabei kaum eine Möglichkeit bestehen, ohne erhebliche Einschränkungen für die Nutzbarkeit des Produkts oder die Alltagserfahrung der Dritten die Informationen bereitzustellen.[520] Es ist beispielsweise nur schwer denkbar, dass jedes Mal, wenn ein Passagier in ein vernetztes Fahrzeug einsteigt, ihm umfängliche Informationen über die Datenverarbeitung in diesem Fahrzeug betreffend seine personenbezogenen Daten angezeigt werden.[521] Eine Einwilligung, der es, wie gesehen, in diesem Kontext häufig auch an der Unmissverständlich-

[514] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 75–81; GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 116–120.

[515] Auf diese rekurriert auch der EuGH, siehe EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 76, 79 f.

[516] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 100.

[517] Siehe oben, § 4 A.III.1.b)dd)(1).

[518] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 102 f.; GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 133–141; *Hanloser*, ZD 2019, 122 (123).

[519] *United States Government Accountability Office*, Internet of Things, 2017, 33 f.; *Edwards*, 2 European Data Protection Law Review 2016, 28 (42); *Banerjee/Hemphill/Longstreet*, Is IOT a Threat to Consumer Consent?, Working Paper, 2017, https://ssrn.com/abstract=3038872.

[520] *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (450).

[521] Vgl. *Ziegler/Menon/Annichino*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 149 (165).

keit fehlen wird, kann daher kaum informiert erteilt werden.[522] Ob ein QR-Code eine zumutbare Informationsmöglichkeit darstellt, darf angesichts der nicht flächendeckenden Ausstattung von Betroffenen mit QR-Code-Scannern erheblich bezweifelt werden.[523] Schlägt in diesen Konstellationen die Einwilligung mithin typischerweise fehl, so kommt auch die individuelle Kontrolle in diesen Fällen an ihre Grenzen. Der Fokus verschiebt sich dann auf die regulatorischen Strukturen des Datenschutzrechts, etwa auf Art. 6 Abs. 1 lit. f DS-GVO, oder neue Formen der Einwilligung, etwa durch maschinelles Lernen unterstützte *technologische Einwilligungen* (siehe unten, § 6 B.I.3.).

dd) Freiwilligkeit

Das vierte Kriterium einer wirksamen Einwilligung hat im Zuge der DS-GVO-Verabschiedung besondere Relevanz gewonnen: die Freiwilligkeit. Zwar galt diese Wirksamkeitsvoraussetzung auch nach dem alten Datenschutzrecht, jedoch wurde erstmals auf europäischer Ebene in Art. 7 Abs. 4 DS-GVO ein Kopplungsverbot eingefügt, welches die Anforderungen an die Freiwilligkeit, wenngleich nicht abschließend, konkretisiert.

(1) Klares Ungleichgewicht und mangelnde Alternativen

Das in Art. 4 Nr. 11 DS-GVO statuierte Kriterium der Freiwilligkeit wird in den Erwägungsgründen näher umschrieben. So weist der 42. Erwägungsgrund am Ende darauf hin, dass eine betroffene Person ihre „Einwilligung [nur dann] freiwillig gegeben [haben soll], wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden." Der 43. Erwägungsgrund ergänzt: „Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern."

Insgesamt sollen mit dem Kriterium der Freiwilligkeit mithin klare Machtungleichgewichte ausgeglichen werden,[524] die dann zu einer Fehlfunktion des marktlichen Allokationsmechanismus führen, wenn sinnvolle Alternativen für

[522] *Edwards*, 2 European Data Protection Law Review 2016, 28 (42).

[523] aA *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 21: QR-Code ausreichend; ebenso *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 1, 2018, 21 Rn. 33.

[524] *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2018, Art. 7 DS-GVO Rn. 50; *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 27 (Schutz vor aufoktroyierter Fremdbestimmung).

die Betroffenen nicht bestehen. Im Fall einer Behörde, die gewissermaßen eine Monopolstellung für die Vergabe bestimmter Rechtstitel innehat, ist die Erfüllung dieser Voraussetzungen evident. Umso mehr umstritten sind sie im privatrechtlichen Kontext.

(2) Gesonderte Einwilligung?

Abzulehnen ist jedoch zunächst der interpretatorische Versuch von GA *Szpunar*, aus dem Erfordernis der Freiwilligkeit und dem 43. Erwägungsgrund die Notwendigkeit einer gesonderten Einwilligung herauszulesen.[525] Eine gesonderte Einwilligung ist nach der Auffassung des Generalanwalts dann gegeben, wenn sie von der eigentlichen Aktivität des Austausches zwischen den Parteien (zum Beispiel: Nutzung der Webseite) getrennt abgegeben wird.[526] Dies kann jedoch als eigenständiges Kriterium im Rahmen der Freiwilligkeit nicht überzeugen, da dies, wie gesehen,[527] gerade eine Frage der Unmissverständlichkeit der Einwilligung ist.[528]

(3) Kopplungsverbot, Art. 7 Abs. 4 DS-GVO

Gerade für den Bereich der Privatwirtschaft werden die vagen Kriterien des 42. und 43. Erwägungsgrunds operationalisiert durch das Kopplungsverbot des Art. 7 Abs. 4 DS-GVO,[529] dessen Inhalt jedoch nicht minder umstritten ist. Danach muss bei „der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, […] dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind." Es handelt sich methodisch mithin um eine regulatorische Struktur, die in das an sich ermöglichende Einwilligungsregime eingebettet ist.

Damit das Kopplungsverbot einschlägig ist, dürfen zunächst einmal die personenbezogenen Daten (oder besser: deren Verarbeitung) für die Erfüllung des Vertrags nicht erforderlich sein (a). Auch dann greift das Koppelungsverbot jedoch nur, wenn die Vertragserfüllung von der Einwilligung abhängig gemacht wird (b), wobei die Rechtsfolge wiederum unbestimmt ist (c). Die Auslegung aller drei Kategorien ist in der Literatur heftig umstritten.

---

525 GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 75.
526 GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 66.
527 Siehe oben, § 4 B.I.3.a)aa)(1)(a)(bb).
528 Kritisch auch *Hanloser*, ZD 2019, 264 (265).
529 *Klement*, *in: Simitis/Hornung/Spiecker gen. Döhmann*, *Datenschutzrecht*, *2019*, Art. 7 Rn. 56.

(a) Erforderlichkeit zur Vertragserfüllung

Das erste Merkmal für die tatbestandliche Einschlägigkeit des Kopplungsverbots ist mithin, dass die Daten für die Erfüllung des Vertrags nicht erforderlich sind.

(aa) Verhältnis zu Art. 6 Abs. 1 lit. b DS-GVO

Der systematische Blick auf Art. 6 Abs. 1 lit. b DS-GVO suggeriert dabei *prima facie* ein Problem. Nach dieser Variante sind solche Verarbeitungen gerade erlaubt, die zur Erfüllung eines Vertrags mit der betroffenen Person erforderlich sind. Ein Beispiel dafür sind Adressdaten beim Fernabsatzvertrag, ohne die das Produkt nicht an den Empfänger ausgeliefert werden kann. Deren Verarbeitung ist mithin bereits nach Art. 6 Abs. 1 lit. b DS-GVO zulässig, eine Einwilligung damit überflüssig. Sind hingegen die Daten zur Erfüllung des Vertrages nicht notwendig, droht die Einwilligung am Kopplungsverbot zu scheitern. Damit stellt sich die Frage, welchen Anwendungsbereich die Einwilligung neben Art. 6 Abs. 1 lit. b DS-GVO im vertraglichen Bereich überhaupt noch hätte.

Zur Lösung bieten sich zwei Varianten an. Einerseits kann man die Erforderlichkeit zur Vertragserfüllung in den beiden Vorschriften unterschiedlich auslegen. Angesichts des sachlich und systematisch engen Zusammenspiels zwischen den beiden Vorschriften erscheint dies jedoch wenig überzeugend.[530] Vielmehr dürfte die Lösung im Blick auf die weitere Tatbestandsvoraussetzung des Kopplungsverbots und die vage Rechtsfolge zu finden sein. Nicht zur Vertragserfüllung erforderliche Daten sind nicht notwendig und automatisch vom Kopplungsverbot erfasst, sondern eben nur dann, wenn die Vertragserfüllung von der Einwilligung in die Verarbeitung dieser Daten auch tatsächlich *abhängig* gemacht wird. Und selbst in diesem Falle führt dies nicht zwangsläufig zur Unwirksamkeit der Einwilligung, sondern es muss diesem Umstand nur in größtmöglichem Umfang *Rechnung getragen* werden. Schließlich kann bei sensitiven Daten im Sinne von Art. 9 DS-GVO auch die Vertragserforderlichkeit keine Rechtmäßigkeit der Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO vermitteln; vielmehr ist nach Art. 9 Abs. 2 DS-GVO zum Beispiel eine ausdrückliche Einwilligung notwendig (lit. a).[531] Damit verbleibt für die Einwilligung neben Art. 6 Abs. 1 lit. b DS-GVO durchaus ein signifikanter, wenn auch eben durch das Kopplungsverbot begrenzter, Anwendungsbereich.

---

[530] Für eine einheitliche Interpretation auch *Engeler*, ZD 2018, 55 (57 f.); *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Article 6(1) (b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8.10.2019, Rn. 27.

[531] *Engeler*, ZD 2018, 55 (58).

(bb) Drei Lesarten

Das Kriterium der zur Erfüllung des Vertrags erforderlichen Daten ist daher in Art. 6 Abs. 1 lit. b und Art. 7 Abs. 4 DS-GVO einheitlich zu interpretieren. Für die Ausfüllung seines Inhalts bieten sich drei Lesarten an.[532] Man kann die Vertragserforderlichkeit (i) ökonomisch, (ii) rechtlich objektiv oder (iii) rechtlich subjektiv im Sinne der Parteivereinbarung verstehen. Dahinter steckt jeweils die Frage, inwiefern besonders Geschäftsmodelle aus dem Bereich von Daten als Gegenleistung in den Genuss der Rechtmäßigkeit der Datenverarbeitung qua Einwilligung gelangen sollen.[533] Irrelevant ist dabei jedoch jeweils, inwieweit die Datenverwendung transparent gemacht wird als Gegenleistung[534] – dies ist allein eine Frage der Informiertheit der Einwilligung.[535]

α. Ökonomischer Erforderlichkeitsmaßstab

Mit einem stärker ökonomisch orientierten Maßstab könnte man all jene Daten für erforderlich halten, welche der Anbieter sammeln und verarbeiten muss, um das Angebot kostendeckend am Markt erbringen zu können.[536] Erforderlichkeit wäre dann letztlich zu orientieren an Wirtschaftlichkeit im ökonomischen Sinne.

In logischer Hinsicht kann diese Argumentation immerhin für sich beanspruchen, dass in der Tat langfristig die Verarbeitung aller ökonomisch erforderlichen Daten auch für die Vertragserfüllung erforderlich ist, da derartige Verträge sonst am Markt nicht existieren würden und auch nicht erfüllt werden könnten. Zugleich liefe dies jedoch auf eine durch das Kopplungsverbot nicht weiter eingehegte Bestandsgarantie für alle denkbaren Geschäftsmodelle im Bereich von Daten als Gegenleistung hinaus. Das Kopplungsverbot liefe in diesem Bereich dann faktisch leer.[537] Das kann jedoch angesichts des klaren Auftrags im 42. und 43. Erwägungsgrund, Ungleichgewichten entgegenzuwirken, nicht überzeugen, da diese gerade im Bereich von Daten als Gegenleistung be-

[532] Vgl. auch *Engeler*, ZD 2018, 55 (57), der die objektive und die subjektive Variante unterscheidet; zu den drei Lesarten bereits *Hacker*, ZfPW 2019, 148 (183).

[533] Siehe nur *Krohm/Müller-Peltzer*, ZD 2017, 551 (553); *Schantz*, NJW 2016, 1841 (1845); *Ziegenhorn/von Heckel*, NVwZ 2016, 1585 (1587 f.).

[534] So aber *Buchner*, DuD 2016, 155 (159); *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 51; *Tavanti*, RDV 2016, 295 (296); Anklänge auch bei *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 30; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 21; *Gierschmann* in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung, 2017, Art. 7 Rn. 65.

[535] Im Ergebnis wie hier *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 Rn. 63.

[536] *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 30; ähnlich *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 48 und 51; *Krohm/Müller-Peltzer*, ZD 2017, 551 (554); *Tavanti*, RDV 2016, 231 (235 f.).

[537] *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2018, Art. 7 DS-GVO Rn. 41.1.

sonders ausgeprägt erscheinen: Man denke nur an die Marktstellung von Facebook, Google und anderen. Zudem können etwa Werbeeinnahmen unstreitig auch ohne Personalisierung erzielt werden, weshalb personalisierte Werbung auch ökonomisch, jedenfalls zur Kostendeckung, nicht zwingend erforderlich ist.[538] Dies deutet bereits darauf hin, dass völlig unklar wäre, wie jeweils exakt eruiert werden könnte, die Verarbeitung welcher Daten ökonomisch erforderlich ist, zumal die ökonomische Tragfähigkeit eines Geschäftsmodells von einer Reihe von Faktoren abhängt, die mit der Datenverarbeitung selbst in keinem Zusammenhang steht (etwa Finanzierungskosten, Produktionskosten etc.).

Daher ist diese Interpretation letztlich abzulehnen. Auch das Bundeskartellamt hat in seiner Facebook-Entscheidung richtigerweise nicht berücksichtigt, ob die Datenverarbeitung das Geschäftsmodell effizienter oder personalisierter macht, da dies – jedenfalls grundsätzlich – gerade keine Frage der Vertragserforderlichkeit ist.[539]

β. Objektiver Erforderlichkeitsmaßstab

Den Gegenpol zu der stark permissiven ökonomischen Interpretation der Vertragserforderlichkeit stellt der restriktive objektive Erforderlichkeitsmaßstab dar. Danach kann nur in die Verarbeitung solcher Daten wirksam eingewilligt werden, die zur Erreichung des objektiv verstandenen, „charakteristischen" Hauptzwecks von Verträgen einer bestimmten Art erforderlich sind.[540] Die auf der Einwilligung beruhende Datenverarbeitung muss daher auf den Kern des Vertrags beschränkt bleiben, bei sozialen Netzwerken also etwa die Ermöglichung des reibungslosen Zugangs zu und des Interagierens in ihnen. Aktivitäten, die mit diesen als Hauptzweck des Vertrages ausgewiesenen Tätigkeiten nicht notwendig, sondern nur aufgrund des ökonomischen Geschäftsmodells verbunden sind (etwa personalisierte Werbung), sind zur Erfüllung des Vertrags dann nicht mehr erforderlich. Eine darauf ausgerichtete Datenverarbeitung kann daher nicht Gegenstand der Einwilligung sein, wenn die Vertragserfüllung von dieser Einwilligung abhängt.

Entscheidend gegen diese Konzeption spricht jedoch, dass der Hauptzweck eines Austauschvertrags schon grundsätzlich, besonders aber im Bereich der

---

538 *Golland*, MMR 2018, 130 (131).

539 Bundeskartellamt, Fallbericht v. 15.2.2019, Az. B6–22/16 (*Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung*), 11 f.; Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 688 ff.; zustimmend *Buchner*, WRP 2019, 1243 (1247).

540 *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8.10.2019, Rn. 27, 30; *Stemmer*, in: BeckOK DatenschutzR, 26. Ed. 1.5.2018, Art. 7 DS-GVO Rn. 41; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 49 f.; *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, Rn. 501; *Golland*, MMR 2018, 130 (130); wohl auch *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 32.

digitalen Wirtschaft, kaum zu ermitteln ist.[541] Typischerweise handelt es sich nicht um einen klassischen, auf einen einmaligen Austausch beschränkten Kaufvertrag, sondern um längerfristige Transaktionen mit komplexen Nebenbedingungen, die verschiedene Vertragstypen ineinander verschmelzen oder diese transzendieren.[542] Daher wird sich der fiktive Zweck eines Vertrages kaum wirklich objektiv bestimmen lassen; vielmehr wird er regelmäßig lediglich die Vorfestlegungen der Interpreten widerspiegeln.

Auch die Entscheidung des EuGH in der Rechtssache *Huber* kann einen objektiven Maßstab nicht rechtfertigen. Dort hat der Gerichtshof zwar festgehalten, dass der Begriff der Erforderlichkeit i. S. v. Art. 7 lit. e DSRL (nunmehr Art. 6 Abs. 1 lit. e DS-GVO) so ausgelegt werden muss, dass er in vollem Umfang dem in Art. 1 Abs. 1 DSRL definierten Ziel des Datenschutzes gerecht wird.[543] Allerdings ist die Zielsetzung der DS-GVO bekanntlich eine doppelte, in der neben dem Datenschutz auch der freie Datenverkehr aufgeführt wird.[544] Schließlich hätte aber selbst eine strikt datenschutzfreundliche Auslegung des Erforderlichkeitsmaßstabs nicht notwendig den soeben erläuterten objektiven Maßstab zur Folge, da auch insofern die Operationalisierungsprobleme bestehen bleiben. Auch ein subjektiver Maßstab kann die Zielsetzungen der DS-GVO wahren, wie gleich zu zeigen ist.

γ. Subjektiver Erforderlichkeitsmaßstab

Die Schwierigkeit der konkreten Bestimmbarkeit vermeidet ein subjektiver, vertragsimmanenter Erforderlichkeitsmaßstab, bei dem sich die Vertragserforderlichkeit danach richtet, was die Vertragsparteien konkret und wirksam vereinbart haben.[545] Dies hat erstens den Vorteil, dem Wortlaut des Kopplungsverbots am klarsten zu entsprechen. Weder Anhaltspunkte für einen ökonomischen Maßstab noch für einen objektiven Hauptzweck finden sich dort. Vielmehr geht es schlicht um die Erfüllung des Vertrags, und erfüllt werden grundsätzlich vertragliche Pflichten im Umfang dessen, was die Parteien vereinbart haben. Zweitens lässt sich dieser subjektive Maßstab einfach mit den hergebrachten Methoden der Vertragsauslegung operationalisieren. Drit-

[541] *Engeler*, ZD 2018, 55 (57); *Indenhuck/Britz*, BB 2019, 1091 (1094).

[542] Zur Frage des Vertragstypus, siehe *Haag*, Direktmarketing mit Kundendaten aus Bonusprogrammen, 2010, 44 ff.; *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012, 125 ff.; *Specht*, JZ 2017, 763; *Metzger*, AcP 216 (2016), 817 (835–838); *Schmidt-Kessel/Erler/Grimm/Kramme*, GPR 2016, 54 (61 f.); speziell zum Internet der Dinge *Heuer-James/Chibanguza/Stücker*, BB 2018, 2818 (2823 ff.); *Wendehorst*, in: Schulze/Staudenmayer (Hrsg.), Digital Revolution. Challenges for Contract Law in Practice, 2016, 189 (203 ff.); *Bräutigam/Klindt*, NJW 2015, 1137 (1138); *Solmecke/Vondrlik*, MMR 2013, 755 (755 ff.).

[543] EuGH, Urt. v. 16.12.2008 – Rs. C-524/06 (*Huber*) – Rn. 52.

[544] Art. 1 Abs. 1 DS-GVO; dazu ausführlich unten, § 5 A.I.2.c)aa).

[545] Dafür auch *Engeler*, ZD 2018, 55 (58); *Heinzke/Engel*, ZD 2020, 189 (191 f.); sowie bereits *Hacker*, ZfPW 2019, 148 (183).

tens besteht bei systematisch-teleologischer Auslegung auch nicht notwendig die Gefahr, dass die Anbieter durch die Aufnahme artifiziell weiter Leistungspflichten das Kopplungsverbot umgehen (und die Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO ermöglichen). Denn die Vertragspflichten müssen *wirksam* vereinbart werden.

Damit kommt den bürgerlich-rechtlichen Grenzen der Privatautonomie entscheidende Bedeutung zu (etwa §§ 138, 305 ff. BGB, dazu im Einzelnen unter § 5 C.).[546] In der Tat erscheint es vorzugswürdig, Korrekturen hinsichtlich der vertraglichen Leistungspflichten im allgemeinen Vertragsrecht, und nicht im Datenschutzrecht, vorzunehmen, da dort die normativen Wertungen, welche hinter den Grenzen der Privatautonomie stehen, am klarsten zutage treten und in positivrechtlichen Vorschriften mit ausgearbeiteter Dogmatik radiziert sind.[547] Die datenschutzrechtlichen Konsequenzen der jeweiligen Leistungspflichten können dann bei der konkreten Bewertung nach der jeweiligen BGB-Vorschrift berücksichtigt werden. Dies deutet nur einmal mehr auf die Notwendigkeit eines rechtsbereichsübergreifend integrierten Datenschutzprivatrechts hin. Dass damit dem nationalen Vertragsrecht erhebliche Bedeutung für das unionale Datenschutzrecht zuwächst, mag man unter Harmonisierungsgesichtspunkten bedauern,[548] ist jedoch letztlich unvermeidbar: Das Datenschutzrecht rekurriert auf vertragliche Kategorien, die ihrerseits jedoch weder im Datenschutzrecht noch (abschließend) im europäischen Privatrecht geregelt sind. Immerhin ist jedoch der praktisch wichtigste Fall, die AGB-Kontrolle, durchaus unionsrechtlich determiniert, so dass insofern auch eine Harmonisierung auf unionaler Ebene gewährleistet ist.

Kurz erwähnt sei an dieser Stelle abschließend noch, dass sich aus dieser subjektiven Vertragsperspektive das Folgeproblem ergibt, inwiefern auch die Erfüllung von Pflichten der betroffenen Person vertragserforderlich im Sinne des Kopplungsverbots sein kann. Dies kann jedoch am besten konkret am ersten Leitfall am Beispiel von Daten als Gegenleistung diskutiert werden.[549]

Zusammenfassend lässt sich damit festhalten, dass der subjektive Erforderlichkeitsmaßstab vorzugswürdig ist aus Gründen des Wortlauts, der Einfachheit der Operationalisierung und infolge der Verortung der Grenzen der Privatautonomie aus systematisch-teleologischer Perspektive.

(b) Abhängigkeit der Vertragserfüllung von der Einwilligung

Wie bereits oben erwähnt, ist es für die Bestimmung des Verhältnisses der Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO zur vertragserforderlichen Daten-

---

[546] *Engeler*, ZD 2018, 55 (57); *Indenhuck/Britz*, BB 2019, 1091 (1093 f.).

[547] *Hacker*, ZfPW 2019, 148 (190 f.); *Indenhuck/Britz*, BB 2019, 1091 (1093 f.); ähnlich auch *Heinzke/Engel*, ZD 2020, 189 (190); aA *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3747).

[548] Für ein Ausblenden nationalen Vertragsrechts daher *Golland*, MMR 2018, 130 (132).

[549] Siehe unten, Teil D.I.2.a)dd)(7)(aa).

verarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO wichtig zu erkennen, dass das Kopplungsverbot bei nicht für die Vertragserfüllung erforderlichen Daten nur dann greift, wenn die Vertragserfüllung von der Einwilligung in die Verarbeitung dieser Daten abhängig ist. Dieses Kriterium verwirklicht die Zielsetzung des 42. Erwägungsgrunds, wonach den betroffenen Personen auch bei Verweigerung der Einwilligung sinnvolle Alternativen zur Verfügung stehen müssen. Umstritten ist jedoch erneut, welche Alternativen als sinnvoll gelten können.

(aa) Die Relevanz der Marktmacht

Unstreitig erscheint, dass eine Abhängigkeit besteht, wenn ein Anbieter die Erteilung der Einwilligung zur Bedingung der Diensterbringung erhebt (*take it or leave it*) und dieser Anbieter eine Monopolstellung innehat (vgl. nochmals den 43. Erwägungsgrund mit dem Beispiel der Behörde). Denn dann kann der Nachfrager auch am Markt nicht auf ein Alternativangebot ohne Einwilligung ausweichen. Die Frage ist nur, ob die Marktmacht des Anbieters notwendige Voraussetzung für die Feststellung der Abhängigkeit ist.[550]

α. Literaturansichten

Noch präziser lässt sich die Frage darauf zuspitzen, ob die Abhängigkeit immer nur im dyadischen Verhältnis zwischen einem Anbieter (Verantwortlicher) und dem Nachfrager (betroffene Person) zu bestimmen ist, oder ob auch am Markt existierende, funktionsäquivalente Substitutverträge berücksichtigt werden müssen.[551] Existiert ein Duopol, bei dem ein Anbieter eine Einwilligung verlangt, der andere für das inhaltlich identische Angebot jedoch nicht,[552] so ist

[550] Dafür *Plath*, in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 7 DSGVO Rn. 19 f. („Monopolstellung" als notwendige Bedingung); *Schneider*, Datenschutz nach der EU-Datenschutz-Grundverordnung, 2. Aufl. 2019, 166 (Erfüllung des Kopplungsgebots nur beim Monopolisten); tendenziell ebenso *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 27, 29; *Krohm/Müller-Peltzer*, ZD 2017, 551 (555); dagegen *Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 Rn. 52 (Marktmacht zu berücksichtigendes, aber nicht notwendiges Kriterium); ebenso *Buchner*, WRP 2019, 1243 (1245); *Buchner*, WRP 2018, 1283 (1286); *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 Rn. 52 f.; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 Rn. 62; *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 33; *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (716); wiederum anders *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 2018, Art. 7 DS-GVO Rn. 44 f. (Marktmacht gar kein relevantes Kriterium); ebenso *Golland*, MMR 2018, 130 (132 f.); Überlegungen zur Berücksichtigung kartellrechtlicher Wertungen ferner auch bei *Schweitzer et al.*, Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, Gutachten für das Bundesministerium für Wirtschaft und Energie, 2018, 116.

[551] Vgl. *Golland*, MMR 2018, 130 (132).

[552] Hinzukommen muss richtigerweise, dass die Daten bei der Alternative auch nicht aufgrund eines anderen Erlaubnistatbestands verarbeitet werden, da dies dem Sachgehalt des Kopplungsverbots entspricht.

bei einer dyadischen Sichtweise die Abhängigkeit zu bejahen, bei einer marktbezogenen hingegen zu verneinen. Letztere Sichtweise dominiert vor allem hinsichtlich der Kopplungsverbote nach altem deutschen Datenschutzrecht,[553] die von Art. 7 Abs. 4 DS-GVO abgelöst wurden. Nach § 28 Abs. 3b BDSG aF etwa durfte die „verantwortliche Stelle […] den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen […] abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist". In gleicher Weise formulierte § 95 Abs. 5 TKG ein Kopplungsverbot für Telekommunikationsdienste. Die Verwendung der Phrase „Zugang zu gleichwertigen vertraglichen Leistungen" sprach in der Tat eindeutig für eine marktbezogene Lesart.

Diese Frage ist für Art. 7 Abs. 4 DS-GVO jedoch in der Literatur, auch unter Kartellrechtlern, außerordentlich umstritten. Sie hängt unter anderem davon ab, inwiefern man das Datenschutzrecht mit kartellrechtlichen Wertungen aufladen möchte.[554] Einerseits wird dies bestritten: „size should not matter when it comes to data protection law".[555] Andererseits hebt der von hochrangigen Kartellrechtlern im Auftrag der EU-Kommission erstellte Bericht zum Kartellrecht im Bereich der digitalen Wirtschaft hervor: „Where Article 7(4) GDPR limits the validity of consent requested by a dominant company to what is necessary for the provision of the service, a permission under Article 6(1)(f) GDPR will arguably not reach further. Dominant firms may be subject to a particularly stringent data protection standard under both tests."[556] Auch das Bundeskartellamt erwähnt Marktmacht im Rahmen der datenschutzrechtlichen Bewertung der Weiterleitung von Daten im Facebook-Fall als Faktor.[557]

β. Stellungnahme: Marktmacht als gewichtiger indirekter Bewertungsfaktor

Nach hier vertretener Auffassung ist Marktmacht ein gewichtiger Parameter, aber keine notwendige Bedingung.[558] Denn sie indiziert, impliziert aber nicht

---

[553] Siehe etwa *Dammann*, ZD 2016, 307 (311); *Krohm/Müller-Peltzer*, ZD 2017, 551 (551 f.); *Gierschmann*, ZD 2016, 51 (54); *Wolff*, in: BeckOK DatenschutzR, 28. Ed. 1.8.2015, Art. 28 BDSG (aF) Rn. 170–172; *Kannenberg/Müller*, in: Scheurle/Mayen, TKG, 3. Aufl. 2018, § 95 Rn. 81; aA *Büttgen*, in: Beck'scher TKG-Kommentar, 4. Aufl. 2013, § 95 Rn. 33.

[554] Siehe dazu die Nachweise in § 4, Fn. 550.

[555] *Colangelo/Maggiolino*, 42(3) World Competition Law and Economics Review 2019, 355 (367).

[556] *Crémer/de Montjoye/Schweitzer*, Competition Policy for the Digital Era, Bericht, 2019, 80; siehe auch ebd., 77.

[557] Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 646; zustimmend *Buchner*, WRP 2019, 1243 (1248).

[558] Ebenso *Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 Rn. 52 (Marktmacht zu berücksichtigendes, aber nicht notwendiges Kriterium); *Buchner*, WRP 2019, 1243 (1245); *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 Rn. 52 f.; *Klement*, *in: Simitis/Hornung/Spiecker gen. Döhmann*, *Datenschutzrecht*, *2019*, Art. 7 Rn. 62; *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 33; *Clifford/Graef/Valcke*, 20

zwingend, dass funktional äquivalente Alternativen am Markt zu vergleichbaren Bedingungen nicht bestehen. Wenn dies der Fall ist, muss eine Abhängigkeit jedoch sicher bejaht werden. Solch ein Mangel an funktional vergleichbaren Alternativen ist insbesondere dann zu konstatieren, wenn direkte oder indirekte Netzwerkeffekte[559] auftreten,[560] wie etwa auf dem Markt von Plattformen, die soziale Medien anbieten.[561] Auch die Verwirklichung datenschutzspezifischer Risiken, wie von *chilling effects*, erscheint bei marktmächtigen Unternehmen plausibler Weise erhöht.[562]

Allerdings sollte man Marktmacht nicht ohne Not zur notwendigen Bedingung für die Erfüllung des Kopplungsverbots erheben. Denn eine Abhängigkeit im Sinne von Art. 7 Abs. 4 DS-GVO kann auch dann bestehen, wenn der Verantwortliche nicht marktmächtig ist, der spezifische Vertrag aber nur gegen Einwilligung in nicht vertragserforderliche Datenverarbeitung angeboten wird. Der Wortlaut des unionalen Kopplungsverbots spricht eindeutig davon, dass nur „*die* Erfüllung *eines* Vertrags“,[563] und nicht die Erfüllung aller wirtschaftlich vergleichbaren Verträge am Markt (aller „gleichwertigen vertraglichen Leistungen“, § 28 Abs. 3b BDSG aF, § 95 Abs. 5 TKG), von der Einwilligung abhängig sein muss. Auch die Nichtübernahme des 34. Erwägungsgrunds des Ratsvorschlags der DS-GVO, der die deutschen Kopplungsverbote nachgebildet hätte,[564] spricht gegen eine rein marktbezogene Sichtweise im Rahmen der Abhängigkeit. Daher erscheint es vorzugswürdig, trotz mangelnder Marktmacht eine Abhängigkeit gegebenenfalls zu bejahen, diesen Umstand aber im Rahmen der Rechtsfolge flexibel zu berücksichtigen (dazu sogleich unter (c)).

(bb) Dienst gegen monetäre Zahlung als zumutbare Alternative

Eine Abhängigkeit im Sinne des Kopplungsverbots ist definitiv zu verneinen, wenn der Anbieter selbst eine funktional vergleichbare Alternative des Pro-

German Law Journal 2019, 679 (716); *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.4.

559 Zu Netzwerkeffekten etwa *Belleflamme/Peitz*, Industrial Organization, 2010, 549 ff.; *Engert*, AcP 213 (2013), 321 (325 ff.).

560 *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 508; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 Rn. 53.

561 Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 413: mehr als 90 % Marktanteil von Facebook auf dem relevanten Markt; ebd., Rn. 417: „Lediglich Facebook.com bietet sämtliche Funktionalitäten zur Abbildung eines virtuellen sozialen Raumes an“; *Hacker/Petkova*, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1 (21); *Raue*, JZ 2018, 961 (965 f.); *Martinelli*, in: Reins (Hrsg.), Regulating New Technologies in Uncertain Times, 2019, 133 (136).

562 *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (715 Fn. 191).

563 Gemeint ist klarerweise der konkret abgeschlossene Vertrag.

564 Siehe Rat der Europäischen Union, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DatenschutzGrundverordnung), Interinstitutionelles Dossier: 2012/0011 (COD), Az. 9565/15 (11.6.2015), 19.

dukts gegen monetäre Zahlung (oder eine Mischung aus monetärer Zahlung und nicht personalisierter Werbung) anbietet.[565] Denn dann ist der Nutzer für die Inanspruchnahme des Angebots nicht mehr darauf angewiesen, seine Einwilligung zu erteilen, sondern kann zu einer adäquaten Alternative, etwa durch monetäre Zahlung, übergehen. Allerdings ist eine taugliche Alternative, welche die Abhängigkeit ausschließt, nur dann anzunehmen, wenn der Nutzer keine signifikanten monetären Nachteile erleidet, der Preis also angemessen ist.[566] Nur dann besteht eine „echte oder freie Wahl" im Sinne des 43. Erwägungsgrunds, bei welcher der Nutzer in den Genuss des Angebots kommt „ohne Nachteile zu erleiden".[567]

(c) Rechtsfolge: Widerlegliche Vermutung

Liegt der Tatbestand des Kopplungsverbots vor, so ist schließlich auch die Rechtsfolge noch umstritten. Dies liegt daran, dass Art. 7 Abs. 4 DS-GVO zwar nur davon spricht, dass der Erfüllung des Kopplungsverbots in größtmöglichem Umfang Rechnung getragen werden soll, der 43. Erwägungsgrund in seinem zweiten Satz jedoch eine Fiktion der Unfreiwilligkeit für genau diesen Fall beinhaltet. Daher wurde in der Literatur teilweise lediglich auf eine gesteigerte Prüfpflicht mit freier Abwägung der Interessen und Grundrechte/-freiheiten der Beteiligten geschlossen.[568] Die, soweit ersichtlich, erste höchstrichterliche Entscheidung zu diesem Spannungsverhältnis erging jedoch noch im August 2018 durch den österreichischen Obersten Gerichtshof. Dieser lehnte unter implizitem Rückgriff auf die *acte clair*-Doktrin eine Vorlage an den EuGH ab und urteilte:

„Das Spannungsverhältnis zwischen dem Text der Verordnung und dem Erwägungsgrund 43 ist offensichtlich dahin aufzulösen, dass an die Beurteilung der ‚Freiwilligkeit' der Einwilligung strenge Anforderungen zu stellen sind. Bei der Koppelung der Einwilligung zu einer Verarbeitung vertragsunabhängiger personenbezogener Daten mit einem Vertragsschluss ist grundsätzlich davon auszugehen, dass die Erteilung der Einwilligung nicht freiwillig erfolgt, wenn nicht im Einzelfall besondere Umstände für eine Freiwilligkeit der datenschutzrechtlichen Einwilligung sprechen".[569]

In der Tat lässt sich eine Fiktion der Unfreiwilligkeit nicht begründen, da diese im Wortlaut der Verordnung keinen Niederschlag gefunden hat. Da jedoch

[565] *Krohm/Müller-Peltzer*, ZD 2017, 551 (553); *Golland*, MMR 2018, 130 (134); *Gierschmann*, ZD 2016, 51 (54); *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 33; *Hacker*, ZfPW 2019, 148 (183); *Hacker*, 7 International Data Privacy Law 2017, 266 (282); dies übersieht *Engeler*, ZD 2018, 55 (59).

[566] Dazu im Einzelnen unten, § 6 C.II.5.b)bb).

[567] Ebenso *Golland*, MMR 2018, 130 (134); *Krohm/Müller-Peltzer*, ZD 2017, 551 (553); *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 8 (erhebliche Zusatzkosten).

[568] *Engeler*, ZD 2018, 55 (58f.); *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 Rn. 58.

[569] ÖOGH, Urteil vom 31.8.2018 – 6 Ob 140/18h, ZD 2019, 72 Rn. 46.

auch dieser Wortlaut mit der Maßgabe, dem Tatbestand des Kopplungsverbots in größtmöglichem Umfang Rechnung zu tragen, von einer grundsätzlichen Rechtsfolge der Unfreiwilligkeit auszugehen scheint, deren Stoßrichtung durch den 43. Erwägungsgrund noch verstärkt wird, dürfte der ÖOGH *de lege lata* korrekt judiziert haben,[570] auch wenn er die Frage dem EuGH hätte vorlegen müssen.[571] Dies zeigt nicht zuletzt die abweichende Entscheidung des italienischen *Corte di Cassazione* (wenngleich zum Begriff der Freiwilligkeit unter Geltung der DSRL),[572] der sich trotz Erwähnung der DS-GVO allerdings ebenfalls eine Vorlage an den EuGH erspart hat.[573]

(aa) Widerlegung durch funktional äquivalentes Marktangebot

Besondere Umstände, die trotz Kopplung für eine Freiwilligkeit sprechen, können nach hier vertretener Auffassung etwa in der Existenz von funktional äquivalenten, marktgängigen Angeboten ohne Einwilligungsnotwendigkeit liegen.[574] Dabei steht der Berücksichtigung von Marktalternativen auch nicht entgegen, dass der Vorschlag des Rates, den „Zugang zu gleichwertigen vertraglichen Leistungen" in die Erwägungsgründe aufnehmen zu lassen, letztlich nicht übernommen wurde.[575] Denn sofern diese vorliegen, korrigiert der Markt selbst das potenzielle Ungleichgewicht zwischen betroffener Person und Verantwortlichem und sorgt für Alternativen.[576] Dann jedoch ist die im 42. und 43. Erwägungsgrund zum Ausdruck kommende Zielsetzung des Kopplungsverbots nicht mehr einschlägig.

---

[570] Für eine Vermutung auch *Ernst*, ZD 2017, 110 (112); *Albrecht*, CR 2016, 88 (91); *Härting*, Datenschutz-Grundverordnung, 2016, Rz. 394; *Schneider*, Datenschutz nach der EU-Datenschutz-Grundverordnung, 2. Aufl. 2019, 166; *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2018, Art. 7 DS-GVO Rn. 46; *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (717); *Gierschmann* in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung, 2017, Art. 7 Rn. 62; *Hacker*, ZfPW 2019, 148 (183); wohl auch *Dammann*, ZD 2016, 307 (311) (striktes Kopplungsverbot); aA *Engeler*, ZD 2018, 55 (59) (grundsätzliche Zulässigkeit, allerdings unter Außerachtlassung des Kriteriums der Abhängigkeit in der Begründung); ähnlich *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 28 (Beschränkung auf sachfremde Begleiterscheinung).

[571] *Sattler*, GRUR 2019, 1023 (1025).

[572] Corte di Cassssazione, Urt. v. 2.7.2018 – Nr. 17278, unter 2.5; dazu *Pertot*, GPR 2019, 54 (55 ff.). Nach dem *Corte* führt eine Kopplung nur dann zur Unfreiwilligkeit, wenn sie eine unverzichtbare und unersetzbare Leistung betrifft („infungibile, […] irrinunciabile").

[573] Kritisch insoweit zu Recht *Sattler*, GRUR 2019, 1023 (1025); *Pertot*, GPR 2019, 54 (56).

[574] Ähnlich *Buchner*, WRP 2019, 1243 (1245); *Krohm/Müller-Peltzer*, ZD 2017, 551 (554); *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 52; grundsätzlich auch *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 82, 87; aA *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 11.

[575] Siehe oben, § 4, Fn. 564.

[576] Ähnlich *Schneider*, Datenschutz nach der EU-Datenschutz-Grundverordnung, 2. Aufl. 2019, 166.

(bb) Widerlegung durch hypothetische wirksame Leistungspflicht

Beachtlich ist ferner auch die Auffassung, wonach es gegen eine Unfreiwilligkeit sprechen soll, wenn die Datenverarbeitung infolge einer hypothetischen wirksamen vertraglichen Leistungspflicht auf Art. 6 Abs. 1 lit. b DS-GVO hätte gestützt werden können.[577] Tatsächlich erscheint es widersprüchlich, eine Einwilligung am Kopplungsverbot scheitern zu lassen, wenn dieselbe Datenverarbeitung auf vertraglicher Grundlage hätte legitimiert werden können. Allerdings wird die Behandlung weiter Leistungspflichten in der AGB-Kontrolle zeigen, dass die wirksame Vereinbarung vertraglicher Pflichten lediglich zur Legitimation von Datenverarbeitungsprozessen typischerweise nur bedingt möglich ist.[578]

Zudem kann von Gerichten nicht verlangt werden, alle auch nur in Betracht kommenden hypothetischen Vertragsgestaltungen auf ihre potenzielle Wirksamkeit und ihre datenschutzrechtlichen Konsequenzen zu prüfen. Daher muss diese Fallgruppe auf naheliegende Gestaltungen, die offensichtlich eine datenschutzrechtliche Legitimierung bewirkt hätten, beschränkt bleiben. Im Übrigen ist die datenschutzrechtskonforme Vertragsgestaltung eine Aufgabe, welche die Vertragsparteien selbst wahrnehmen müssen.

(cc) Beschränkung des Kopplungsverbots auf dringliche Angewiesenheit?

Allenfalls zurückgenommene Bedeutung kommt allerdings nach hier vertretener Auffassung der ökonomischen Dringlichkeit zu, mit welcher der Nutzer Zugang zu den Diensten begehrt. Dieses Kriterium hatte der *Corte di Cassazione* seiner Entscheidung zugrunde gelegt.[579] Zwar kann eine besondere Angewiesenheit auf einen Dienst (z. B. Daseinsvorsorge) in der Tat für eine Unfreiwilligkeit sprechen. Allerdings indiziert umgekehrt die mangelnde ökonomische Dringlichkeit keine Freiwilligkeit,[580] da sich Ungleichgewichte (43. Erwägungsgrund) und mangelnde Alternativen (42. Erwägungsgrund) auch beim Zugang zu einer Taschenlampen-App auftun können. Abgesehen davon, dass eine derartige Dringlichkeit objektiv nur schwer zu bestimmen wäre, differenzieren beide Erwägungsgründe schon dem Wortlaut nach an keiner Stelle nach der Angewiesenheit auf das jeweilige Angebot. Vielmehr spricht der 42. Erwägungsgrund davon, dass eine freie Wahl nur besteht, wenn die Einwilligung verweigert werden kann, ohne dass die betroffene Person „Nachteile“ erleidet. Es ist nicht ersichtlich, dass entgangene Möglichkeiten des Kon-

[577] *Engeler*, ZD 2018, 55 (59); dagegen *Golland*, MMR 2018, 130 (132). Auch für die hypothetische Prüfung muss der subjektive Erforderlichkeitsmaßstab unter Ausblendung von Nutzerpflichten gelten, dazu sogleich, § 4 B.II.2.b)bb).

[578] Siehe bereits *Hacker*, ZfPW 2019, 148 (190 f.) und unten, § 5 C.II.1.e)cc)(1)(b).

[579] Siehe oben, § 4, Fn. 572.

[580] So aber *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 Rn. 61 und 63; *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 27; *Pertot*, GPR 2019, 54 (56).

sums oder der einfachen Bewältigung des Alltags keine Nachteile im Sinne des Erwägungsgrunds darstellen sollten. Wäre eine Beschränkung auf besondere Angewiesenheit intendiert gewesen, so hätte die Formulierung lauten müssen, dass der Nutzer keine „erheblichen" oder „existenziellen" Nachteile erleiden darf.

Diese Exegese ist auch in teleologischer Hinsicht stimmig, da datenschutzrechtliche Risiken ja nicht deswegen geringer ausfallen, weil der Nutzer auf die jeweiligen Angebote nicht besonders dringlich angewiesen ist. Sie ist nach hier vertretener Ansicht zudem diejenige, welche die beteiligten Grundrechte unter der Prämisse heterogener Datenschutzpräferenzen am ehesten in einen schonenden Ausgleich bringt (dazu sogleich). Vor dem Hintergrund des risikobasierten Ansatzes der DS-GVO und des Wortlauts des 42. und 43. Erwägungsgrunds sind die genannten Risiken daher auch in vergleichbar trivialen Situationen von Bedeutung: Datenschutz und Wahlfreiheit sollten nicht dort enden, wo die Freizeitgestaltung beginnt.

(d) Grundrechtskonformität des Kopplungsverbots

Die soeben genannten Möglichkeiten, das Kopplungsverbot auszuschalten, sind entscheidend für seine Vereinbarkeit mit den Chartagrundrechten. Denn es greift unübersehbar in die Vertragsfreiheit sowie die unternehmerische Freiheit ein (Art. 16 GRCh[581]).[582] Kunden bleibt es verwehrt, ihre Daten rechtswirksam maximal zu monetarisieren[583] und damit ihre Budgetrestriktionen zu erweitern.[584] Allerdings müssen diese Grundrechte abgewogen werden mit dem unionalen Datenschutzgrundrecht aus Art. 8 GRCh. Denn in der Tat kommen die Budgeterweiterung und die stärkere Gewährleistung der Vertragsfreiheit, die ein Verzicht auf das Kopplungsverbot oder eine deutlich permissivere Lesart bedingen würde, nur einem Teil der Beteiligten zugute: Denjenigen Unternehmen, die ein datenfinanziertes Geschäftsmodell anbieten, und den Betroffenen, die gering ausgeprägte Datenschutzpräferenzen haben. Ein völliger Verzicht auf ein Kopplungsverbot ließe jedoch, ebenso wie eine sehr permissive Lesart, die Betroffenen mit starken Datenschutzpräferenzen außen vor.

Der Weg des Unionsgesetzgebers und die hier vorgeschlagene Interpretation ermöglichen insoweit einen nachvollziehbaren und schonenden Ausgleich. Einerseits wird der Weg dahin geebnet, nicht als Eintrittsbillet zu digitalen Dienstleistungen erheblich Mengen an funktional nicht erforderlichen personenbezogenen Daten preisgeben zu müssen. Das dahingehende Interesse ist

[581] Nach dem EuGH ist die Vertragsfreiheit Bestandteil von Art. 16 GRCh, siehe EuGH, Urt. v. 18.7.2013 – Rs. C-426/11 (*Alemo-Herron*) – Rn. 32.

[582] Siehe nur *Engeler*, ZD 2018, 55 (56); *Krohm/Müller-Peltzer*, ZD 2017, 551 (555); *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 Rn. 59.

[583] Vgl. *Krohm/Müller-Peltzer*, ZD 2017, 551 (553); *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 Rn. 60.

[584] Siehe oben, § 3 B.I.1.c).

grundsätzlich schutzwürdig (vgl. neben Art. 8 auch Art. 11 Abs. 1 GRCh) und entspricht den Präferenzen der Betroffenen auf der rechten Seite der U-förmigen Präferenzkurve.[585] Andererseits können die Parteien – bei Zugrundelegung des subjektiven Erforderlichkeitsmaßstabs – durch Gestaltung ihrer Vertragsbeziehungen Art. 6 Abs. 1 lit. b DS-GVO in Anspruch nehmen und das Kopplungsverbot aus dem Weg räumen. Zudem bietet sich gerade Unternehmen die Option, zumindest parallel zu datenfinanzierten Geschäftsmodellen monetär (durch Geldzahlung und/oder nicht personalisierte Werbung) finanzierte Alternativen zu eröffnen und damit ebenfalls das Kopplungsverbot rechtssicher auszuhebeln. Da einige Unternehmen derartige Modelle auch bereits jetzt schon am Markt anbieten,[586] lässt sich auch nicht argumentieren, dass die Umsetzung technisch oder ökonomisch unzumutbar wäre. Ferner spricht ohnehin die Existenz von nicht datenbasierten Alternativen am Markt gegen eine Unfreiwilligkeit der Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO. Auch dies entlastet die Anbieter.

Insofern bietet das Kopplungsverbot in der hier vorgeschlagenen Interpretation einen schonenden Ausgleich zwischen den beteiligten Grundrechten und Interessen, der insbesondere der Heterogenität der Datenschutzpräferenzen unter den Nutzern Rechnung trägt.[587] Um es auf den Punkt zu bringen: Nutzer mit schwach ausgeprägten Datenschutzpräferenzen werden nicht schlechter gestellt, sofern Anbieter durch Vertragsgestaltung oder die Eröffnung einer monetären Alternative das Kopplungsverbot aushebeln.[588] Dies ist letzteren jedoch zumutbar, da andernfalls angesichts der zunehmenden Vernetzung aller Austauschprozesse Nutzer mit stark ausgeprägten Datenschutzpräferenzen von erheblichen Teilen der digitalen Wirtschaft faktisch ausgeschlossen würden. Insofern zeigt sich noch einmal, dass eine Beschränkung des Kopplungsverbots auf existenzielle Angebote[589] dem Grad der Durchdringung der vernetzten Wirtschaft durch datenverarbeitende Prozesse nicht gerecht würde. Im *Internet of Everything* ist die hier vorgeschlagene Auslegung vielmehr für eine signifikante Nutzergruppe notwendige Bedingung der Möglichkeit digitaler Teilhabe.[590]

---

[585] Siehe oben, § 3, Fn. 163.

[586] Siehe *Hacker*, ZfPW 2019, 148 (156).

[587] Im Ergebnis ähnlich *Krohm/Müller-Peltzer*, ZD 2017, 551 (555).

[588] Diese Nutzer können in diesem Fall weiterhin ihre personenbezogenen Daten als Budgeterweiterung einsetzen, sodass sich im Ergebnis für sie nichts ändert.

[589] Dazu oben, § 4 B.I.3.a)dd)(3)(c)(bb).

[590] Vgl. auch BVerfG GRUR 2020, 74 Rn. 85 – Recht auf Vergessen I: „In allen Lebensbereichen werden zunehmend für die Allgemeinheit grundlegende Dienstleistungen auf der Grundlage umfänglicher personenbezogener Datensammlungen und Maßnahmen der Datenverarbeitung von privaten, oftmals marktmächtigen Unternehmen erbracht, die maßgeblich über die öffentliche Meinungsbildung, die Zuteilung und Versagung von Chancen, die Teilhabe am sozialen Leben oder auch elementare Verrichtungen des täglichen Lebens entscheiden. Die einzelne Person kommt kaum umhin, in großem Umfang personenbezogene Daten gegenüber Unternehmen preiszugeben, wenn sie nicht von diesen grundlegenden

(4) Weitere Abwägungsgesichtspunkte

Neben den Kriterien des Kopplungsverbots kommen schließlich noch weitere Abwägungsgesichtspunkte in Betracht, die eine Unfreiwilligkeit der Einwilligung bedingen können.

(a) Täuschung, Drohung und Zwang

Zunächst sind hier die klassischen Antagonisten freier Entscheidung zu nennen: Täuschung,[591] Drohung und Zwang. Die Frage der Anwendbarkeit von § 123 Abs. 1 BGB neben dem Freiwilligkeitsgebot der DS-GVO wird ausführlich im Rahmen der zivilrechtlichen Ordnungskategorien behandelt.[592] Bereits hier kann jedoch festgehalten werden, dass im Ergebnis die Kriterien von § 123 Abs. 1 BGB in das Tatbestandsmerkmal der Freiwilligkeit nach Art. 4 Nr. 11 DS-GVO hineingelesen werden müssen,[593] da dieses nicht auf bestimmte Formen der Unfreiwilligkeit, wie etwa ökonomische Abhängigkeit, festgelegt, vielmehr für die Ausfüllung mit derartigen Freiwilligkeitshindernissen offen und auch die Zielsetzung, privatautonome Gestaltung im Rahmen der Einwilligung zu gewährleisten, einschlägig ist.

(b) Einwilligung im Beschäftigtenverhältnis, § 26 Abs. 2 BDSG

Eine besondere Bedeutung hat die Freiwilligkeit der Einwilligung ferner traditionell im Beschäftigungsverhältnis. Sie hat daher, infolge der Öffnungsklausel in Art. 88 Abs. 1 DS-GVO, eine spezifische Regelung in § 26 Abs. 2 BDSG erfahren.[594] Ohne hier ins Detail gehen zu können, lässt sich festhalten, dass nach herkömmlicher Auffassung grundsätzlich das hierarchische Verhältnis zwischen Arbeitgeber und Beschäftigten der Freiwilligkeit der Einwilligung entgegensteht, allerdings eine Einzelfallbetrachtung angezeigt ist.[595] § 26 Abs. 2 S. 2 BGB statuiert jedoch, dass Freiwilligkeit insbesondere dann vorliegen kann, „wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen." Auch der 155. Erwägungsgrund geht zumindest grundsätzlich von der Möglichkeit einer wirksamen Einwilligung aus. Ob Arbeitgeber das rettende Ufer dieser Ausnahmebestimmung erreichen können, wenn

Dienstleistungen ausgeschlossen sein will." Dies gilt freilich nicht nur für „grundlegende", sondern für Dienstleistungen und Angebote jeglicher Art.

591 Bei einer Täuschung fehlt zudem zumeist die Informiertheit; nichtsdestoweniger wird die Täuschung auch als Fall der Unfreiwilligkeit behandelt, siehe *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 8; ferner unten, § 5, Fn. 321.

592 Siehe unten, § 5 B.II.2.e).

593 *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2018, Art. 7 DS-GVO Rn. 39; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 42.

594 Dazu etwa *Reiserer/Christ/Heinz*, DStR 2018, 1501.

595 Ausführlich *Wybitul/Böhm*, BB 2015, 2101.

sie eine Einwilligung zur Verarbeitung von Daten im Rahmen der Bewerberauswahl einholen (*people analytics*), ist umstritten,[596] kann hier jedoch nicht vertieft werden.

(5) Anwendung auf die drei Leitfälle

Auch diese Kriterien müssen sich wiederum bei der Anwendung auf die drei Leitfälle bewähren.

(a) Daten als Gegenleistung

Eine zentrale Stellung kommt dabei der Frage zu, inwiefern im Rahmen von Geschäftsmodellen, bei denen Daten als Gegenleistung fungieren, eine im Lichte des Kopplungsverbots wirksame Einwilligung eingeholt werden kann. Dabei ist zwar nicht im Ergebnis, aber analytisch doch zwischen den unterschiedlichen Typen dieses Geschäftsmodells zu differenzieren. Wie oben ausführlich dargelegt,[597] lässt sich ein datenbasiertes Grundmodell von einem monetären unterscheiden. Das datenbasierte Geschäftsmodell umfasst vollkommen datenfinanzierte Dienste, bei denen keinerlei monetäre Gegenleistung fällig wird, sowie Freemium-Angebote. Unter das monetäre Grundmodell fallen hingegen Rabattmodelle, bei denen die Überlassung von Daten zu einem expliziten Preisnachlass führt, sowie data on top-Modelle, bei denen zusätzlich zu dem monetären Marktpreis Daten überlassen werden, deren Entgeltqualität nicht eigens ausgewiesen wird.

(aa) Vertragsinhalt bei „Daten als Gegenleistung" mit datenbasiertem Grundmodell

Im Rahmen des datenbasierten Grundmodells hat die Überlassung von Daten typischerweise Entgeltqualität. Für den (nach Einschätzung des Bundeskartellamts allerdings marktmächtigen) Anbieter Facebook hat das Bundeskartellamt insoweit zum Kopplungsverbots geurteilt: „Eine wirksame Einwilligung liegt nur dann vor, wenn die Bereitstellung des Dienstes Facebook.com nicht von der Erteilung der Einwilligung abhängig gemacht wird."[598] Eine diametral entgegengesetzte, gleich im Einzelnen darzustellende Sichtweise verneint jedoch gerade in den Fällen des datenbasierten Grundmodells die Anwendbarkeit des Kopplungsverbots, auch auf Grundlage des subjektiven Erforderlich-

[596] Differnzierend *Betz*, ZD 2019, 148 (151); ablehnend *Rudkowski*, NZA 2019, 72 (73) für die Vorhersage von Straftaten; siehe auch *Aloisi/Gramano*, Comparative Labor Law & Policy Journal 2020 (im Erscheinen).

[597] Siehe oben, § 3 A.II.2.

[598] Bundeskartellamt, Fallbericht v. 15.2.2019, Az. B6–22/16 (*Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung*), 1; siehe auch Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, 2; zustimmend *Buchner*, WRP 2019, 1243 (1247 f.).

keitsmaßstabs. Dogmatischer Ausgangspunkt ist dabei, dass möglicherweise eine Pflicht der Nutzer zur Überlassung von Daten und zur Einwilligung in deren Verarbeitung (konkludent) vertraglich vereinbart wurde.

α. Legitimation durch Nutzerpflichten?

Wenn tatsächlich eine Rechtspflicht der Nutzer zur Erteilung einer Einwilligung oder zur Überlassung von Daten besteht, dann ist denkbar, dass die Einwilligung zur Erfüllung des Vertrages erforderlich ist: nämlich zur Erfüllung der Vertragspflichten *des Nutzers*. Dies entspricht einer Auffassung in der Literatur,[599] der sich GA *Szpunar* in einem obiter dictum ausdrücklich angeschlossen hat.[600] Zwar hat sich die bisherige Diskussion des Erforderlichkeitsmaßstabs in der Literatur darauf fokussiert, ob die Verarbeitung für die Erfüllung der Pflichten *des Verantwortlichen* notwendig ist.[601] In der Tat ist jedoch zumindest nach dem Wortlaut von Art. 7 Abs. 4 DS-GVO nicht ausgeschlossen, dass auch Pflichten des Betroffenen legitimatorisch wirken können, da nur allgemein von der Erfüllung des Vertrags, und nicht der Pflichten des Verantwortlichen, die Rede ist.

Schlösse man sich dieser Auffassung an, so wäre die Konsequenz, dass die Einschlägigkeit des Kopplungsverbots maßgeblich davon abhinge, welche Pflichten für den Nutzer ausdrücklich oder konkludent vereinbart wurden, und ob diese Vereinbarungen wirksam sind. Dies wiederum sind Fragen, welche das nationale Vertragsrecht beantworten muss. GA *Szpunar* scheint der Auffassung zu sein, dass jedenfalls bei vollkommen datenfinanzierten Austauschverhältnissen, in denen der Betroffene einen Anspruch auf eine ökonomisch werthaltige Leistung erhält, konkludent zugleich eine Pflicht zur Überlassung von personenbezogenen Daten vereinbart wird. Seine Argumentation betrifft nicht nur das von ihm diskutierte Beispiel der Teilnahme an einem Gewinnspiel, sondern alle Formen von Daten als Gegenleistung mit datenbasiertem Grundmodell, mithin praktisch alle Bereiche der „kostenlos" angebotenen Dienstleistungen im Internet, etwa den Zugang zu sozialen Netzwerken oder die Nutzung einer Suchmaschine. Diese Auffassung eines synallagmatischen Modells entspricht jedenfalls für das deutsche Recht auch der wohl herrschenden Meinung im Vertragsrecht.[602]

---

[599] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 48; *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 31; *Heinzke/Engel*, ZD 2020, 189 (191, 193); wohl auch *Krohm/Müller-Peltzer*, ZD 2017, 551 (555).

[600] GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 99.

[601] Siehe emblematisch *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8.10.2019, Rn. 26 ff.

[602] Für eine synallagmatische Verknüpfung *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 268; *Bräutigam*, MMR 2012, 635 (640); *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 44; *Metzger*, AcP 216 (2016), 817 (834); *Specht*, JZ 2017, 763 (763); *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (221 f.); *Schmidt-Kessel/Grimm*, ZfPW 2017,

Nach hier vertretener Auffassung jedoch kann zwar, wie der Verfasser an anderer Stelle ausgeführt hat,[603] eine derartige Pflicht zur Überlassung von personenbezogenen Daten und zur Duldung von deren Verarbeitung durchaus nach deutschem Vertragsrecht wirksam vereinbart werden.[604] Dann wäre die Einwilligung in der Tat zur Vertragserfüllung erforderlich im Sinne von Art. 7 Abs. 4 DS-GVO – sofern denn Nutzerpflichten für diese Norm relevant sind. Ob allerdings die vertragliche Pflicht tatsächlich auch die Duldung des „Verkaufs"[605] der Daten an Dritte zu Zwecken personalisierter Werbung umfasst und ob diese Pflicht wirksam vereinbart wurde, ist jeweils eingehend durch Auslegung und konsequente Anwendung der Wirksamkeitsgrenzen des allgemeinen Vertragsrechts zu prüfen.[606]

In den meisten Fällen jedoch verzichten die Parteien auf eine diesbezügliche ausdrückliche Vereinbarung.[607] Dann jedoch wird bei Auslegung der Willenserklärungen gemäß §§ 133, 157 BGB nach hier vertretener Auffassung regelmäßig lediglich eine konditionale Gegenleistung dergestalt vereinbart, dass die Leistung des Anbieters nur geschuldet ist unter der (atypischen aufschiebenden Dauer-) Bedingung, dass der Nutzer (kontinuierlich) Daten überlässt.[608] Es besteht dann mithin keine vertragliche Pflicht des Nutzers, zu deren Erfüllung die Datenverarbeitung erforderlich sein könnte. Die Erfüllung einer Bedingung ist jedoch nicht mit der in Art. 7 Abs. 4 DS-GVO angesprochenen Erfüllung des Vertrags unmittelbar gleichzusetzen, da die aufschiebende Bedingung gem. § 158 Abs. 1 BGB regelmäßig gerade Voraussetzung für die Wirksamkeit des Vertrags ist, die logisch der Erfüllung vorgeschaltet und daher von dieser verschieden ist.

Allerdings ist letztlich kein wertungsmäßiger Unterschied zwischen der konditionalen und der synallagmatischen Verknüpfung erkennbar, der für die Frage der Anwendbarkeit des Kopplungsverbots relevant wäre. Daher dürfte

84 (104); *Langhanke*, Daten als Leistung, 2018, 131; auch andere mögliche Verknüpfungsformen betonend *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.5.

603 *Hacker*, ZfPW 2019, 148 (168 ff.).

604 So auch *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.5.–6; siehe auch *de Franceschi*, in: Schmidt-Kessel/Kramme (Hrsg.), Geschäftsmodelle in der digitalen Welt, 2017, 113 (120).

605 So ausdrücklich GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 99.

606 Siehe auch *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.5.; ferner ausführlich unten, § 5 C.I.-II.

607 Vereinbart wird bisweilen eine Klarnamenpflicht; zu deren Schicksal *Hacker*, ZfPW 2019, 148 (189 f.); zu weitergehenden Verpflichtungen, korrekte Daten zu überlassen, *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.5.; *Hacker*, ZfPW 2019, 148 (169 f.).

608 *Hacker*, ZfPW 2019, 148 (170 ff.); knapp auch *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (290); vgl. auch *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, 2016, 15 (synallagmatische oder auch konditionale Verknüpfung).

die Vertragserforderlichkeit im Falle einer konditionalen Verknüpfung jedenfalls im Wege der Analogie zu bejahen sein, sofern Nutzerpflichten dafür relevant sind. Dies führt in der Konsequenz zu einer engen Verzahnung des nationalen Vertragsrechts mit dem unionalen Datenschutzrecht. Diese Verbindung ist durchaus nicht untypisch, wie auch die DIDD-Richtlinie zeigt, die an diversen Stellen auf das nationale Vertragsrecht verweist, bisweilen gar als Voraussetzung für ihre eigene Anwendbarkeit.[609] Insgesamt hätte diese Konstruktion zur Folge, dass immer dann, wenn eine wirksame Pflicht des Nutzers zur Erteilung der Einwilligung oder der Überlassung von Daten (oder eine wirksame dahingehende Bedingung) ausdrücklich oder konkludent vereinbart wurde, der Schutz des Kopplungsverbots entfiele. Den Schutzmechanismen des allgemeinen Zivilrechts für die wirksame Inanspruchnahme von Privatautonomie käme dann noch größere Bedeutung zu.

β. Ablehnung aus teleologischer Perspektive

Diese Konsequenz zeigt jedoch zugleich, dass die Auffassung, wonach auch Nutzerpflichten (sowie durch den Nutzer zu erfüllende Bedingungen) für die Beurteilung der Vertragserforderlichkeit relevant sind, aus teleologischer Perspektive letztlich nicht überzeugen kann.[610] Nur vordergründig kann das Argument fruchten, dass der Betroffene bei Nichtberücksichtigung der Nutzerpflichten daran gehindert wäre, wirksam seine Einwilligung zu einer Verarbeitung zu erklären, zu deren Duldung er sich bereits vertraglich verpflichtet hat. Denn die Wirksamkeit einer Einwilligung wird regelmäßig eine Geschäftsgrundlage darstellen, wie später noch zu zeigen ist.[611] Zudem wäre bei Relevanz der Nutzerpflichten eine Verarbeitung bei unterstellter Wirksamkeit der Verpflichtung zur Datenüberlassung und Duldung der Verarbeitung bereits nach Art. 6 Abs. 1 lit. b DS-GVO zulässig, sodass eine Einwilligung aus datenschutzrechtlicher Perspektive schlicht obsolet wäre.[612]

Entscheidend dürfte jedoch sein: Da fast immer bei einem datenbasierten Grundmodell eine Pflicht des Nutzers zur Überlassung von Daten oder zur Erteilung einer Einwilligung (oder eine dahingehende Bedingung) konkludent anzunehmen ist, würde das Kopplungsverbot in diesem zentralen Bereich der digitalen Wirtschaft faktisch leerlaufen.[613] Dies jedoch würde die Zielsetzung des Kopplungsverbots fundamental konterkarieren: Denn das aus Sicht materiell verstandener Privatautonomie problematische Verhandlungs- und Macht-

[609] Art. 3 Abs. 10 und 48. Erwägungsgrund aE DIDD-Richtlinie.

[610] Ebenso im Ergebnis *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 9; *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2018, Art. 7 DS-GVO Rn. 41.1.

[611] Siehe unten, § 5 C.I.1.c)bb)(2)(a).

[612] Vgl. *Engeler*, ZD 2018, 55 (56); die gilt jedoch nicht, wenn auch für Art. 6 Abs. 1 lit. b DS-GVO die Nutzerpflichten irrelevant sind, siehe dazu unten, § 4 B.II.2.b)aa)(2).

[613] *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2018, Art. 7 DS-GVO Rn. 41.1.

ungleichgewicht[614] bleibt bestehen, vor allem, weil Pflichten (im Rahmen der AGB-Kontrolle) seitens der Verantwortlichen durch AGB einseitig statuiert werden können. Daher liegt es näher, das Kopplungsverbot bereits dann greifen zu lassen, wenn die Vertragserfüllung abhängig gemacht wird von der Verarbeitung personenbezogener Daten, die für die Erfüllung der Pflichten *des Verantwortlichen* nicht erforderlich sind, auch wenn sich die Verarbeitung als Erfüllung von Nutzerpflichten darstellen würde.

In systematischer Perspektive streitet dafür zudem in gewisser Weise die nähere Bestimmung der Vertragserfüllung als „einschließlich der Erbringung einer Dienstleistung" in Art. 7 Abs. 4 DS-GVO, was zumindest nahelegt, dass an die Erfüllung durch den Verantwortlichen, der typischerweise die Dienstleistung erbringt, gedacht wurde.

Schließlich legt die DIDD-Richtlinie in Art. 3 Abs. 1 UAbs. 2 fest, dass solche datenbasierten Gegenleistungen vom Anwendungsbereich der Richtlinie ausgenommen sind, bei denen personenbezogene Daten „durch den Unternehmer ausschließlich zur Bereitstellung digitaler Inhalte oder digitaler Dienstleistungen im Einklang mit [der DIDD-]Richtlinie" verarbeitet werden. Die Formulierung umfasst daher nur Daten, die für die Erfüllung der Pflichten des Verantwortlichen erforderlich sind.[615] Daraus lässt sich aber nicht ex negativo schließen, dass die allgemeinere Formulierung in Art. 7 Abs. 4 DS-GVO auch Nutzerpflichten umfassen müsse. Denn diese konkrete Formulierung der DIDD-Richtlinie war bei Erlass der DS-GVO noch nicht in der Diskussion. Für die Auslegung der DS-GVO, die ohnehin nach Art. 3 Abs. 8 UAbs. 2 DIDD-Richtlinie unberührt bleiben soll, lässt sich daher Art. 3 Abs. 1 UAbs. 2 der DIDD-Richtlinie nicht fruchtbar machen. Insgesamt kann daher die Erfüllung von Nutzerpflichten nicht als Vertragserfüllung im Sinne des Kopplungsverbots angesehen werden.

γ. Rekurs auf Verarbeiterpflichten

Ob beim datenbasierten Grundmodell die Verarbeitung für die Vertragserfüllung erforderlich ist, muss daher allein unter Rekurs auf die Pflichten des Verantwortlichen (Verarbeiterpflichten) bestimmt werden. Im Fall der Nutzung personenbezogener Daten für personalisierte Werbung bedeutet dies, dass bei Zugrundelegung des subjektiven Erforderlichkeitsmaßstabs die Verarbeitung nur dann vertragserforderlich ist, wenn eine Pflicht des Verantwortlichen zur

---

[614] Dazu eingehend *Starke*, EU-Grundrechte und Vertragsrecht, 2016, § 7.

[615] Die Beschränkung auf Verarbeiterpflichten war bei der DIDD-Richtlinie sachlich geboten, da eine Berücksichtigung von Nutzerpflichten zu einer weitgehenden Unanwendbarkeit der Richtlinie in gerade den Fällen geführt hätte, die sie erfassen sollte (z. B. Zugang zu einem sozialen Netzwerk, siehe 19. Erwägungsgrund DIDD-Richtlinie); siehe zu der Ausnahme auch *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.4.; *Spindler/Sein*, MMR 2019, 415 (418).

Schaltung personalisierter Werbung wirksam vereinbart wurde. Dies ist gegenwärtig, soweit ersichtlich, in den Nutzungsbedingungen regelmäßig nicht der Fall.[616] Daher ist die Überlassung von Daten und die Einwilligung zu diesem Zweck typischerweise für die Vertragserfüllung nicht erforderlich.[617] Sofern der Anbieter kein funktionsäquivalentes Angebot unter Verzicht auf eine Einwilligung und entsprechende Datenverarbeitung macht, ist auch die Abhängigkeit gegeben. Jedenfalls in Konstellationen, die von signifikanten Netzwerkeffekten geprägt sind, wie etwa bei sozialen Netzwerken,[618] ist damit in der Rechtsfolge die Unfreiwilligkeit nach dem Kopplungsverbot regelmäßig zu bejahen.[619] Auch die beschränkte Opt-Out-Möglichkeit (innerhalb der jeweiligen Seiten oder Apps) hinsichtlich einiger Typen der nicht vertragserforderlichen Datenverarbeitung ändert daran nichts.[620] Die Einwilligung ist daher insoweit unwirksam.

Dies stellt das Modell datenfinanzierter Dienste, wie erörtert, jedoch nicht grundsätzlich infrage. Denn den Unternehmen steht es frei, ihre Dienste zumindest auch gegen Bezahlung anzubieten, sodass die Abhängigkeit der Vertragserfüllung von der Einwilligung entfällt und das Kopplungsverbot kein Hindernis mehr für die Einwilligung darstellt. Eine derartige Wahlmöglichkeit zwischen der Bezahlung mit Daten und der Bezahlung mit Geld wäre ohnehin, wie im Folgenden noch zu erörtern sein wird,[621] für die Wahlfreiheit der Nutzer und deren materielle Ausübung von Privatautonomie sehr förderlich.

(bb) Rabattmodell

Anders stellt sich wiederum die Rechtslage beim Rabattmodell dar. Hier ist die Verarbeitung bestimmter personenbezogener Daten für die vertragliche Pflicht des Verantwortlichen, einen Rabatt zu gewähren, erforderlich. Hinsichtlich dieser Daten greift daher das Kopplungsverbot nicht ein. Darüberhinausgehende Verarbeitungen, etwa zu Zwecken personalisierter Werbung, die nicht Teil des vertraglich vereinbarten Rabatts sind, sind jedoch ebenso wie beim datenbasierten Grundmodell nach hier vertretener Auffassung (subjektiver Erforderlichkeitsmaßstab, Rekurs auf Verarbeiterpflichten) vom Kopplungsverbot umfasst.

---

616 Siehe die umfangreiche Recherche zum Inhalt von Nutzungsbedingungen führender Internetunternehmen in *Hacker*, ZfPW 2019, 148 (169 mit Fn. 146).

617 Ebenso im Ergebnis *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 Rn. 57; *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2018, Art. 7 DS-GVO Rn. 41.1; *Weidert/Klar*, BB 2017, 1858 (1860); *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8.10.2019, Rn. 52 f.; aA *Heinzke/Engel*, ZD 2020, 189 (193).

618 Siehe im Einzelnen dazu unten, § 6 C.II.4.a).

619 Im Ergebnis ebenso Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 645 f.; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 51; aA *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 Rn. 63.

620 Zutreffend Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 651 ff.

621 Siehe unten, § 6 C.II.

(cc) Data on top-Modell

Beim data on top-Modell hingegen steht typischerweise die monetäre Entlohnung als Gegenleistung im Vordergrund, sodass grundsätzlich keine konkludente Pflicht zur Überlassung von personenbezogenen Daten oder eine diesbezügliche Bedingung anzunehmen ist.[622] Daher entfällt das Problem, inwiefern Nutzerpflichten für die Vertragserfüllung relevant sein können. Bei Zugrundelegung eines subjektiven Erforderlichkeitsmaßstabs werden daher im Übrigen Datenverarbeitungen nach denselben Maßstäben wie beim datenbasierten Grundmodell vom Kopplungsverbot umfasst sein.[623]

(b) Datenerhebung durch Dritte (*tracking walls*)

Ganz ähnliche Ergebnisse liefert auch die Analyse der Datenerhebung durch Dritte. Wird etwa die Nutzung einer Seite von der Einwilligung in Datenverarbeitungen durch Drittanbieter-Tracking-Instrumente abhängig gemacht (*tracking walls*[624]), so wird darin regelmäßig ebenfalls ein Verstoß gegen das Kopplungsverbot liegen,[625] sofern keine entsprechenden Anbieterpflichten einschlägig sind oder ein funktionsäquivalenter Dienst auch ohne die Einwilligung angeboten wird. Dies steht allerdings unter der Prämisse, dass die Einwilligung in Tracking-Instrumente nach der DS-GVO zu beurteilen ist.[626]

(c) Datenerhebung bei Dritten

Im Rahmen der Datenerhebung bei Dritten, etwa durch IoT-Geräte, stellt sich das Problem des Kopplungsverbots regelmäßig nicht, da typischerweise eine Einwilligung gerade nicht Voraussetzung für die Drittnutzung eines IoT-Geräts ist. Dieses lässt sich vielmehr zumeist einfach durch Aktivierung (z. B. in Verbindung mit einem Sprachbefehl) verwenden. Ferner scheitert die Einwil-

---

[622] Siehe ausführlich *Hacker*, ZfPW 2019, 148 (164); ebenso *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.5. (keine schuldrechtliche Gegenleistung, wenn Datenüberlassung/Einwilligung für den Anbieter nur von untergeordneter Bedeutung sind, was z. B. bei *paid services* möglich sei).

[623] Siehe auch *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 10 (Weiterleitung an Dritte durch Bank zu Zwecken durch Bank); für die Einschlägigkeit des Kopplungsverbots bei bestimmten IoT-Daten nach Gerätekauf auch *Steege*, MMR 2019, 509 (511).

[624] Laut einer Studie mit einem Beobachtungszeitraum in 2018/19 nutzten 7 % der populärsten Webseiten der EU *tracking walls*, siehe *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (3); zu Begriff und Bedeutung auch *European Data Protection Supervisor*, EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), Opinion 6/2017, 2017, 17.

[625] So auch *Zuiderveen Borgesius et al.*, 3 European Data Protection Law Review 2017, 1 (9); *European Data Protection Supervisor*, EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), Opinion 6/2017, 2017, 17.

[626] Dazu unten, §4 B.I.4.b).

ligung, sofern sie denn eingeholt wird, häufig am Kriterium der Unmissverständlichkeit oder der Informiertheit.[627] Ist dies einmal nicht der Fall, so sind die Fälle analog zu denen des datenbasierten Grundmodells zu lösen, da bei der Datenerhebung bei Dritten typischerweise von diesen kein monetäres Entgelt entrichtet wird.

Durchaus denkbar ist dabei allerdings, dass jedenfalls gegenüber dem Primärnutzer eine vertragliche Verpflichtung des IoT-Anbieters besteht, das Produkt in gewissem Umfang in seiner Funktionsweise zu personalisieren. Sofern diese Verpflichtung wirksam eingegangen wurde, greift insofern das Kopplungsverbot nicht. Inwiefern eine solche Vertragsbindung gegenüber Drittnutzern etabliert werden kann, wird im weiteren Verlauf der Arbeit noch eingehend untersucht.[628]

(6) Zusammenfassung zur Freiwilligkeit

Das Kriterium der Freiwilligkeit der Einwilligung wird für den Bereich marktförmiger Austauschprozesse vor allem durch das Kopplungsverbot in Art. 7 Abs. 4 DS-GVO operationalisiert. Beide Tatbestandsmerkmale und auch die Rechtsfolge sind jedoch umstritten. Nach hiesiger Auffassung muss, erstens, im Rahmen der Vertragserforderlichkeit ein subjektiver Erforderlichkeitsmaßstab angelegt werden, der sich strikt nach den wirksam durch die Parteien vereinbarten Pflichten richtet. Allerdings können allein Verarbeiterpflichten, und nicht solche des Nutzers (etwa zur Überlassung personenbezogener Daten und zur Einwilligung in deren Verarbeitung) Vertragserforderlichkeit im Sinne der Vorschrift herstellen. Dies hat zur Folge, dass etwa hinsichtlich personenbezogener Daten, die für personalisierte Werbung genutzt werden, ohne dass dafür eine rechtliche Verpflichtung des Verantwortlichen bestünde, die Verarbeitung für die Vertragserfüllung nicht erforderlich ist.

Zweitens ist im Rahmen des Tatbestandsmerkmals der Abhängigkeit der Vertragserfüllung von der Einwilligung die jeweilige Marktmacht des Anbieters als ein gewichtiger Faktor zu berücksichtigen. Sie ist jedoch keine notwendige Bedingung für die Abhängigkeit. Bestehen keine funktional äquivalenten Alternativen am Markt, die ohne eine Verarbeitung der nicht vertragserforderlichen Daten die Dienstleistung oder das Produkt bereitstellen, so ist die Abhängigkeit jedenfalls erfüllt. Werden solche Alternativen nur von anderen Anbietern angeboten, so kann dennoch nach dem Wortlaut des Kopplungsverbots eine Abhängigkeit zu bejahen sein.

Drittens besteht bei Vorliegen der beiden Tatbestandsvoraussetzungen eine Vermutung zugunsten der Unfreiwilligkeit. Die Existenz von marktgängigen, einwilligungsfreien Alternativen ist jedoch im Rahmen der Rechtsfolge zu be-

[627] Vgl. *Steege*, MMR 2019, 509 (511).
[628] Siehe unten, § 5 B.III.2.b).

achten und kann entscheidend gegen die Unfreiwilligkeit sprechen. Damit geht einher, dass auch das Kriterium der Marktmacht, das typischerweise mit der Inexistenz derartiger Alternativen verknüpft ist, für die Rechtsfolge relevant ist. Bei nicht marktmächtigen Unternehmen, bei denen taugliche Alternativen durch andere Anbieter am Markt existieren, wird daher in der Regel die Unfreiwilligkeit auf Basis des Kopplungsverbots zu verneinen sein. Bei marktmächtigen Unternehmen hingegen, insbesondere beim Vorliegen signifikanter Netzwerkeffekte, wird etwa eine Einwilligung zur Verarbeitung von Daten für personalisierte Werbung, sofern keine dahingehende wirksame Verarbeiterpflicht besteht, typischerweise am Kopplungsverbot scheitern. Diesen Unternehmen steht es jedoch offen, das Kopplungsverbot bereits tatbestandsmäßig auszuschalten, indem sie durch monetäres Entgelt finanzierte vertragliche Alternativen vorhalten.

ee) Einwilligung und Genehmigungsmöglichkeit

Schließlich sei noch erwähnt, dass eine Einwilligung, damit sie ihren prospektiven Schutz vor den Risiken der Datenverarbeitung entfalten kann, nach ganz herrschender Meinung *vor* der Verarbeitung abgegeben werden muss: Dieses ungeschriebene Tatbestandsmerkmal ist danach auch dem unionalen, autonom zu bestimmenden Einwilligungsbegriff der DS-GVO inhärent.[629]

An der rigorosen Ablehnung der Möglichkeit einer nachträglichen Genehmigung der Datenverarbeitung mit der Folge von deren Rechtmäßigkeit bestehen jedoch mit Blick auf den Schutzzweck der Einwilligung erhebliche Zweifel.[630] Zwar ist in der Tat, wenn die Datenverarbeitung ohne Einwilligung (und Eingreifen einer sonstigen Rechtsgrundlage) stattgefunden hat, das Kind im sprichwörtlichen Sinne bereits in den Brunnen gefallen. Jedoch ist nicht ersichtlich, dass es den Grundsätzen des Datenschutzrechts oder auch dem Schutz des Datenschutzgrundrechts zuwiderliefe, wenn die betroffene Person im Nachhinein die Datenverarbeitung billigt. Insbesondere ist nicht erkennbar, dass die Risiken, die mit der Datenverarbeitung einhergehen, im Nachhinein schwerer einzuschätzen wären als vor Beginn der Datenverarbeitung; wenn überhaupt, dürfte das Gegenteil zutreffen. Die Möglichkeit einer Genehmigung hat damit im Prinzip keine Nachteile, die nicht auch die Einwilligung betreffen würden. Ihre Zubilligung würde jedoch zu einem signifikanten Gewinn an Gestaltungsfähigkeit durch die betroffene Person führen.

---

[629] *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 21; *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 2018, Art. 7 DS-GVO Rn. 85; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 30; *Ernst* in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 4 DS-GVO Rn. 64; vgl. auch EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 102; GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (*Fashion ID*) – Rn. 132, 140.

[630] Siehe auch *Riesenhuber*, RdA 2011, 257 (259).

Allerdings kann eine Genehmigung nur dann die Rechtmäßigkeit der Datenverarbeitung bewirken, wenn die Voraussetzungen vorliegen, die, wäre die Datenverarbeitung noch nicht erfolgt, zu einer wirksamen Einwilligung geführt hätten. Auch aus der Perspektive des Schutzes der betroffenen Person erscheint es daher unproblematisch, ihr ein Genehmigungsrecht zuzubilligen, wenn bereits vor der Datenverarbeitung die Voraussetzungen für eine wirksame Einwilligung erfüllt waren, die Erklärung jedoch erst nach der Datenverarbeitung abgegeben wurde. Fraglich ist allein, ob es ausreichen kann, dass die Pflichtinformationen, unter Verstoß gegen Art. 13 Abs. 1 DS-GVO, erst nach der Datenverarbeitung, aber vor der Abgabe der Genehmigung, zur Verfügung gestellt werden. Hier dürfte jedoch die Sanktion der Verletzung von Art. 13 Abs. 1 DS-GVO ausreichen; für die Wirksamkeit einer Genehmigung kommt es nach hier vertretener Auffassung nur darauf an, dass die Informationen vor der Abgabe der Erklärung erteilt werden, sodass die Genehmigung in informierter Weise erfolgen kann.

Aufgrund des abschließenden Charakters von Art. 6 Abs. 1 DS-GVO muss die Genehmigung jedoch letztlich als besondere Ausprägung der Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO betrachtet werden. Da die dogmatische Unterscheidung von Einwilligung und Genehmigung aus §§ 183 f. BGB jedenfalls hinsichtlich der Begrifflichkeit auf das Unionsrecht nicht übertragen werden muss und Art. 4 Nr. 11 DS-GVO nicht explizit die Abgabe der Einwilligung vor Beginn der Datenverarbeitung fordert, ist der unionsrechtliche Einwilligungsbegriff für eine derartige Extension offen. Als Folge dürfte dann allerdings eine rechtfertigende, nicht eine tatbestandsausschließende Wirkung anzunehmen sein.[631]

b) Besondere Voraussetzungen, Art. 7–9 DS-GVO

Zu diesen allgemeinen Voraussetzungen der Einwilligung gesellen sich einige besondere Voraussetzungen für spezifische Kontexte der Einholung oder der Verarbeitung, die in den Art. 7–9 DS-GVO verortet sind.

aa) Separierungsgebot, Art. 7 Abs. 2 S. 1 DS-GVO

Zunächst beinhaltet Art. 7 Abs. 2 S. 1 DS-GVO eine besondere Voraussetzung für schriftliche Einwilligungserklärungen, die mit Erklärungen zu anderen Sachverhalten (etwa anderen Vertragsklauseln[632]) verbunden werden. Danach muss „das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist." Entscheidend ist mithin, dass

631 *Riesenhuber*, RdA 2011, 257 (259); für die urheberrechtliche Einwilligung auch BGH GRUR 2010, 628 Rn. 33 – Vorschaubilder I.

632 *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 Rn. 76.

die Einwilligung von den anderen Sachverhalten klar abgetrennt wird. Insofern muss man eher von einem Separierungsgebot als einem Hervorhebungsgebot (so noch § 4a Abs. 1 S. 4 BDSG) sprechen.[633] Die Anforderungen an die Verständlichkeit ergeben sich parallel auch aus Art. 12 DS-GVO. Letztlich dient das Separierungsgebot der Informiertheit der Einwilligung, indem ein versehentliches Übersehen der Einwilligung durch die betroffene Person unwahrscheinlicher gemacht wird.[634] Allerdings wurde bereits gezeigt, dass das Kriterium der Unmissverständlichkeit ohnehin ein eigenständiges Absonderungsgebot beinhaltet, neben dem das Separierungsgebot keine entscheidende Relevanz mehr hat.[635] In faktischer Hinsicht kommt es ohnehin nur zum Tragen, wenn der Vertragstext inklusive der Einwilligung überhaupt gelesen wird – was selten der Fall sein wird.

bb) Widerruf, Art. 7 Abs. 3 DS-GVO

Deutlich bedeutsamer, insbesondere auch in seinen Beziehungen zum allgemeinen Zivilrecht, ist das in Art. 7 Abs. 3 S. 1 DS-GVO verankerte jederzeitige Widerrufsrecht des Einwilligenden. Damit soll dem Einzelnen ermöglicht werden, sein Recht auf informationelle Selbstbestimmung auch in jenen Fällen effektiv auszuüben, in denen er erst nach der Einwilligung erkennt, dass der (erwartete) Nutzen der Einwilligung geringer ist als ihre (erwarteten) Kosten bzw. Nachteile.[636]

(1) Datenschutzrechtliche Rechtsfolgen

Rechtsfolge des Widerrufs, der nach Art. 7 Abs. 3 S. 4 DS-GVO ebenso einfach zu erteilen sein muss wie die Einwilligung, ist in datenschutzrechtlicher Hinsicht, dass die Datenverarbeitung auf Grundlage der Einwilligung ex nunc unwirksam wird, Art. 7 Abs. 3 S. 2 DS-GVO. Umstritten ist jedoch, inwiefern der Verantwortliche nach dem Widerruf auf andere Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO zurückgreifen kann.

Gesichert dürfte einzig sein, dass dies insoweit möglich ist, als der Verarbeiter die betroffene Person bei Einholung der Einwilligung darauf hingewiesen hat, dass die Datenverarbeitung parallel auf andere Erlaubnistatbestände gestützt werden kann.[637] Dies ist ohne Weiteres möglich, da Art. 6 Abs. 1 DS-GVO davon spricht, dass für die Rechtmäßigkeit der Datenverarbeitung „mindestens" einer

[633] Vgl. *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 Rn. 77: Unterscheidbarkeitsgebot; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 24: Transparenzgebot.

[634] *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 Rn. 75.

[635] Siehe oben, § 4 B.I.3.a)aa)(1)(a)(bb).

[636] Vgl. *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 34.

[637] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-

der Erlaubnistatbestände vorliegen muss. Eine Kumulation ist demnach schon dem Wortlaut zufolge ausdrücklich vorgesehen und angesichts der erheblichen Rechtsunsicherheit bei den einzelnen Tatbeständen auch gerechtfertigt.[638]

Problematisch hingegen ist, inwiefern ein Rückgriff auf andere Tatbestände möglich ist, wenn der Verantwortliche keinen derartigen Hinweis bei Einholung der Einwilligung gegeben hat. An sich stehen zwar die übrigen Erlaubnistatbestände gleichrangig neben der Einwilligung.[639] Allerdings sieht eine starke Literaturmeinung in dem Rückgriff auf andere Tatbestände in dieser Konstellation einen Verstoß gegen den Grundsatz von Treu und Glauben.[640] Denn der betroffenen Person wird zunächst suggeriert, durch die Einwilligung über die Datenverarbeitung bestimmen zu können. Erteilte sie diese nicht oder widerruft sie diese, wird diese Erwartung enttäuscht, wenn die Verarbeitung auf andere Tatbestände gestützt wird.

Nach hier vertretener Auffassung muss jedoch genügen, wenn der Verantwortliche den Hinweis, dass die Datenverarbeitung nunmehr auf andere Tatbestände gestützt wird, zum Zeitpunkt des Widerrufs bzw. der Ablehnung der Einwilligung erteilt.[641] Denn ein früherer Hinweis hätte an den möglichen Handlungsoptionen der betroffenen Person nichts geändert. Dies muss zumal dann gelten, wenn die betroffene Person initial vertraglich versprochen hatte, Daten zur Verfügung zu stellen, was im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO entscheidend für ein Überwiegen des Verarbeiterinteresses sprechen kann.[642] Auch Art. 17 Abs. 1 lit. b DS-GVO geht klar davon aus, dass nach dem Wider-

GVO Rn. 18; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO Rn. 89 f.

[638] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 17; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 34; *Krusche*, ZD 2020, 232 (233 f.).

[639] *Engeler*, ZD 2018, 55 (56); *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 34; *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Anhang 3 zu Artikel 6: Datenverarbeitung für Zwecke der Werbung Rn. 10; *Tavanti*, RDV 2016, 231 (234); aA *Sattler*, JZ 2017, 1036 (1039).

[640] *DSK*, Kurzpapier Nr. 20 – Einwilligung nach der DS-GVO, 2019, 3; *Uecker*, ZD 2019, 248 (249); *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 18; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO Rn. 89; *Wolff*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 475.

[641] So auch *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 27; *Krusche*, ZD 2020, 232 (234 f.); im Ergebnis auch *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 34; *Albers/Veit*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2019, Art. 6 DS-GVO Rn. 27; ähnlich *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2019, Art. 7 DS-GVO Rn. 91.1.; *Tavanti*, RDV 2016, 231 (238).

[642] Zwar kann der Widerruf zugleich als Widerspruch i. S. d. Art. 21 Abs. 1 S. 1 DS-GVO gedeutet werden, *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO Rn. 89. Allerdings können in der Erfüllung der initial zugesagten Vertragsordnung zwingende Gründe i. S. d. Art. 21 Abs. 1 S. 2 DS-GVO liegen; dazu unten, Text bei § 4, Fn. 656 und § 4 C.I.2.c)bb)(2).

ruf andere Rechtsgrundlagen eingreifen können, ohne dies mit einer initialen Hinweispflicht zu verbinden.[643]

Lediglich die heimliche Fortführung der Datenverarbeitung auf anderer Grundlage verstößt in der Tat gegen die Grundsätze von Treu und Glauben und der Transparenz, weil die betroffene Person dann über die weitere Analysemöglichkeit (als juristischer Laie) im Irrtum ist. Dieser Irrtum kann aber erhebliche Auswirkungen auf das Verhalten der betroffenen Person (etwa die Nutzung von Verschlüsselung oder anderen Werkzeugen, welche die Analyse erschweren) haben. Allerdings darf nicht verkannt werden, dass ein derartiger Hinweis ohnehin nach Art. 13 Abs. 1 lit. c DS-GVO bei Wechsel der Rechtsgrundlage geschuldet ist.[644] Der zusätzliche Verstoß gegen die Grundsätze ist daher lediglich für die Höhe eines etwaigen Bußgeldes relevant (vgl. Art. 83 Abs. 2 lit. a, Abs. 5 lit. a DS-GVO).

(2) Vertraglicher Ausschluss oder Erschwernis des Widerrufs?

Das Widerrufsrecht des Betroffenen hinsichtlich der Einwilligung ist nach dem Wortlaut des Art. 7 Abs. 3 DS-GVO keinerlei Einschränkungen unterworfen. Dies verleiht Verträgen, bei denen die Datenverarbeitung auf eine Einwilligung gestützt wird, eine inhärente Unsicherheit hinsichtlich der zukünftigen Möglichkeit des Leistungsaustauschs. Daher werden in der Literatur verschiedene Instrumente diskutiert, um einen Widerruf der Einwilligung zeitweise auszuschließen oder ihm die datenschutzrechtlich vorgesehene Rechtsfolge zu nehmen.[645] So postulieren Teile der datenschutzrechtlichen Literatur Grenzen des freien Widerrufs, die je nach Kontext und vertraglichem Bedürfnis bestehen sollen.[646] Darüber hinaus wird in der Literatur vertreten, dass zumindest (für eine bestimmte Zeit) eine unwiderrufliche schuldrechtliche Gestattung (z. T. als „schuldvertragliche“[647] oder „schuldrechtliche Einwilligung“[648] bezeichnet) möglich sein sollte.[649]

---

[643] *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 34; *Tavanti*, RDV 2016, 231 (238 mit Fn. 63).

[644] *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 27.

[645] Zu Grenzen des Widerrufs nach der Rechtslage vor Geltung der DS-GVO siehe *Langhanke*, Daten als Leistung, 2018, 116 f.; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 270.

[646] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 38 f. (bei Verträgen: mangelnde Zumutbarkeit für den Betroffenen oder Änderunge wesentlicher Umstände); ähnlich *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 57; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 92 (Beschränkung durch vertragliche Vereinbarung); siehe grundsätzlich zur Beschränkung des Widerrufs einer Einwilligung *Ohly*, „Volenti non fit iniuria“ – Die Einwilligung im Privatrecht, 2002, 348 ff.

[647] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 232, 253; kritisch *Riesenhuber*, RdA 2011, 257 (258).

[648] *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 44.

De lege lata muss diesen Einschränkungen jedoch nach hiesiger Auffassung klar entgegengetreten werden: Das Widerrufsrecht ist nicht beschränkbar.[650] Ganz parallel gilt dies auch für den Ausschluss des Widerspruchs nach Art. 21 Abs. 1 S. 1 DS-GVO hinsichtlich der Verarbeitung basierend auf Art. 6 Abs. 1 lit. e und f DS-GVO. Dies folgt zunächst aus dem klaren und eindeutigen Wortlaut der DS-GVO („jederzeit", Art. 7 Abs. 3 S. 1, Art. 21 Abs. 1 S. 1). Auch der 42. Erwägungsgrund der DS-GVO verbürgt die Möglichkeit, die Einwilligung „zurückzuziehen, ohne Nachteile zu erleiden".[651] Hinzu kommt zweitens, dass auch in teleologischer Hinsicht die grundrechtlich durch Art. 8 GRCh verbürgte informationelle Selbstbestimmung für ein unbeschränktes Widerrufsrecht spricht. Denn die Ausführungen zum Marktversagen haben ergeben, dass typischerweise die Voraussetzungen für eine informierte, präferenzkonforme Erteilung der Einwilligung aufgrund rationaler Ignoranz und verhaltensökonomischer Effekte gerade nicht vorliegen.[652] Dann ist es jedoch umso wichtiger für Betroffene, im Nachhinein eine etwaig unvorteilhafte Entscheidung, die zu einer nicht präferenzkonformen Einwilligung geführt hat, korrigieren zu können.[653] Drittens ist zu beachten, dass das Datenschutzgrundrecht zwar nicht schrankenlos gewährleistet wird,[654] entgegenstehenden Interessen der Verantwortlichen sowie von Dritten jedoch hinreichend auf anderem Wege Rechnung getragen werden kann. Wie soeben gesehen, kann der Verarbeiter auch nach dem Widerruf der Einwilligung richtigerweise auf andere Erlaubnistatbestände ausweichen. Insofern kann eine Weiterverarbeitung insbesondere nach Art. 6 Abs. 1 lit. f DS-GVO zulässig sein.[655] Dafür sind zwar, sofern der Widerruf zugleich als Widerspruch im Sinne von Art. 21 Abs. 1 S. 1 DS-GVO

[649] Dafür zuletzt eingehend *Sattler*, JZ 2017, 1036 (1043 ff.), unter Rückgriff auf *Ohly*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, 2002, 143 ff.; ebenso bereits *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 36, 136; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 253 ff.; siehe auch *Langhanke*, Daten als Leistung, 2018, 148 ff.

[650] So auch *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.4.; *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (91); *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (220 f.); *Schmidt-Kessel/Erler/Grimm/Kramme*, GPR 2016, 54 (60); *de Franceschi*, in: Schmidt-Kessel/Kramme (Hrsg.), Geschäftsmodelle in der digitalen Welt, 2017, 113 (134); *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2019, Art. 7 DS-GVO Rn. 89; *Tavanti*, RDV 2016, 231 (238 mit Fn. 61); *Hacker*, ZfPW 2019, 148 (170); zur Rechtslage vor Geltung der DS-GVO *Langhanke*, Daten als Leistung, 2018, 118.

[651] Gleiches Argument bei *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.4 mit Fn. 39.

[652] Siehe oben, § 3 B.II.1.a)-b).

[653] Vgl. *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 16; Dieses Korrekturbedürfnis untermauert auch die Literatur zu *exploitative contracts*, dazu ausführlich *Hacker*, in: Faust/Schäfer (Hrsg.), Zivilrechtliche und rechtsökonomische Probleme des Internet und der künstlichen Intelligenz, 2019, 97.

[654] Dies betont in diesem Kontext *Specht*, JZ 2017, 763 (769), die allerdings Art. 6 Abs. 1 lit. f DS-GVO außer Acht lässt.

[655] Siehe dazu im Einzelnen unten, § 4 C.I.2.c)bb)(2).

gewertet wird,[656] nach Art. 21 Abs. 1 S. 2 DS-GVO zwingende schutzwürdige Gründe erforderlich. Hierbei wird man jedoch den Umstand, dass der Betroffene sich zur Einwilligung in die Datenverarbeitung verpflichtet hatte, zugunsten des Verantwortlichen berücksichtigen können.

Dieser Rückgriff auf zwingende schutzwürdige Gründe erlaubt eine gemessen am Datenschutzgrundrecht chartakonforme und systematisch im Rahmen der DS-GVO schlüssige partielle Aufrechterhaltung des gegenseitigen Leistungsaustauschs unter den Voraussetzungen eines Widerrufs der Einwilligung. Dies geht auch nicht notwendig mit einer größeren Rechtsunsicherheit als die Datenverarbeitung auf Grundlage der Einwilligung einher, wie die vielfältigen Grenzen der Einwilligung zeigen.[657] Die Überwindbarkeit des Widerspruchs belegt im Übrigen *ex negativo*, dass eine Einschränkung der Folgen des Widerrufs der Einwilligung auch bei entsprechenden Interessen des Verantwortlichen in systematischer Hinsicht gerade nicht anerkannt werden kann. Die Lösung über Art. 6 Abs. 1 lit. f DS-GVO versagt lediglich bei einem Widerspruch gegen die Direktwerbung nach Art. 21 Abs. 2, 3 DS-GVO[658] und bei sensitiven Daten im Sinne von Art. 9 DS-GVO, was angesichts der klaren Regelungsanordnung hinsichtlich des Schutzbedürfnisses dieser Daten jedoch hinzunehmen ist.

Schließlich ist viertens in systematischer Perspektive weiter zu bemerken, dass die Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO abschließend sind und daher keine zur Einwilligung funktionsäquivalente rechtsgeschäftliche Konstruktion, wie etwa eine schuldrechtliche Gestattung, die Erlaubniswirkung hinsichtlich der Datenverarbeitung herbeiführen kann. Diesen abschließenden Charakter hat der EuGH schon zu der Vorgängervorschrift, Art. 7 DSRL, in der Rechtssache *ASNEF* betont.[659] Den Mitgliedstaaten ist es, in den Worten des EuGH, verwehrt, „zusätzliche Bedingungen [zu] stellen, die die Tragweite eines der sechs in [Art. 7 Abs. 1 DSRL] vorgesehenen Grundsätze verändern würden."[660] Genau eine solche qualitative Veränderung würde sich jedoch durch die Möglichkeit des vertraglichen Ausschlusses des Widerrufsrechts oder funktional äquivalente rechtsgeschäftliche Konstruktionen, die eine freie Widerruflichkeit garantieren, ergeben. Denn infolge der Gefahr eines Marktversagens hinsichtlich der Erteilung der Einwilligung ist die Widerrufsmöglichkeit für das unionsrechtliche System der Einwilligung essenziell.

Die genannten Argumente zeigen ferner, dass auch *de lege ferenda* die Anerkennung der Beschränkung des Widerrufsrechts nicht notwendig erscheint. Denn die Möglichkeit eines Ausweichens auf Art. 6 Abs. 1 lit. b und f DS-GVO genügt, um den Interessen der Anbieter Rechnung zu tragen. Dies gilt ins-

656 Siehe dazu oben, § 4, Fn. 642.
657 *Veil*, NJW 2018, 3337 (3343).
658 Zu diesem Widerspruchsrecht *Tavanti*, RDV 2016, 295 (302).
659 Urt. v. 24.11.2011 – verb. Rs. C-468/10 und C-469/10 (*ASNEF*) – Rn. 30 f.
660 Urt. v. 24.11.2011 – verb. Rs. C-468/10 und C-469/10 (*ASNEF*) – Rn. 32.

besondere auch für den Widerruf zur Unzeit, bei dem regelmäßig Art. 6 Abs. 1 lit. f DS-GVO einschlägig sein wird.[661] Zusätzlich können diese sich dadurch absichern, dass sie, wie dies in der Praxis auch typisch ist, die Datenschuldner in Vorleistung treten lassen.[662] Mit diesen Instrumenten kann sich der Anbieter gegen eine opportunistische Verwendung des Widerrufs schützen. Dies zeigt weiterhin, dass auch eine schuldrechtliche Pflicht zur Wiedererteilung der Einwilligung nach erfolgtem Widerruf selbst dann nicht anzuerkennen ist, wenn die Erteilung der Einwilligung schuldrechtlich vereinbart war.[663] Wie sogleich im Einzelnen zu zeigen sein wird, ist eine derartige Verpflichtung nach dem Widerruf jedenfalls nicht mehr durchsetzbar.[664]

Letztlich ähneln Verträge, bei denen Daten als Gegenleistung verwendet werden, daher Verträgen mit einseitigem, jederzeitigem Kündigungsrecht (z. B. § 605 Nr. 1 BGB), sofern die Datenverarbeitung lediglich auf Art. 6 Abs. 1 lit. a (Widerrufsmöglichkeit), lit. e oder lit. f (Widerspruchsmöglichkeit) DS-GVO gestützt wird.[665]

(3) Vertragsrechtliche Folgen des Widerrufs

Sofern die betroffene Person ihre Einwilligung wirksam widerruft bei einem Vertrag, hinsichtlich dessen Daten als Gegenleistung fungieren, stellt sich die Frage nach den in der DS-GVO nicht geregelten vertragsrechtlichen Konsequenzen des Widerrufs: einem Schadensersatzanspruch und einem Vertragslösungsrecht des Verantwortlichen. Auch in der DIDD-Richtlinie sind diese Fragen, schon ausweislich ihres 40. Erwägungsgrunds, nicht geregelt. Schadensersatzansprüche werden dort gar nicht mehr angesprochen,[666] Vertragsbeendigungsrechte lediglich zugunsten des Verbrauchers in Art. 13 Abs. 1 und 2, Art. 14 Abs. 4 und 6 und Art. 16 Abs. 2. Für die Beantwortung dieser Fragen muss daher auf das allgemeine Vertragsrecht des BGB zurückgegriffen werden.[667]

(a) Schadensersatz des Verantwortlichen

Im Fall von Daten als Gegenleistung stellt sich zunächst die Frage, inwiefern der datenschutzrechtlich Verantwortliche möglicherweise einen Schadensersatzanspruch gegen die betroffene Person geltend machen kann. Dies mag etwa relevant sein, wenn der Verarbeiter einen Gewinn aus einem anvisierten

661 Dies erwägen auch *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (104 Fn. 97).
662 Dazu *Sattler*, JZ 2017, 1036 (1041); *Hacker*, ZfPW 2019, 148 (180).
663 *Spindler*, DB 2016, 937 (940).
664 Siehe unten, Text bei § 4, Fn. 689.
665 Vgl. *Langhanke*, Daten als Leistung, 2018, 119; *Hacker*, ZfPW 2019, 148 (170).
666 Dies war im Kommissionsentwurf noch anders, siehe eingehend *Graf von Westphalen*, BB 2016, 1411.
667 Siehe nochmals den 40. Erwägungsgrund der DIDD-Richtlinie; ferner *Metzger*, AcP 216 (2016), 817 (852).

Datenverkauf nicht realisieren konnte oder die Daten nicht mehr gewinnbringend für personenbezogene Werbung nutzen kann. Es sei unterstellt, dass die betroffene Person in diese Verarbeitungen zunächst wirksam eingewilligt hatte, bevor sie ihre Einwilligung widerrief. Dabei ist zunächst danach zu unterscheiden, worauf sich der Anspruch des Verantwortlichen gegen die betroffene Person überhaupt bezog. Bei der Nutzung von Daten als Gegenleistung existieren potenziell zwei unterschiedliche Verpflichtungen, die alternativ oder auch kumulativ eine Gegenleistung darstellen können:[668] einerseits ein Anspruch auf die Überlassung von personenbezogenen Daten (inklusive der Duldung von deren Erhebung durch den Verantwortlichen, etwa mithilfe von Cookies) und andererseits ein Anspruch auf die Erteilung einer wirksamen Einwilligung.[669]

Der BGH hat bereits zu erkennen gegeben, dass seiner Auffassung nach wohl beide Varianten grundsätzlich eine Gegenleistung im schuldrechtlichen Sinne darstellen können.[670] *En passant* hat auch der EuGH, ebenso wie das LG Berlin,[671] jedenfalls die Überlassung personenbezogener Daten als Gegenleistung für Onlinedienste (konkret: die Nutzung der Funktionen des Facebook Like Buttons durch Betreiber von Webseiten, die dieses Social Plug-In einbinden) qualifiziert.[672] Als dritte Möglichkeit ist ferner denkbar, dass in Einzelfällen zusätzlich eine Pflicht zur Duldung der Werbeexposition besteht.[673] Sofern man diesen dritten Weg beschreitet, können die schadensersatzrechtlichen Fragen analog zu den beiden anderen Optionen gelöst werden, die daher im Folgenden im Zentrum stehen.

---

668 Siehe auch noch unten, § 5 B.I.

669 *Hacker*, ZfPW 2019, 148 (159) m. w. N.; *Specht*, JZ 2017, 763 (764); vgl. auch schon *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012, 119 f.; siehe auch bereits oben, § 3 B.I.2.

670 BGH NJW 2017, 2119 Rn. 22 – Robinson Liste; vgl. auch LG Berlin MMR 2018, 328 Rn. 51; BT-Drucks. 17/13951, 72; aA hinsichtlich der Datenüberlassung KG BeckRS 2019, 8570 Rn. 43; allerdings düfte auch nach der dort gegebenen Begründung die Datenüberlassung eine Gegenleistung darstellen, wenn sich die betroffene Person zur Überlassung schuldrechtlich verpflichtet.

671 LG Berlin BeckRS 2018, 1060, Rn. 51: bei einem Vertrag mit Facebook besteht „eine[] ‚Gegenleistung' in Form der Datenübertragung"; siehe auch *Hacker*, ZfPW 2019, 148 (163).

672 EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 80.

673 Siehe *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.5. unter Verweis auf ein noch unveröffentlichtes Manuskript von *Riehm*; siehe auch zu einem „Recht, den Betroffenen zu bewerben" bereits *Patzak/Beyerlein*, MMR 2007, 687 (688); dazu kritisch *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012, 119 ff. Dazu ist anzumerken, dass personenbezogene Daten, die auch bei lediglich einmaligem Kontakt zwischen Anbieter und Nutzer überlassen werden, auf ganz verschiedene Arten monetarisiert werden können (siehe oben, § 3 A.II.1.b)), von denen personalisierte Werbung nur eine Form darstellt. Auch bei einem zunächst einmaligen Austausch können diese Daten z. B. für A/B Testing oder zur Personalisierung des Produkts und damit zur Erhöhung der Wahrscheinlichkeit der erneuten Nutzung des Angebots durch den Nutzer verwendet werden (siehe *Hacker*, ZfPW 2019, 148 [152]). Daher dürfte selbst in Fällen, in denen primär eine Werbeexposition bezweckt ist, zumindest auch in der Überlassung der Daten (und ggf. der Einwilligung) eine eigenständige Gegenleistung erblickt werden können.

Daher ist primär das genaue Objekt der Gegenleistung jeweils durch Auslegung im Einzelfall zu ermitteln:[674] Datenüberlassung (aa) oder (auch) Abgabe der Einwilligung (bb). Sodann muss sekundär nach der Art der potentiellen Pflichtverletzung unterschieden werden: Nichtüberlassung von Daten; Überlassung von inkorrekten Daten; Nichtabgabe bzw. Widerruf der Einwilligung. Tertiär schließlich ist die Frage der Rechtmäßigkeit der Datenverarbeitung nach Widerruf der Einwilligungserklärung zu berücksichtigen.

(aa) Anspruch auf Datenüberlassung

Ergibt die Vertragsauslegung, dass es sich bei der Gegenleistung um einen Anspruch auf die Überlassung von personenbezogenen Daten handelt, so kann eine Pflichtverletzung entweder in der Nichtüberlassung von Daten (α) oder in der Überlassung inkorrekter Daten liegen (β). Dies ist auch rechtspolitisch nicht zu beanstanden (γ).

α. Nichtüberlassung von Daten

Ist die Überlassung von Daten geschuldet, so wird die Nichtüberlassung regelmäßig eine Pflichtverletzung darstellen. Ob diese jedoch einen Schadensersatzanspruch auslöst, hängt nach hier vertretener Ansicht entscheidend davon ab, ob der Verantwortliche die Möglichkeit hätte, die Daten, würden sie denn weiterhin überlassen werden, trotz Widerrufs der Einwilligung rechtmäßig zu verarbeiten.

(α) Möglichkeit der rechtmäßigen Verarbeitung weiterer Daten
Wird zugleich mit der Nichtüberlassung die Einwilligung widerrufen, so kann der Verantwortliche die Verarbeitung nicht mehr auf Art. 6 Abs. 1 lit. a DS-GVO stützen. Allerdings ist denkbar, dass andere, gesetzliche Erlaubnistatbestände von Art. 6 Abs. 1 DS-GVO einschlägig sind. Die Zulässigkeit der Datenverarbeitung ist dann vom Widerruf der Einwilligung unabhängig.[675] In diesem Fall können durchaus die Voraussetzungen für einen Schadensersatzanspruch neben oder auch statt der Leistung vorliegen.

– Verpflichtung zur Datenüberlassung

Allerdings ist gerade auch in Anbetracht des Schutzes der personenbezogenen Daten durch das Datenschutzgrundrecht jeweils genau zu prüfen, ob tatsächlich eine wirksame *Verpflichtung* zur Überlassung von Daten eingegangen wurde. Wie bereits erwähnt, ist dies nach hier vertretener Auffassung nur dann der Fall, wenn eine dahingehende Verpflichtung ausdrücklich in den Vertrag aufgenommen wurde.[676] Bei Stillschweigen hinsichtlich einer derartigen

[674] So auch *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.5.
[675] Siehe oben, § 4 B.I.3.b)bb)(1).
[676] Siehe oben, Text bei § 4, Fn. 607 ff.

Verpflichtung ist vielmehr von einer Bedingung der Leistungserbringung des Anbieters durch die Datenüberlassung auszugehen, sodass kein durchsetzbarer Anspruch des Anbieters auf eine datenbasierte Gegenleistung und in der Folge insoweit auch (mit Ausnahme der Regelung in § 160 Abs. 2 BGB[677]) kein Anspruch auf Schadensersatz besteht.

– Durchsetzbarer Anspruch

Können die Daten auch nach einer *anderen* Rechtsgrundlage als auf Grundlage einer Einwilligung verarbeitet werden (Art. 6 Abs. 1 lit. b oder f DS-GVO, ggf. i. V. m. Art. 21 Abs. 1 S. 2 DS-GVO), so steht einem durchsetzbaren Anspruch insoweit nichts entgegen.[678] Insbesondere spricht allein der Umstand, dass personenbezogene Daten durch das Datenschutzgrundrecht geschützt sind, nicht dagegen, ihre Überlassung zum Gegenstand eines kommerziellen Vertrags zu machen.[679] Dies zeigt in aller Deutlichkeit auch die Kommerzialisierung des Urheberpersönlichkeitsrechts[680] und des allgemeinen Persönlichkeitsrechts.[681]

– Pflichtverletzung und sonstige Voraussetzungen

Wenn ein echter Anspruch des Verantwortlichen auf Datenüberlassung bejaht wird, so kann dieser, wenn nicht nur eine (etwaige) Einwilligung widerrufen, sondern auch die Überlassung der Daten eingestellt wird, nach erfolglosem Fristablauf nach Maßgabe von §§ 280 Abs. 1, Abs. 3, 281 BGB Schadensersatz statt der Leistung gerichtet auf das positive Interesse geltend machen; daneben kann gem. §§ 280 Abs. 1, Abs. 2, 286 BGB der Verzögerungsschaden er-

677 Dazu *Hacker*, ZfPW 2019, 148 (179).

678 *Hacker*, ZfPW 2019, 148 (170); vgl. aber *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (103); *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (221); *Langhanke*, Daten als Leistung, 2018, 126, die eine Naturalobligation ins Spiel bringen; dagegen treffend *Sattler*, JZ 2017, 1036 (1040); ferner für eine Undurchsetzbarkeit des Anspruchs auf Erteilung der Einwilligung pauschal *Schmidt-Kessel/Erler/Grimm/Kramme*, GPR 2016, 54 (60); *Langhanke*, Daten als Leistung, 2018, 138; in Analogie zu § 120 Abs. 3 FamFG auch *Specht*, JZ 2017, 763 (767); für die Wertung von § 888 Abs. 3 ZPO *Langhanke*, Daten als Leistung, 2018, 128 f. Diese Beiträge setzen jedoch implizit voraus, dass eine Einwilligung einzig möglicher Erlaubnisgrund für die Verarbeitung ist.

679 *Metzger*, AcP 216 (2016), 817; *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 43; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 200; vgl. auch *Langhanke*, Daten als Leistung, 2018, 99, 110 ff.; *Metzger et al.*, 9 JIPITEC 2018, 90 Rn. 19; *Metzger*, in: Festschrift Basedow, 2018, 131 (133); *Indenhuck/Britz*, BB 2019, 1091 (1095); *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen); aA *European Data Protection Supervisor*, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 2017, 9 f.; wohl auch *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8.10.2019, Rn. 54.

680 Dazu etwa *Metzger*, Rechtsgeschäfte über das Droit moral im deutschen und französischen Urheberrecht, 2002, insbesondere 105 ff., 165 ff.; *Unseld*, GRUR 2011, 982 (986).

681 BGH NJW 2000, 2195 – Marlene Dietrich; *Unseld*, GRUR 2011, 982 (984 ff.); *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 42 f.

setzt werden.[682] Die Pflichtverletzung liegt dann jedoch, wie gesehen, nicht im (ohnehin immer rechtmäßigen) Widerruf der Einwilligung,[683] sondern in der Nichtüberlassung von vertraglich geschuldeten Daten.

(β) Keine Möglichkeit der rechtmäßigen Verarbeitung weiterer Daten

Anders hingegen ist die Konstellation zu beurteilen, wenn infolge des Widerrufs der Einwilligung eine rechtmäßige Verarbeitung personenbezogener Daten nicht mehr zulässig ist. Dies ist dann der Fall, wenn entweder außer Art. 6 Abs. 1 lit. a DS-GVO keine anderen Rechtsgrundlagen in Betracht kommen oder aber eine Datenverarbeitung lediglich auf Art. 6 Abs. 1 lit. f DS-GVO gestützt werden könnte, in dem Widerruf der Einwilligung jedoch zugleich ein wirksamer Widerspruch nach Art. 21 Abs. 1 S. 1 oder Art. 21 Abs. 2 DS-GVO erblickt werden muss,[684] der nicht nach Art. 21 Abs. 1 S. 2 DS-GVO überwunden werden kann. In diesen Fällen muss danach differenziert werden, ob die Nichtüberlassung der Daten vor oder nach Widerruf der Einwilligung erfolgte.

– Nichtüberlassung nach Widerruf der Einwilligung

Sofern nach Maßgabe des soeben Gesagten die nicht überlassenen Daten ohnehin nicht hätten rechtmäßig verarbeitet werden können, besteht nach dem Widerruf der Einwilligung kein durchsetzbarer Anspruch auf Überlassung dieser Daten mehr. Vielmehr hätte die betroffene Person, würde der Verantwortliche doch an die Daten gelangen, einen Anspruch auf Löschung aus Art. 17 Abs. 1 lit. d DS-GVO und gegebenenfalls auf Herausgabe der Daten nach Art. 20 Abs. 1 DS-GVO. Damit steht dem Anspruch auf Überlassung der Daten die *dolo agit*-Einrede entgegen.[685] Es wäre treuwidrig vom Verantwortlichen, eine Überlassung von Daten zu fordern, die unmittelbar gelöscht bzw. zurückgegeben werden müssten.[686] In dem Widerruf der Einwilligung wird man regelmäßig auch eine konkludente Erhebung dieser Einrede

[682] *Metzger*, AcP 216 (2016), 817 (852 f.); für eine Begrenzung auf das negative Interesse hingegen *Langhanke*, Daten als Leistung, 2018, 138; angesichts der Durchsetzbarkeit des Anspruchs des Anbieters (Text bei § 4, Fn. 678 und 687) besteht dafür jedoch nach hier vertretener Auffassung kein Grund.

[683] Siehe Text bei und Nachweise in § 4, Fn. 726.

[684] Zu dieser Möglichkeit *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO Rn. 89; siehe auch unten, Text bei § 4, Fn. 1004.

[685] Siehe *Langhanke*, Daten als Leistung, 2018, 127; *Hacker*, ZfPW 2019, 148 (161); *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen); zur Anwendbarkeit von § 242 BGB genauer unten, § 5 C.II.3.b)bb). Zudem kann die betroffene Person nach Art. 17 DS-GVO die Unterlassung der rechtswidrigen Datenverarbeitung verlangen (LG Frankfurt a. M. ZD 2019, 410 Rn. 30 ff.), siehe dazu unten, § 5 C.III.4.

[686] Zur Erfassung gesetzlicher Rückgewähransprüche durch die *dolo agit*-Einrede *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 462. Zwar stellen Löschung und Übertragung nach der DS-GVO keine Rückgewähr im klassischen Sinne dar, was jedoch aufgrund der digitalen Natur der Daten (Nicht-Rivalität) ohnehin regelmäßig ausscheidet. Aber sie

erblicken können. Mangels durchsetzbaren Anspruchs scheidet ein Schadensersatzanspruch wegen Nichtüberlassung der Daten *nach* Widerruf der Einwilligung daher aus.

– Nichtüberlassung vor Widerruf der Einwilligung

Vor dem Widerruf der Einwilligung hingegen ist der Anspruch auf Datenüberlassung nach hier vertretener Auffassung durchaus durchsetzbar, auch wenn die Verarbeitung lediglich auf eine Einwilligung gestützt werden kann.[687] Die betroffene Person kann gegen diesen Anspruch zwar infolge der Widerrufsmöglichkeit jederzeit die *dolo agit*-Einrede erheben.[688] Die bloße Existenz dieser Möglichkeit jedoch hindert die Durchsetzbarkeit so lange nicht, als die Einrede nicht tatsächlich erhoben wird.[689] Sonst müsste man bei anderen Ansprüchen, die auf einem zumindest durch eine Seite jederzeit kündbaren Rechtsverhältnis aufruhen (z. B. bei der Leihe, vgl. § 605 Nr. 1 BGB,[690] oder bei während des Laufs der Widerrufsfrist widerruflichen Verbraucherverträgen[691]), ebenso von einer mangelnden Durchsetzbarkeit ausgehen, was jedoch, soweit ersichtlich, nirgends vertreten wird.[692] Es würde auch der gesetzlichen Systematik, wonach gerade Verbraucherverträge mit Widerrufsrecht, das bekanntlich über ein Jahr lang bestehen kann,[693] grundsätzlich entgeltliche Verträge darstellen (vgl. § 312 Abs. 1 BGB), diametral zuwider laufen.

Dieses Ergebnis deckt sich auch damit, dass Einreden materielle Wirksamkeit grundsätzlich nur entfalten, wenn sie wirksam erhoben werden.[694] Wird daher die Datenüberlassung *vor* dem Widerruf der Einwilligung eingestellt, und sieht man in der Nichtüberlassung bei Auslegung entsprechend §§ 133, 157 BGB nicht zugleich einen konkludenten Widerruf der Einwilligung, so hätte die Verarbeitung der nicht überlassenen Daten auf Art. 6 Abs. 1 lit. a DS-GVO gestützt werden können. Die Voraussetzungen eines Schadensersatzanspruchs sind dann typischerweise, ebenso wie im gerade behandelten Fall der Rechtmäßigkeit der Verarbeitung wegen Einschlägigkeit einer anderen Rechtsgrundlage als der Einwilligung, gegeben.

---

berauben das Leistungsinteresse des Gläubigers ebenso wie ein klassischer Rückgewähranspruch der Legitimität: Seine Durchsetzung verhilft dem Gläubiger zu keinem schützenswerten Vorteil, bedingt aber eine Belastung des Datenschuldners (vgl. wiederum *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 462).

687 So auch *Metzger*, AcP 216 (2016), 817 (834 f.); *Hacker*, ZfPW 2019, 148 (170); vgl. auch *Langhanke*, Daten als Leistung, 2018, 119, 127 f.

688 Siehe oben, § 4, Fn. 685.

689 *Hacker*, ZfPW 2019, 148 (170).

690 Dieses Beispiel verdanke ich Herrn Professor *Sebastian Lohsse*.

691 Siehe *Langhanke*, Daten als Leistung, 2018, 119 Fn. 154.

692 Vgl. *Häublein*, in: MüKo, BGB, 7. Aufl. 2016, § 598 Rn. 1 f.

693 Siehe z. B. § 356 Abs. 3 S. 2 BGB.

694 Siehe *H. Roth*, Die Einrede des bürgerlichen Rechts, 1988, 169; *Emmerich*, in: MüKo, BGB, 8. Aufl. 2019, § 320 Rn. 46.

(γ) Keine Reformnotwendigkeit de lege ferenda

Der Verantwortliche hat mithin im Fall der Nichtüberlassung von Daten insoweit keinen Anspruch auf Schadensersatz, als eine Weiterverarbeitung nach dem Widerruf der Einwilligung unrechtmäßig wäre. Es besteht jedoch auch in rechtspolitischer Hinsicht kein Bedürfnis, dies zu ändern. Denn die Möglichkeit des Widerrufs der Einwilligung ist dem Verantwortlichen regelmäßig bekannt, der sich daher, wie gesehen,[695] durch zusätzliche vertragliche Abreden, etwa eine Vorleistungspflicht der betroffenen Person, schützen kann. Vor allem aber lässt sich ein fortbestehendes, erhebliches Interesse des Verantwortlichen an der Verarbeitung weiterer Daten, und die Existenz signifikanter Schäden bei deren Unterbleiben, unproblematisch im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO berücksichtigen, wie bei der Analyse der Interessenabwägungsklausel noch im Einzelnen zu zeigen ist.[696] Insbesondere kann hier auch die vertragliche Vereinbarung, dass die betroffene Person über einen längeren Zeitraum hinweg zuverlässig Daten überlassen soll, Relevanz gewinnen.

Wäre die Datenverarbeitung aber rechtmäßig, so besteht nach dem soeben Gesagten auch ein Schadensersatzanspruch, wenn die Überlassung von Daten unterbleibt. Auf diesem Wege können die Interessen und legitimen Erwartungen des Verantwortlichen daher bereits *de lege lata* in hinreichender Weise berücksichtigt werden.

β. Überlassung von inkorrekten Daten

Denkbar ist ferner, dass die betroffene Person die Überlassung von geschuldeten Daten zwar nicht vollständig einstellt, jedoch inkorrekte Daten liefert. Sofern korrekte Daten geschuldet sind, ist wiederum ein Anspruch auf Schadensersatz statt der Leistung gem. §§ 280 Abs. 1, Abs. 3, 281 BGB sowie ein Anspruch auf Schadensersatz neben der Leistung gem. §§ 280 Abs. 1, Abs. 2, 286 BGB denkbar.[697] Auch hier wird man jedoch zunächst unterscheiden müssen, ob diese inkorrekten Daten vor oder nach dem Widerruf der Einwilligung bereitgestellt wurden.

(α) Überlassung inkorrekter Daten vor Widerruf der Einwilligung

Zunächst ist es möglich, dass bereits vor dem Widerruf der Einwilligung inkorrekte Daten durch die betroffene Person geliefert werden. Hier lässt sich etwa das Beispiel konstruieren, wonach ein aufgrund der Einwilligung daten-

[695] Siehe bereits oben, Text bei § 4, Fn. 661 f.

[696] Siehe unten, § 4 C.I.2.c)bb)(2).

[697] Siehe allgemein (§§ 280 ff. BGB) *Langhanke*, Daten als Leistung, 2018, 142 f.; vgl. aber auch *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (104), die den Schadensersatzanspruch bei fehlerhaften Daten auf §§ 280 Abs. 1, 241 Abs. 2 BGB stützen wollen. Da jedoch, wenn eine Verpflichtung zur Überlassung von korrekten Daten besteht, diese das Erfüllungsinteresse betrifft, dürften §§ 280 Abs. 1, 3, 281 Abs. 1 BGB bzw. §§ 280 Abs. 1, Abs. 2, 286 BGB die richtigen Anspruchsgrundlagen darstellen.

schutzrechtlich zulässiger Verkauf der Daten an Dritte abredegemäß bereits vor dem Widerruf vollzogen wurde, die betroffene Person jedoch einen falschen Namen angegeben hatte, sodass die Daten für den Dritten wertlos waren und dieser beim Verkäufer, dem Vertragspartner der betroffenen Person, nunmehr Regress nimmt.

In der Übermittlung inhaltlich fehlerhafter Daten wird man regelmäßig keinen konkludenten Widerruf der Einwilligung erblicken können,[698] da die mangelnde Korrektheit für den Verantwortlichen zum Zeitpunkt der Übermittlung typischerweise gar nicht erkennbar ist. Der Widerruf der Einwilligung muss angesichts der damit verbundenen erheblichen Rechtsfolgen jedoch für den Verantwortlichen klar zum Ausdruck kommen.[699] Hinsichtlich der einzelnen Voraussetzungen des Schadensersatzanspruchs ergeben sich allerdings einige Besonderheiten wegen der datenschutzrechtlichen Implikationen.

– Anspruch auf Überlassung korrekter Daten

Zunächst stellt sich die Frage, ob überhaupt *korrekte* Daten geschuldet werden, was wiederum eine Frage der Vertragsauslegung ist. Zwar finden sich in Nutzungsbedingungen von Anbietern digitaler Leistungen teilweise dahingehende Formulierungen;[700] diese müssen jedoch auch wirksam vereinbart werden.[701] So wurde die Klarnamenpflicht etwa vom LG Berlin als nicht mit der AGB-Kontrolle vereinbar angesehen;[702] eine obergerichtliche Klärung steht jedoch noch aus.[703] Ferner muss im Einzelfall untersucht werden, ob die Pflicht zur Überlassung korrekter Daten auf Registrierungsdaten bzw. explizit genannte Datentypen beschränkt ist[704] oder sie sich auf alle überlassenen Daten, mithin auch solche der Verhaltensbeobachtung durch Tracking-Technologien, erstreckt. Jedenfalls grundsätzlich wird auch hier gelten, dass eine genuine Verpflichtung zur Überlassung korrekter Daten, und nicht lediglich eine dahingehende Bedingung, nur bei ausdrücklicher Vereinbarung angenommen werden kann.[705]

---

[698] Anders, einen konkludenten Widerruf annehmend, tendenziell *Metzger*, AcP 216 (2016), 817 (850).

[699] Vgl. *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 88.

[700] Siehe die Beispiele bei *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.5.

[701] *Metzger*, AcP 216 (2016), 817 (850).

[702] LG Berlin MMR 2018, 328 Rn. 62–64 (zu § 4a BDSG aF); zustimmend, auch unter Berücksichtigung der DS-GVO, *Hacker*, ZfPW 2019, 148 (189 f.); ablehnend *Konrad*, K&R 2018, 275 (276); für eine AGB-Widrigkeit bzw. die Möglichkeit pseudonymer Nutzung auch, aus der Literatur vor der Entscheidung des LG Berlin, *Hullen/Roggenkamp*, in: Plath, DS-GVO/BDSG, 3. Aufl. 2018, § 13 TMG Rn. 42; *Heckmann* in: Heckmann, juris PraxisKommentar Internetrecht, 4. Aufl. 2014, Kap. 9 Rn. 486; *Schnabel/Freund*, CR 2010, 718 (720).

[703] Die Berufung wurde insoweit zurückgenommen, siehe KG MMR 2020, 239 Rn. 48.

[704] So *Metzger*, AcP 216 (2016), 817 (850).

[705] So auch *Metzger*, AcP 216 (2016), 817 (850).

Ist die Pflicht zur Überlassung korrekter Daten nicht auf bestimmte Datentypen beschränkt, so erfasst sie, wie im Ergebnis bereits *Metzger* herausgearbeitet hat,[706] bei Auslegung gemäß §§ 133, 157 BGB lediglich aktiv durch den Nutzer übermittelte Daten (z. B. Registrierungsdaten). Hinsichtlich solcher Daten hingegen, die der Anbieter selbst erhebt (z. B. durch Tracking), muss er, wie in § 6 noch ausführlich diskutiert wird,[707] den Einsatz von Instrumenten des Selbstdatenschutzes (z. B. Verschleierung der IP-Adresse durch Tor-Browser; Standortdaten-Blocker; *obfuscation*[708]) schon wegen der zwingenden Pflicht zum Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gem. Art. 25 DS-GVO grundsätzlich tolerieren.[709]

Eine solche Tolerierungspflicht muss hingegen abgelehnt werden, wenn die Überlassung der fraglichen Tracking-Daten wirksamer Inhalt einer Bedingung oder einer synallagmatischen Gegenleistungspflicht ist. Der Einsatz von Verschleierungsstrategien steht dann, aus der Perspektive des Anbieters, einer Nichtüberlassung von Daten gleich. Der Nutzer kann jedoch nicht erwarten, gewissermaßen kostenlos bzw. bei einseitiger Preisreduzierung in den Genuss der Leistung zu gelangen. Der Anbieter dürfte die Leistungserbringung daher grundsätzlich nach § 158 BGB oder § 320 Abs. 1 S. 1 BGB (teilweise) verweigern. Allerdings wird regelmäßig keine rechtswidrige Pflichtverletzung vorliegen (dazu sogleich).

– Durchsetzbarkeit des Anspruchs

Vor dem Widerruf der Einwilligung ist in Übertragung des soeben zum Anspruch auf Datenüberlassung Gesagten[710] auch der Anspruch auf die Korrektheit der Daten durchsetzbar, sofern die *dolo agit*-Einrede noch nicht erhoben wurde.

– Eingeschränkte Pflichtverletzung durch Überlassung inkorrekter Daten

Sofern nach der Vertragsauslegung korrekte Daten geschuldet sind, stellt die Überlassung inkorrekter Daten grundsätzlich eine Pflichtverletzung dar (vgl. § 243 Abs. 2 BGB).[711] Hier ist jedoch zwischen aktiv überlassenen Daten und vom Anbieter (oder Dritten) erhobenen Tracking-Daten zu unterscheiden. Grenzfälle konstituieren Daten, die zwar aktiv vom Nutzer übermittelt wer-

---

706 *Metzger*, AcP 216 (2016), 817 (850).

707 Siehe unten, § 6 B.I.2.

708 Siehe etwa *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (409, 422).

709 *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 63; siehe auch *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 172; *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Einleitung Rn. 246; aA, sogar mit Blick auf sensible Daten, *Langhanke*, Daten als Leistung, 2018, 142 f.

710 Siehe oben, § 4, Fn. 687.

711 *Metzger*, AcP 216 (2016), 817 (852 f.).

den, aber einen starken Bezug zur Persönlichkeitsentfaltung aufweisen. So wird man diesbezügliche Verschleierungsstrategien, z. B. die Setzung von bewusst falschen Likes zur Verschleierung der tatsächlichen Interessengebiete, im Zweifel angesichts des Rechts auf informationelle Selbstbestimmung (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG) und des Rechts auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG), die zumindest im Wege mittelbarer Drittwirkung die Frage der Vertragsauslegung beeinflussen,[712] als rechtmäßig, und nicht als Pflichtverletzung, werten müssen. Allerdings ist hier jeweils eine Analyse im Einzelfall vorzunehmen, die auch die (wirksamen) Nutzungsbedingungen, legitimen Erwartungen und Interessen der jeweiligen Anbieter einbezieht. Dabei muss jedoch ebenfalls berücksichtigt werden, dass diejenigen, die derartige Instrumente des Selbstdatenschutzes einsetzen, für personalisierte Werbung ohnehin in der Regel wenig empfänglich sind und daher dem Anbieter aus der fehlerhaften Information, infolge der bei diesen Personen ohnehin niedrigen Werbekonversionsrate, jedenfalls insoweit kaum marginale Kosten entstehen dürften. Anders liegt es wiederum, wenn wie im oben gebildeten Beispiel ein echter Datenverkauf in Rede steht, der jedoch selbst wiederum datenschutzrechtlich zulässig sein muss, um überhaupt als schützenswertes Interesse des Anbieters anerkannt zu werden. Letztlich bleibt dieser Grenzbereich jedoch, trotz dieser allgemeinen Richtlinien, von erheblicher Rechtsunsicherheit gekennzeichnet.

Der Einsatz von Verschleierungsmaßnahmen hinsichtlich nicht aktiv durch den Nutzer überlassener Daten (Tracking-Daten) kann jedoch nach hier vertretener Auffassung schon grundsätzlich keine rechtswidrige Pflichtverletzung darstellen. Andernfalls wäre letztlich in jedem präferenzinkonformen getrackten Verhalten eine Pflichtverletzung zu erblicken, da auch insofern inkorrekte Daten zur Verfügung gestellt würden. Der daraus resultierende Konformitätszwang ist jedoch in Anbetracht des Rechts auf informationelle Selbstbestimmung (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG) und des Rechts auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) kein sachgerechtes Ergebnis. Die Rechtswidrigkeit der Pflichtverletzung entfällt daher regelmäßig. Aus diesem Grund dürfte die Korrektheit von Tracking-Daten, sollte sie einmal ausdrücklich im Vertrag festgehalten werden, bei Vorliegen von AGB ohnehin regelmäßig bereits als unangemessen im Sinne von § 307 BGB zu klassifizieren sein.[713]

– Keine Berufung auf rechtmäßiges Alternativverhalten

Sofern demnach eine Pflichtverletzung bejaht werden kann, wird man der betroffenen Person allerdings den Einwand rechtmäßigen Alternativverhaltens

[712] Zur mittelbaren Drittwirkung des Rechts auf informationelle Selbstbestimmung siehe unten, Text bei und Nachweise in § 5, Fn. 1076.

[713] Vgl. auch *Schnabel/Freund*, CR 2010, 718 (720); *Hacker*, ZfPW 2019, 148 (189); zur AGB-Kontrolle der Einwilligung und Nutzungsbedingungen noch ausführlich unten, § 5 C.II.1.

verwehren müssen.[714] Dessen Anerkennung ist ohnehin immer von wertender Betrachtung gekennzeichnet.[715] Zwar könnte die betroffene Person in Anschlag bringen, dass sie hypothetisch durch einen (immerhin nach Art. 7 Abs. 3 DS-GVO möglichen) Widerruf *vor* der Verarbeitung diese hätte unrechtmäßig werden lassen[716] und dadurch z. B. den Datenverkauf hätte verhindern können.

Dies hieße jedoch in der Konsequenz, dass der Verantwortliche in diesen Situationen keinerlei Handhabe hätte, auf einer korrekten Datenüberlassung zu bestehen, da angesichts der unbeschränkten Widerrufsmöglichkeit immer der Einwand rechtmäßigen Alternativverhaltens im Raum stünde. Dies scheint aber insbesondere dann unangemessen, wenn die Überlassung korrekter Daten ohnehin, wie hier angenommen, nur dann geschuldet ist, wenn sie auch ausdrücklich und wirksam[717] im Vertrag vereinbart wurde. Eine diesbezügliche vertragliche Verpflichtung schließt daher richtigerweise bei wertender Betrachtung auch gem. §§ 133, 157 BGB den Einwand rechtmäßigen Alternativverhaltens aus.

– Schaden

Der Schadensersatzanspruch im Falle der Überlassung inkorrekter Daten erfasst jedenfalls solche Schäden, die entstehen, weil eine rechtmäßige Verarbeitung vor dem Widerruf bereits stattgefunden und infolge mangelnder Korrektheit der Daten zu Einbußen geführt hat. Etwaige Schäden wegen des verminderten ökonomischen Werts weiterer Verarbeitungen der inkorrekten Daten *nach* Widerruf der Einwilligung müssen hingegen unberücksichtigt bleiben, wenn und soweit die Verarbeitung infolge des Widerrufs nunmehr unrechtmäßig wäre – auch wenn die Daten selbst bereits vor dem Widerruf der Einwilligung überlassen wurden. Denn dann hätte der Verantwortliche auch im Falle der korrekten Überlassung daraus keinen rechtmäßigen Vorteil mehr ziehen können; ein Gewinn aus verbotener Tätigkeit bleibt jedoch im Rahmen von § 252 BGB unberücksichtigt.[718]

Insgesamt kann daher unter diesen Voraussetzungen, und mit den geschilderten Einschränkungen, ein Schadensersatzanspruch im Fall der vor dem Widerruf inkorrekt überlassenen Daten bejaht werden.[719]

---

[714] Dazu *Oetker*, in: MüKo, BGB, 8. Aufl. 2019, § 249 Rn. 217 ff.

[715] *Oetker*, in: MüKo, BGB, 8. Aufl. 2019, § 249 Rn. 221.

[716] Dies gilt wiederum nur unter der Prämisse, dass kein gesetzlicher Erlaubnistatbestand einschlägig ist.

[717] Zu Grenzen der Privatautonomie in diesem Kontext allgemein unten, § 5 C.I.-II.; zur Unwirksamkeit konkret der AGB-mäßigen Klarnamenpflicht bereits oben, § 4, Fn. 702.

[718] Siehe nur BGH NJW 1974, 1374 (1376); BGH NJW 1976, 1883 (1884); *Oetker*, in: MüKo, BGB, 8. Aufl. 2019, § 252 Rn. 7.

[719] Grundsätzlich auch für einen Schadensersatzanspruch bei inkorrekter Datenüberlassung *Metzger*, AcP 216 (2016), 817 (853); *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (104).

(β) Überlassung inkorrekter Daten nach Widerruf der Einwilligung
Werden hingegen *nach* dem Widerruf der Einwilligung noch inkorrekte Daten überlassen, so ist hinsichtlich der Voraussetzungen für einen Schadensersatzanspruch wiederum danach zu differenzieren, ob eine Möglichkeit zur rechtmäßigen Verarbeitung dieser Daten besteht.

– Keine Möglichkeit zur rechtmäßigen Verarbeitung der Daten

Sofern der Verantwortliche nach dem Widerruf der Einwilligung keine Möglichkeit zur rechtmäßigen Verarbeitung der Daten mehr hat, besteht, wie gesehen, infolge der regelmäßig mit dem Widerruf konkludent erhobenen *dolo agit*-Einrede kein durchsetzbarer Anspruch auf die Überlassung von Daten überhaupt und daher *a fortiori* nicht auf die Überlassung von korrekten Daten. Bereits daran scheitert ein Schadensersatzanspruch des Anbieters.

– Möglichkeit zur rechtmäßigen Verarbeitung der Daten

Besteht hingegen für den Verantwortlichen die Möglichkeit, nach dem Widerruf überlassene Daten rechtmäßig zu verarbeiten (z. B. auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO), so ist der Anspruch auf die Überlassung korrekter Daten weiterhin durchsetzbar. Denn eine *dolo agit*-Einrede scheidet dann gerade aus.

Allenfalls lässt sich fragen, ob die Möglichkeit des Schadensersatzes die betroffene Person von der Wahrnehmung ihres unionsrechtlich garantierten Rechts auf Widerruf der Einwilligung abhalten könnte, was wiederum den Effektivitätsgrundsatz des Unionsrechts verletzen könnte.[720] Allerdings ist dies aus zwei Gründen abzulehnen. Erstens kann die betroffene Person ihr Recht auf Widerruf weiterhin ausüben und dieses entfaltet auch seine volle datenschutzrechtliche Wirkung unabhängig davon, ob wegen des davon zu trennenden Tatbestands der Überlassung inkorrekter Daten Schadensersatz geschuldet ist oder nicht. Zweitens bewirkt der Widerruf der Einwilligung jedenfalls keine Verschlechterung der Lage der betroffenen Person, was allein eine abschreckende Wirkung entfalten könnte. Vielmehr ist vor dem Widerruf die Überlassung korrekter Daten genauso geschuldet wie nach dem Widerruf, nur mit dem für die betroffene Person tendenziell vorteilhaften Unterschied, dass die Erlaubniswirkung der Einwilligung entfällt. Daher sind eine Abschreckungswirkung und damit auch eine Verletzung des Effektivitätsgrundsatzes nicht ersichtlich.

Sofern die Überlassung inkorrekter Daten daher nach dem oben Erläuterten eine Pflichtverletzung darstellt, etwa bei aktiv falschen Registrierungsdaten, besteht also, bei Vorliegen der übrigen Voraussetzungen, ein Schadensersatzanspruch des Anbieters.

---

[720] EuGH, Urt. v. 17.4.2008 – Rs. C-404/06 (*Quelle*) – Rn. 34 f.; EuGH, Urt. v. 23.5.2019 – Rs. C-52/18 (*Fülla*) – Rn. 40.

(bb) Anspruch auf Einwilligung

Damit bleibt noch der Fall zu untersuchen, in dem (auch) ein Anspruch auf Abgabe einer Einwilligungserklärung besteht. Hier kann fraglich sein, ob überhaupt ein Anspruch besteht (α), ob dieser durchsetzbar ist (β) und worin schließlich eine Pflichtverletzung liegen könnte (γ–δ).

α. Bestehen des Anspruchs

Ob überhaupt ein Anspruch auf Abgabe einer Einwilligungserklärung besteht, entscheidet die Vertragsauslegung. Einerseits kann dieser Anspruch ausdrücklich vereinbart werden, was jedoch gegenwärtig in der Vertragspraxis kaum vorkommt.[721] Andererseits wird man jedenfalls dann, wenn die Überlassung von personenbezogenen Daten geschuldet (und nicht lediglich Bedingung) ist, ein anderer Erlaubnistatbestand als Art. 6 Abs. 1 lit. a DS-GVO jedoch nicht in Betracht kommt, bei Auslegung des Vertragsinhalts nach §§ 133, 157 BGB auch einen Anspruch auf Abgabe einer entsprechenden Einwilligung annehmen müssen, selbst wenn dieser nicht ausdrücklich vorgesehen ist. Der Anspruch auf Abgabe der Einwilligung ist dann ein rechtslogisch erforderlicher Annex zum Anspruch auf Datenüberlassung: Ohne jenen wäre dieser nichts wert.

β. Durchsetzbarkeit des Anspruchs

Der Anspruch ist jedoch von vornherein durch die Möglichkeit des jederzeitigen Widerrufs der Einwilligung beschränkt.[722] Er ähnelt damit, wie gesehen,[723] einem Anspruch aus einem Rechtsverhältnis, welches eine Partei jederzeit grundlos kündigen kann. Dies stellt jedoch die Durchsetzbarkeit des Anspruchs nicht an sich infrage. Denkbar ist zum Beispiel, dass der Anspruch auf Abgabe der Einwilligungserklärung gegen eine betroffene Person durchgesetzt wird, die zwar gegen die geschuldete Abgabe der Einwilligung nichts einzuwenden und daher auch keine Widerrufsintention hat, die Einwilligung aber bislang schlichtweg vergessen oder aus Bequemlichkeit unterlassen hat.

Es ist, entgegen manchen Bekundungen im Schrifttum,[724] nicht ersichtlich, warum der Verantwortliche seinen Anspruch auf Abgabe der Einwilligungserklärung in diesem Fall nicht auch gerichtlich durchsetzen können sollte, um der betroffenen Person „auf die Sprünge zu helfen“ und notfalls die Einwilligung durch die Fiktion des § 894 ZPO[725] zu ersetzen. Da die betroffene Person den Anspruch jederzeit durch Erhebung der *dolo agit*-Einrede bzw. durch (antizipierten) Widerruf der Einwilligung zu Fall bringen kann, werden ihre

721 Siehe *Hacker*, ZfPW 2019, 148 (169).
722 *Metzger*, AcP 216 (2016), 817 (850).
723 Siehe oben, Text bei § 4, Fn. 665.
724 Siehe die Nachweise in § 4, Fn. 678.
725 Zur Anwendbarkeit von § 894 ZPO auf geschäftsähnliche Handlungen (wie die Einwilligung), siehe *Gruber*, in: MüKo, ZPO, 5. Aufl. 2016, § 894 Rn. 3.

Interessen inklusive ihres Datenschutzgrundrechts hinreichend gewahrt. Wer jedoch diese einfachen Möglichkeiten zur Rechtsverteidigung nicht nutzt, aber die Abgabe einer Einwilligungserklärung wirksam versprochen hatte, muss auch damit rechnen, dass diese Abgabe letztlich durch ein Gerichtsurteil durchgesetzt wird.

γ. Keine Pflichtverletzung durch Widerruf der Einwilligung

Allerdings kann die Ausübung des in Art. 7 Abs. 3 DS-GVO unentziehbar verbürgten Rechts auf Widerruf nicht als rechtswidrige Pflichtverletzung gewertet werden kann.[726] Gleiches gilt für die schon initial nicht abgegebene Einwilligung. Da diese unmittelbar widerrufen werden könnte, stellt die Unterlassung der Abgabe keine Pflichtverletzung dar – auch wenn die Abgabe, wie soeben gesehen, eingeklagt werden kann. Ferner lässt sich einem Schadensersatzanspruch unter dem Gesichtspunkt des Schutzzwecks der Norm entgegenhalten, dass der Verarbeiter angesichts der jederzeitigen Widerrufbarkeit ohnehin keine schutzwürdige Erwartung dahingehend haben durfte, auch zukünftig mit den Daten auf Grundlage der Einwilligung zu verfahren.[727] Insofern ist ein Schadensersatzanspruch für diesen Fall klar abzulehnen.

δ. Pflichtverletzung durch Nichtüberlassung von Daten oder Überlassung inkorrekter Daten

Auch wenn die Abgabe einer Einwilligungserklärung geschuldet ist, kann eine Pflichtverletzung daher letztlich nur in der Nichtüberlassung von Daten oder der Überlassung inkorrekter Daten erblickt werden.[728] Die Existenz eines Schadensersatzanspruchs beurteilt sich dann nach den soeben dargestellten Maßstäben.

(cc) Zusammenfassung zum Schadensersatzanspruch bei Widerruf der Einwilligung

Insgesamt lässt sich damit festhalten, dass hinsichtlich eines möglichen Schadensersatzanspruchs nach unterschiedlichen Arten von Gegenleistung und verschiedenen Formen der Pflichtverletzung zu differenzieren ist. Der Anspruch auf Abgabe einer Einwilligungserklärung ist für einen Schadensersatzanspruch letztlich irrelevant, da weder in der Nichtabgabe noch in dem Wi-

[726] Ebenso *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (222); im Ergebnis ebenso *de Franceschi*, in: Schmidt-Kessel/Kramme (Hrsg.), Geschäftsmodelle in der digitalen Welt, 2017, 113 (136); wohl auch *Metzger*, AcP 216 (2016), 817 (855 mit Fn. 164); dies erwägend auch *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (103); *Langhanke*, Daten als Leistung, 2018, 138; ähnlich *Specht*, JZ 2017, 763 (767) (Verschuldensausschluss).

[727] *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (98).

[728] Zur Möglichkeit der mangelnden Exposition gegenüber einer Werbung als Pflichtverletzung siehe die Nachweise oben, in § 4, Fn. 673.

derruf der Einwilligung eine rechtswidrige Pflichtverletzung erblickt werden kann.

Durch Auslegung ist ferner regelmäßig zu ermitteln, ob ein Anspruch auf Überlassung von Daten oder gar auf Überlassung von korrekten Daten vereinbart wurde. Ist dies der Fall, so stellt die Nichtüberlassung regelmäßig eine Pflichtverletzung dar. Hinsichtlich der Überlassung fehlerhafter Daten gilt dies jedoch grundsätzlich nur für aktiv überlassene Daten, während Maßnahmen des Selbstdatenschutzes gegen Tracking-Technologien von der Pflicht zur Überlassung korrekter Daten nicht erfasst werden.

Schließlich ist danach zu unterscheiden, ob die vom Anbieter begehrte Datenverarbeitung, deren Unterlassung zu einem Schaden geführt hat, überhaupt in Anbetracht des Widerrufs der Einwilligungserklärung rechtmäßig gewesen wäre. Ist dies nicht der Fall, so steht die *dolo agit*-Einrede der Durchsetzbarkeit des jeweiligen Primäranspruchs und damit auch einem Schadensersatzanspruch entgegen. Wäre die Datenverarbeitung hingegen rechtmäßig, weil sie auf eine andere Rechtsgrundlage gestützt werden kann, so besteht grundsätzlich ein Schadensersatzanspruch. Dass die Anbieter diesen aus Reputationsgründen wohl häufig nicht durchsetzen werden,[729] steht freilich auf einem anderen Blatt.

(b) Zurückbehaltungs- und Vertragslösungsrecht des Verantwortlichen

Neben einem Schadensersatzanspruch kommen ferner ein Zurückbehaltungs- und ein Vertragslösungsrecht des Verantwortlichen in Betracht.[730] Dessen Notwendigkeit und die Erfüllung seiner Voraussetzungen hängen primär davon ab, ob eine synallagmatische oder eine konditionale Verknüpfung vorliegt.

(aa) Synallagmatische Verknüpfung

Sofern die Leistungen von Verantwortlichen und betroffener Person synallagmatisch verknüpft sind, kommen bei Nichtleistung der betroffenen Person ein Zurückbehaltungsrecht nach § 320 Abs. 1 S. 1 BGB (α) sowie ein Rücktrittsrecht nach § 323 BGB, aber auch Kündigungsrechte und ein Wegfall der Geschäftsgrundlage in Betracht (β).

α. Zurückbehaltungsrecht

Zunächst kann der Verantwortliche jedenfalls seine Leistung gem. § 320 Abs. 1 S. 1 BGB verweigern, wenn der Nutzer seinerseits nicht pflichtgemäß leistet, also entgegen einer vertraglichen Verpflichtung keine oder nur fehlerhafte

[729] Vgl. *Metzger*, AcP 216 (2016), 817 (853).

[730] *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.4.; *Hacker*, ZfPW 2019, 148 (178); *Specht*, JZ 2017, 763 (767 f.); *Metzger*, AcP 216 (2016), 817 (852, 863 f.).

Daten überlässt, eine wirksame Einwilligung nicht erteilt oder widerruft.[731] Dass der Widerruf bzw. die Nichtabgabe der Einwilligung, wie gesehen,[732] keine rechtswidrige Pflichtverletzung darstellen, ist für die Anwendbarkeit von § 320 Abs. 1 S. 1 BGB irrelevant, da es insoweit lediglich auf die Nichtleistung ankommt. Auch lässt sich nicht argumentieren, dass die Zurückbehaltung der Leistung des Anbieters die Ausübung des Widerrufsrechts unzulässig erschwert und damit den Effektivitätsgrundsatz des Unionsrechts verletzt.[733] Denn die betroffene Person kann regelmäßig gerade nicht erwarten, in den Genuss des Angebots zu kommen, wenn sie nicht ihrerseits ihre Leistungspflichten erfüllt.[734] Ihr Vertrauen auf den insoweit kostenfreien Erhalt der Leistung ist nicht schutzwürdig und begründet daher auch keine im Rahmen des Effektivitätsgrundsatzes zu berücksichtigende Beschwer.

β. Rücktritt, Kündigung und Wegfall der Geschäftsgrundlage

Denkbar ist darüber hinaus auch ein Rücktrittsrecht des Verantwortlichen gem. § 323 Abs. 1, Abs. 2 Nr. 2 BGB.[735] Allerdings stellt der Widerruf der Einwilligung nach dem soeben Gesagten keine Pflichtverletzung dar. Nichtsdestoweniger ist erwägenswert, § 323 Abs. 1 BGB analog anzuwenden, sofern ein Interesse des Verarbeiters auf Rückabwicklung erkennbar ist. Denn das Leistungsgefüge des Vertrags wird durch den Widerruf der Einwilligung jedenfalls dann, wenn eine Verarbeitung nicht aufgrund anderer Erlaubnistatbestände möglich ist, ganz erheblich gestört. Allerdings wird eine Rückabwicklung schon deshalb häufig ausscheiden, weil bei in Vollzug gesetzten Dauerschuldverhältnissen, wie sie bei einer kontinuierlichen Datenüberlassung in der Regel anzunehmen sind (Zugang zum sozialen Netzwerk), aufgrund der Komplexität und Interessenwidrigkeit der Rückabwicklung lediglich eine Auflösung des Vertragsverhältnisses ex nunc möglich ist.[736] Dann greift vorrangig § 314 BGB oder, je nach Vertragstypus, ein spezielles Kündigungsrecht wie § 543 Abs. 2 Nr. 1 BGB,[737] was auch insofern stimmig ist, als dafür auch besondere Umstände ausreichen, die, wie der Widerruf der Einwilligung, keine rechtswidrige Pflichtverletzung darstellen.[738]

---

[731] Vgl. zur Anwendbarkeit von § 320 Abs. 1 S. 1 BGB *Metzger*, AcP 216 (2016), 817 (852); *Tavanti*, RDV 2016, 231 (238).

[732] Siehe oben Text bei und Nachweise in § 4, Fn. 726.

[733] Vgl. insoweit nochmals EuGH, Urt. v. 17.4.2008 – Rs. C-404/06 (*Quelle*) – Rn. 34 f.; EuGH, Urt. v. 23.5.2019 – Rs. C-52/18 (*Fülla*) – Rn. 40.

[734] Vgl. *Metzger*, AcP 216 (2016), 817 (849).

[735] Vgl. *Metzger*, AcP 216 (2016), 817 (852); *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (98).

[736] *Ernst*, in: MüKo, BGB, 8. Aufl. 2019, § 323 Rn. 35 f.

[737] Zu letzterer Grundlage *Metzger*, AcP 216 (2016), 817 (853); *Specht*, JZ 2017, 763 (768); ein Kündigungsrecht grundätzlich bejahend auch *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (98), sowohl für den Fall des Widerrufs als auch der Überlassung inkorrekter Daten; für eine Anwendung von § 314 BGB auf die Überlassung inkorrekter Daten *Langhanke*, Daten als Leistung, 2018, 142 f.

[738] Siehe nur *Gaier*, in: MüKo, BGB, 8. Aufl. 2019, § 314 Rn. 18 f.

Ferner wäre im Rahmen des Rücktrittsrechts wiederum zu berücksichtigen, dass für den Verbraucher keine erheblichen Nachteile entstehen dürfen, die ihn von der Geltendmachung des Widerrufsrechts hinsichtlich der Einwilligung abhalten könnten, da andernfalls der Effektivitätsgrundsatz des Unionsrechts nun tatsächlich verletzt wäre.[739] Wertersatz für die bisherige Nutzung des Angebots des Verarbeiters scheidet daher nach hier vertretener Auffassung aus,[740] was auch insofern gerechtfertigt ist, als dem Verarbeiter die Vorteile der vor dem Widerruf vorgenommenen Verarbeitungen erhalten bleiben (Art. 7 Abs. 3 S. 2 DS-GVO)[741] und der Nutzer bei Bezahlung mit Daten auch keinen Nutzungspreis in Geld erstattet bekommt.[742] Einen Anspruch auf Herausgabe seiner personenbezogenen Daten bietet bereits das Datenschutzrecht nach Maßgabe von Art. 20 DS-GVO, so dass auch insoweit ein Rekurs auf § 346 Abs. 1 BGB obsolet ist. Ein über Art. 17 Abs. 1 lit. b DS-GVO hinausgehender, rückabwicklungsimmanenter Löschungsanspruch, der bereits bei Wegfall nur der Einwilligung (ohne Rücksicht auf die Möglichkeit der Verarbeitung nach anderen Erlaubnistatbeständen) griffe, würde hingegen am Anwendungsvorrang des Unionsrechts wegen der klaren, direkten Kollision mit Art. 17 Abs. 1 lit. b DS-GVO scheitern.[743]

Die Notwendigkeit dieser Anpassungen zeigt bereits, dass es interessengerechter, aber auch systematisch stimmiger ist, die vertragsrechtlichen Folgen des Widerrufs der Einwilligung für den Fall, dass mangels Dauerschuldverhältnis kein Kündigungsrecht greift, nicht über eine Analogie zum Rücktrittsrecht, sondern über § 313 BGB zu lösen.[744] Geschäftsgrundlage sind nach herrschender Meinung Umstände, die zwar nicht Vertragsinhalt geworden, für den vertraglichen Interessenausgleich jedoch von erheblicher Bedeutung und nicht der Risikosphäre lediglich einer Partei zuzurechnen sind.[745] Der Fortbestand der Einwilligung kann in der Tat nach diesem Maßstab als Geschäftsgrundlage des Vertrags angesehen werden, wenn eine Verarbeitung aufgrund anderer Erlaubnistatbestände nicht möglich ist und die Einwilligung wirksam erteilt wurde.

---

739 Vgl. EuGH, Urt. v. 17.4.2008 – Rs. C-404/06 (*Quelle*) – Rn. 34 f.; EuGH, Urt. v. 23.5.2019 – Rs. C-52/18 (*Fülla*) – Rn. 40.

740 Vgl. nochmals EuGH, Urt. v. 17.4.2008 – Rs. C-404/06 (*Quelle*) – Rn. 43; zum Wertersatz für fortgesetzte Nutzung *Specht*, JZ 2017, 763 (769).

741 Er muss lediglich auf Aufforderung der betroffenen Person die personenbezogenen Daten löschen, die auf Grundlage der Einwilligung verarbeitet wurden, sofern keine andere Rechtsgrundlage eingreift, Art. 17 Abs. 1 lit. b DS-GVO.

742 Dies allerdings erwägend *Graf von Westphalen*, BB 2016, 1411 (1417 f.).

743 Dies lassen *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (105) sowie *Specht*, JZ 2017, 763 (768) außer Acht.

744 Für eine Anwendung von „§§ 313, 314 Abs. 1, 2 BGB" bei Widerrruf der Einwilligung auch *Tavanti*, RDV 2016, 231 (238); zur Möglichkeit der Überschneidung von §§ 313 und 314 BGB auch *Gaier*, in: MüKo, BGB, 8. Aufl. 2019, § 314 Rn. 22; *Finkenauer*, in: MüKo, BGB, 8. Aufl. 2019, § 313 Rn. 169.

745 Siehe nur BGH DtZ 1995, 285 (289); *Finkenauer*, in: MüKo, BGB, 8. Aufl. 2019, § 313 Rn. 8; *Stadler*, in: Jauernig, BGB, 17. Aufl. 2018, § 313 Rn. 3 f.

Denn einerseits kann der Fortbestand nicht zum wirksamen Vertragsinhalt gemacht werden, da dem das nicht abdingbare Widerrufsrecht nach Art. 7 Abs. 3 S. 1 DS-GVO entgegensteht. Andererseits erscheint es unbillig, dem Verantwortlichen allein das Risiko des Fortbestands aufzuerlegen. Denn er kann den Widerruf nicht verhindern, der wiederum allein in der Sphäre der betroffenen Person wurzelt. Diese kann auch erkennen, dass der Fortbestand der Einwilligung beim Einsatz von Daten als Gegenleistung typischerweise für den Vertragspartner besonders bedeutsam ist.

Bei Rekurs auf § 313 BGB kann dann einerseits in Betracht gezogen werden, inwieweit dem Verarbeiter das Festhalten am Vertrag tatsächlich nicht mehr zumutbar ist, und es können andererseits die Rechtsfolgen flexibel gestaltet werden. Die Art. 16 f. DIDD-Richtlinie können insoweit als Vorbild dienen.

Daher erscheint die Lösung über § 313 BGB letztlich für Verträge ohne Dauerschuldcharakter vorzugswürdig; mangels Regelungslücke liegen dann auch die Voraussetzungen für einen Analogieschluss zu § 323 BGB nicht vor. Bei Dauerschuldverhältnissen hingegen bestimmen sich die Vertragslösungsmöglichkeiten des Verantwortlichen nach § 314 BGB[746] oder etwaig einschlägigen Kündigungsrechten des besonderen Schuldrechts (z. B. § 543 BGB).

(bb) Konditionale Verknüpfung

Etwas einfacher gestaltet sich die Rechtslage bei Widerruf der Einwilligung oder Nichtüberlassung von Daten, wenn eine konditionale Verknüpfung angenommen wird. Dabei entfällt mit der Nichterfüllung der (atypischen Dauer-) Bedingung die Wirksamkeit des Leistungsversprechens des Anbieters.[747] Es findet kein weiterer Leistungsaustausch mehr statt, aber auch keine Rückabwicklung. Dies entspricht im Wesentlichen dem Leitbild von Art. 16 f. DIDD-Richtlinie bei der Verwendung von Daten als Gegenleistung.

Hinsichtlich der Datenüberlassung, die typischerweise den Kern der datenbasierten Gegenleistung ausmacht, ist eine konditionale Verknüpfung regelmäßig anzunehmen.[748] Die Abgabe bzw. Widerruf der Einwilligung hingegen dürften nur dann eine konkludent vereinbarte (aufschiebende bzw. auflösende) Bedingung für die Inanspruchnahme der Leistung des Anbieters darstellen, wenn die Datenverarbeitung lediglich auf Art. 6 Abs. 1 lit. a DS-GVO gestützt werden kann.[749] Denn wenn die Rechtmäßigkeit der Datenverarbeitung auf Grundlage eines anderen Erlaubnistatbestands erreicht werden kann, ist der Widerruf der Einwilligung für den Anbieter unerheblich,[750] sodass auch kein Grund zur Einstellung der Leistung besteht.

---

[746] *Tavanti*, RDV 2016, 231 (238).
[747] Dazu ausführlich *Hacker*, ZfPW 2019, 148 (175 f., 178).
[748] *Hacker*, ZfPW 2019, 148 (172).
[749] *Hacker*, ZfPW 2019, 148 (178).
[750] Siehe oben, § 4 B.I.3.b)bb)(1).

Bei der konditionalen Verknüpfung ist der Fortbestand der Einwilligung nach hier vertretener Auffassung also gegebenenfalls Teil der Bedingung, an welche die Erbringung der Leistung des Anbieters geknüpft ist, und nicht Geschäftsgrundlage wie bei der synallagmatischen Verknüpfung. Denn im Rahmen der synallagmatischen Verknüpfung musste insoweit auf die Figur der Geschäftsgrundlage nur deshalb zurückgegriffen werden, weil die Garantie des Fortbestands der Einwilligung in Ansehung des unbeschränkbaren Widerrufsrechts nicht als wirksame schuldrechtliche Verpflichtung ausgestaltet werden kann. Demgegenüber negiert die Ausgestaltung des Fortbestands der Einwilligung als Bedingung in keiner Weise das Widerrufsrecht – bei Ausübung dieses Rechts entfällt lediglich der Anspruch auf die Leistung des Anbieters.

Dies hat gegenüber der Annahme einer Geschäftsgrundlage den Vorzug, dass die Leistungspflicht des Anbieters automatisch erlischt, ohne dass es einer Kündigungserklärung bedürfte. Dies dürfte regelmäßig den Interessen des Anbieters an einer automatisierten, codebasierten Regelung des Zugriffs auf das Leistungsangebot (*governance by code*) eher entsprechen.[751] Die Interessen des Nutzers hingegen werden dadurch nicht ungebührlich beschnitten, da er nicht damit rechnen kann, bei Widerruf einer datenschutzrechtlich erforderlichen Einwilligung noch in den Genuss der Leistung zukommen.

Da der Fortbestand der Einwilligung, sofern sie für die Verarbeitung notwendig ist, bei der konditionalen Verknüpfung Gegenstand der Bedingung ist, stellt sie einen Teil des Vertragsinhalts und damit keine Geschäftsgrundlage dar.[752] Eines eigenen Vertragslösungsrechts bedarf es jedoch typischerweise auch nicht, weil ein weiterer Leistungsaustausch nicht stattfindet und eine Rückabwicklung den Interessen der Partei in der Regel nicht entspricht. Sollte dies doch der Fall sein, kann wiederum auf § 314 BGB zurückgegriffen werden.

(4) Zusammenfassung zum Widerruf

Insgesamt zeigt sich damit, dass eine ausgewogene Interpretation der Vorschriften der DS-GVO zum Widerruf, im Zusammenspiel mit dem allgemeinen Teil des BGB, eine sach- und interessengerechte Bewältigung der damit verbundenen Probleme ermöglicht. Der Widerruf kann zwar durch vertragliche Abreden nicht beschränkt werden, sperrt jedoch seinerseits nicht den Rückgriff auf andere Erlaubnistatbestände. Einem etwaigen dringenden Bedürfnis des Verantwortlichen, zur Aufrechterhaltung der vertraglichen Äquivalenzordnung Daten weiter zu verarbeiten, kann daher im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO flexibel Rechnung getragen werden.

---

751 Vgl. *Hacker*, ZfPW 2019, 148 (177).

752 Zum wechselseitigen Ausschluss von Vertragsinhalt und Geschäftsgrundlage BGH NJW-RR 1995, 853 (854).

Um eine Verletzung des unionalen Effektivitätsgrundsatzes zu vermeiden, kann jedoch an den Widerruf der Einwilligung selbst kein Schadensersatzanspruch des Verantwortlichen gerichtet auf das positive Interesse geknüpft werden. Dies ist lediglich möglich für die Überlassung fehlerhafter Daten oder die Nichtüberlassung von Daten vor Widerruf, sofern die Überlassung korrekter Daten vertraglich wirksam vereinbart wurde. Schließlich zeigt sich, dass der Verarbeiter mit Kündigungsrechten aus § 314 BGB oder § 543 Abs. 2 BGB bei Dauerschuldverhältnissen wirksam auf den Widerruf der Einwilligung reagieren kann, sofern er auf diese angewiesen ist. Bei punktuellem Leistungsaustausch bleibt eine Vertragsanpassung nach § 313 BGB möglich. Insgesamt können damit gerade auch die Interessen des Verantwortlichen im Rahmen von Verträgen mit Daten als Gegenleistung gewahrt werden.

cc) Minderjährige, Art. 8 DS-GVO

Besondere zusätzliche Voraussetzungen für die Einwilligung bestehen nach Art. 8 DS-GVO ferner für Minderjährige. Danach kann die oder der Minderjährige (in der Diktion der DS-GV: das Kind) ab Vollendung des 16. Lebensjahrs wirksam selbst bei Angeboten im Rahmen von Diensten der Informationsgesellschaft[753] einwilligen (Art. 8 Abs. 1 UAbs. 1 S. 1 DS-GVO); jüngere Minderjährige benötigen die Einwilligung der Eltern[754] oder deren Zustimmung zu ihrer Einwilligung (Art. 8 Abs. 1 UAbs. 1 S. 2 DS-GVO). Die Mitgliedstaaten können jedoch gem. Art. 8 Abs. 1 UAbs. 2 DS-GVO diese Grenze der Einwilligungsfähigkeit bis auf das 13. Lebensjahr absenken, worauf Deutschland allerdings verzichtet hat. Damit hat die DS-GVO (zumindest bei Onlinediensten[755]) für Klarheit hinsichtlich der Kriterien der Einwilligungsfähigkeit gesorgt,[756] die nach altem Recht in Deutschland stark umstritten waren.[757]

Die mit der auf 16 Jahre abgesenkten Einwilligungsfähigkeit einhergehenden datenschutzrechtlichen Risiken sollen dadurch abgefedert werden, dass der Minderjährige jederzeit die Löschung der nach Art. 8 Abs. 1 S. 1 DS-GVO verarbeiteten Daten nach Art. 17 Abs. 1 lit. f DS-GVO verlangen kann. Insbesondere kommt es hier nicht auf das etwaige Vorliegen anderer Rechtfertigungs-

[753] Diese bestimmt Art. 4 Nr. 25 DS-GVO durch Verweis näher.

[754] Die DS-GVO spricht von den „Trägern elterlicher Verantwortung". Dies wird man als Referenz auf die gesetzlichen Vertreter lesen müssen, *Joachim*, ZD 2017, 414 (416).

[755] Für eine Indizwirkung der Altersgrenze der DS-GVO auch in anderen Konstellationen überzeugend *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 8 DS-GVO Rn. 12; aA *Joachim*, ZD 2017, 414 (415 f.).

[756] *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 8 DS-GVO Rn. 2, 10; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 8 DS-GVO Rn. 3, 19; aA *Joachim*, ZD 2017, 414 (415 f.: Fortgeltung der alten Kriterien nach Maßgabe von Art. 6 Abs. 1 lit. a DS-GVO).

[757] Siehe zu den alten Kriterien etwa *Metzger*, AcP 216 (2016), 817 (840); *Bräutigam*, MMR 2012, 635 (638).

gründe an, wie Art. 17 Abs. 1 lit. b DS-GVO ex negativo zeigt. Nach Art. 8 Abs. 3 DS-GVO haben diese Regelungen zur Einwilligungsfähigkeit jedoch keine Auswirkungen auf das allgemeine Vertragsrecht der Mitgliedstaaten.

(1) Mangelnder Gleichlauf mit dem BGB

Dennoch ist eine Abweichung von den Grundsätzen des Minderjährigenrechts des BGB unübersehbar. Zwar richtet sich die Einwilligungsfähigkeit im allgemeinen Zivilrecht nach der natürlichen Einsichts- und Urteilsfähigkeit und ist damit unabhängig von der beschränkten Geschäftsfähigkeit nach §§ 2, 106 BGB.[758] Typischerweise wird damit die zivilrechtliche Einwilligungsfähigkeit auch etwa um das 16. Lebensjahr herum erreicht sein, auch wenn kontextbezogene Varianz besteht.[759] Die datenschutzrechtliche Einwilligung ist jedoch regelmäßig verknüpft mit dem Abschluss eines Vertrags, etwa über die Nutzung eines sozialen Netzwerks oder eines IoT-Geräts. Hinsichtlich dieses Vertrags gelten unstrittig die Regelungen der §§ 106 ff. BGB. Ist der Minderjährige mithin zwischen 16 und 18 Jahren alt, so kann er zwar die Einwilligung in die Datenverarbeitung wirksam abgeben, jedoch nicht (vorbehaltlich der Regelungen in §§ 110, 112 f.) selbstständig den Vertrag abschließen, wenn dieser für ihn nicht lediglich rechtlich vorteilhaft ist (§ 107 F1 BGB).[760] Jedenfalls dann, wenn eine Pflicht zur Überlassung von Daten oder zur Abgabe einer Einwilligung Bestandteil des Vertrags ist, ist dieser mit rechtlichen Nachteilen für den Minderjährigen verbunden, sodass gem. § 107 F2 BGB oder § 108 Abs. 1 BGB die Zustimmung der Eltern erforderlich ist.[761] Datenschutzrechtliche Einwilligungsfähigkeit und zivilrechtliche Vertragsabschlusskompetenz fallen dann auseinander.[762] Dies bleibt auch dann der Fall, wenn man mit der herrschenden Literatur davon ausgeht, dass der Minderjährige wegen der Implikation seines informationellen Selbstbestimmungsrechts dem Vertragsschluss, zusätzlich zu den Eltern, ebenfalls zustimmen muss.[763] Auch dann kann der Minderjährige

[758] BGH NJW 1972, 335 (337); *Wagner*, in: MüKo, BGB, 7. Aufl. 2016, § 630d Rn. 20; *Lauf/Birck*, NJW 2018, 2230 (2234).

[759] Gegen eine Einwilligungsfähigkeit 15-jähriger in die Verarbeitung personenbezogener Daten bei einem Gewinnspiel OLG Hamm, ZD 2013, 29; für eine flexible Handhabung auch *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 250.

[760] Zu einem ähnlichen Konfliktbereich beim ärztlichen Behandlungsvertrag *Lauf/Birck*, NJW 2018, 2230 (2234).

[761] *Metzger*, AcP 216 (2016), 817 (839); *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, 2016, 10; *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.6.

[762] *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.6.

[763] *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 275 f.; *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 54 f.; *Metzger*, AcP 216 (2016), 817 (839); allgemein für die Einwilligung in Persönlichkeitsrechte *Ohly*, „Volenti non fit iniuria" – Die

allein lediglich die Einwilligung abgeben, nicht den Vertrag schließen.[764] Dies ist insofern rechtspolitisch bedenklich,[765] als Risiken für den Minderjährigen typischerweise eher aus der Datenverarbeitung, welche durch die Einwilligung erlaubt wird,[766] als aus einer Verpflichtung zur Datenüberlassung erwachsen, welche zumeist durch die Unternehmen ohnehin nicht durchgesetzt wird.[767]

Aber auch im umgekehrten Fall, in dem der Minderjährige das 16. Lebensjahr noch nicht vollendet hat, ergeben sich Reibungspunkte zwischen Datenschutzrecht und BGB. Hier kann der Minderjährige ab Vollendung des siebten Lebensjahrs einen Vertrag in bestimmten Konstellationen wirksam abschließen (§§ 107 F1, 110, 112 f. BGB), die jedoch im Datenschutzrecht keine Entsprechung finden. Die Folge ist, dass der Minderjährige sich zwar wirksam vertraglich verpflichten kann, beispielsweise nach § 113 Abs. 1 S. 1 BGB personenbezogene Daten für die Nutzung eines für ein Arbeitsverhältnis erforderlichen IoT-Geräts zu überlassen, jedoch die entsprechende Einwilligung in die Datenverarbeitung nicht selbst erklären kann.

Hinzu kommt das praktische Problem, dass die Anbieter bei Fernabsatzverträgen kaum wirksam kontrollieren können, ob die jeweils gesetzlich vorgesehene Altersgrenze erreicht ist oder nicht.[768] Zwar sieht Art. 8 Abs. 2 DS-GVO die Einrichtung technischer und organisatorischer Maßnahmen zur Sicherstellung des Vorliegens der elterlichen Einwilligung vor; wie diese wirksam umgesetzt werden können, ist jedoch kaum ersichtlich.[769]

Einwilligung im Privatrecht, 2002, 320, einschränkend für die datenschutzrechtliche Einwilligung 324.

[764] Ob der Minderjährige die Einwilligung kondizieren kann, wenn eine dahingehende Verpflichtung mangels Zustimmung der Eltern unwirksam ist (so *Metzger*, AcP 216 [2016], 817 [840]; *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, 2016, 10), bleibt zweifelhaft. Denn die Einwilligung kann auch unabhängig von Verpflichtungsgeschäften erteilt werden, trägt daher grundsätzlich ihren Rechtsgrund in sich. Ferner wird eine konkrete Verpflichtung zur Erteilung einer Einwilligung in der Praxis kaum vereinbart, siehe *Hacker*, ZfPW 2019, 148 (169). Sollte dies doch einmal der Fall sein, so mag eine Kondiktion der Einwilligung (mit der Folge eines Nutzungs- und Wertersatzanspruches gem. § 818 Abs. 1 und 2 BGB) möglich sein. Dass dies jedoch auch die darauf basierende Datenverarbeitung rückwirkend unwirksam macht, die bei Fehlen einer Verpflichtung zur Einwilligung nach Art. 7 Abs. 3 S. 2 DS-GVO bis zum Widerruf rechtmäßig gewesen wäre, erscheint eher fernliegend. Zur Kondiktion der auf Grundlage der Einwilligung rechtmäßig verarbeiteten Daten siehe noch unten, Text bei § 5, Fn. 552.

[765] *Metzger*, AcP 216 (2016), 817 (840); *Bräutigam*, MMR 2012, 635 (638).

[766] Vgl. den 38. Erwägungsgrund der DS-GVO.

[767] Zur mangelnden Durchsetzung *Metzger*, AcP 216 (2016), 817 (853); *Hacker*, ZfPW 2019, 148 (173).

[768] *Tinnefeld/Conrad*, ZD 2018, 391 (393).

[769] Eine Möglichkeit bieten zwar digitale Identifizierungsverfahren (Video-Ident o. Ä.), die zur Erfüllung von KYC-Pflichten im Bankverkehr entwickelt wurden, jedoch bei vielen kleinen Online-Diensten zu aufwändig sein dürften („angemessene Anstrengungen"), siehe *Tinnefeld/Conrad*, ZD 2018, 391 (393).

(2) Partielle Auflösung durch Auslegung

Die rechtsgeschäftliche Gestaltungsmacht des Minderjährigen bleibt also im Datenschutzrecht für Minderjährige unter 16 Jahren hinter den Möglichkeiten des BGB zurück, übertrifft sie hingegen für Minderjährige, die älter als 16 Jahre sind. An den klaren Altersvorgaben der DS-GVO führt *de lege lata* kein Weg vorbei; dies gilt auch für Einwilligungen im Rahmen von Verträgen, da diese Konstellation von der DS-GVO ausweislich Art. 6 Abs. 1 lit. b und des 65. Erwägungsgrundes durchaus gesehen wurde.[770] Um hier eine gewisse Konvergenz zwischen BGB und DS-GVO zu gewährleisten, sind vielmehr auf zivilrechtlicher Seite zwei Wege denkbar.

Zum einen könnte man § 110 BGB so auslegen, dass unter die Mittel, mit welchen die vertragsgemäße Leistung bewirkt wird, auch die personenbezogenen Daten des Minderjährigen fallen. Dies passt jedoch weder zum Wortlaut noch zum Schutzzweck des § 110 BGB. Denn die personenbezogenen Daten werden dem Minderjährigen nicht vom gesetzlichen Vertreter, oder einem Dritten mit dessen Zustimmung, überlassen, wie dies § 110 BGB fordert. Dies ist jedoch essenziell, da (nach zutreffender Ansicht) in dieser Überlassung gerade die antizipierte, konkludente Einwilligung des gesetzlichen Vertreters in die Verwendung dieser Mittel zu Vertragsschlüssen steckt.[771] Diese Vorabkontrolle des eingesetzten Vermögensumfangs fehlt bei durch den Minderjährigen selbst generierten Daten.

Denkbar ist daher allenfalls eine analoge Anwendung des § 110 BGB. Hier kommt jedoch in teleologischer Hinsicht hinzu, dass § 110 BGB gerade deshalb die Wirksamkeit des Vertragsschlusses anordnet, weil die vertragsgemäße Leistung vollständig mit den überlassenen Mitteln bewirkt wird. Es kann daher, jedenfalls grundsätzlich, kein weiterer Schaden für das Vermögen des Minderjährigen entstehen.[772] Dies ist jedoch im Falle der Verwendung personenbezogener Daten grundsätzlich anders. Hier bestehen, gerade bei Minderjährigen, erhebliche Datenschutzrisiken, welche diese typischerweise nicht überblicken können;[773] man denke nur an die viel zitierte Suche des potenziellen Arbeitgebers oder Versicherers in den Posts eines Kandidaten in sozialen Netzwer-

[770] Damit dürften die nach altem Recht vertretenen Einschränkungen der Einwilligungsfähigkeit im Rahmen von Verträgen (*Metzger*, AcP 216 [2016], 817 [840]; *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 47 ff.) überholt sein; aA wohl *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 8 DS-GVO Rn. 12, dessen Ansicht aber, wenn sie sich auch auf Dienste der Informationsgesellschaft bezieht, zu erheblicher Rechtsunsicherheit („Gegenstand der vertraglichen Leistungspflichten") führen würde, was den Zweck von Art. 8 Abs. 1 S. 1 DS-GVO gerade konterkarieren würde.

[771] *Spickhoff*, in: MüKo, BGB, 8. Aufl. 2018, § 110 Rn. 3.

[772] *Spickhoff*, in: MüKo, BGB, 8. Aufl. 2018, § 110 Rn. 1.

[773] Siehe nochmals den 38. Erwägungsgrund der DS-GVO; *Spickhoff*, in: MüKo, BGB, 8. Aufl. 2018, § 110 Rn. 24; *Bräutigam*, MMR 2012, 635 (638); *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, 2016, 10.

ken. Daher ist eine (analoge) Anwendung von § 110 BGB auf von Minderjährigen selbst generierte, personenbezogene Daten klar abzulehnen.[774]

Aussichtsreicher ist hingegen eine zweite Lösungsvariante. Denn dem Minderjährigen steht es frei, nach § 107 F1 BGB solche Verträge abzuschließen, die für ihn lediglich rechtlich vorteilhaft sind. Dies bedeutet, dass keine persönlichen Pflichten des Minderjährigen begründet oder bestehende Rechte eingeschränkt werden dürfen.[775] Darunter kann man die konditionale Verknüpfung von Datenüberlassung oder Einwilligung mit der Erfüllung der Leistungspflichten des Anbieters fassen. Denn eine Bedingung generiert gerade keine Pflicht des Minderjährigen, Daten zu überlassen oder eine Einwilligung zu erklären. Unterlässt er dies, erlangt er schlicht keinen weiteren Zugang zur Dienstleistung. Auch wird man in dem Vertrag keine relevante Einschränkung des Datenschutzrechts des Minderjährigen sehen können,[776] da insofern die Wertung des Art. 8 Abs. 1 S. 1 DS-GVO klarstellt, dass der mindestens 16-jährige Minderjährige nach Auffassung des Unionsgesetzgebers über seine informationelle Selbstbestimmung qua Einwilligung disponieren können soll.[777] Die konditionale Konstruktion ermöglicht daher, für Minderjährige zwischen 16 und 18 Jahren, einen Gleichlauf zwischen Einwilligungsfähigkeit nach der DS-GVO und beschränkter Geschäftsfähigkeit nach dem BGB. Dies gilt jedoch selbstverständlich nur, wenn nicht durch den Vertrag noch andere persönliche Pflichten des Minderjährigen begründet oder Rechte beschränkt werden. Bei vielen Onlinediensten ist dies z. B. durch Lizenzen, welche diese sich an von den Nutzern hochgeladenen Inhalten einräumen lassen, der Fall.[778]

Für den umgekehrten Altersfall, in welchen der Minderjährige das 16. Lebensjahr noch nicht vollendet hat, lässt sich hingegen keine Konkordanz zwischen den weitergehenden Regelungen des BGB und der DS-GVO herstellen. Dies ist jedoch auch gerechtfertigt, da insofern die datenschutzrechtlichen Risiken aufgrund der altersspezifischen kognitiven Konstitution des Minderjährigen für diesen noch weniger überschaubar sind und daher die Einwilligung

---

[774] *Spickhoff*, in: MüKo, BGB, 8. Aufl. 2018, § 110 Rn. 24; *Bräutigam*, MMR 2012, 635 (638); *Jandt/Roßnagel*, MMR 2011, 637 (640); *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, 2016, 10; aA *Wintermeier*, ZD 2012, 210 (213).

[775] Siehe BGH NJW 2005, 415 (417); *Spickhoff*, in: MüKo, BGB, 8. Aufl. 2018, § 107 Rn. 40 ff., besonders Rn. 54.

[776] So aber *Bräutigam*, MMR 2012, 635 (637); *Wintermeier*, ZD 2012, 210 (212); wie hier im Ergebnis *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, 2016, 9.

[777] Dies läge nur dann anders, wenn Art. 6 Abs. 1 lit. b DS-GVO eine Datenverarbeitung erlauben würde, in welche der Minderjährige nicht wirksam nach Art. 8 Abs. 1 S. 1 DS-GVO einwilligen könnte. Diesbezügliche Fälle sind jedoch nicht ersichtlich, wenn die Vertragserforderlichkeit in Art. 7 Abs. 4 und Art. 6 Abs. 1 lit. b DS-GVO einheitlich ausgelegt wird (dazu unten, § 4 B.II.2.b)).

[778] *Bräutigam*, MMR 2012, 635 (637); ähnlich *Jandt/Roßnagel*, MMR 2011, 637 (639).

in diese Risiken richtigerweise dem gesetzlichen Vertreter überantwortet werden muss. Hier ist insbesondere wichtig zu sehen, dass bei Ausbleiben einer derartigen elterlichen Einwilligung typischerweise auch andere Erlaubnistatbestände nicht in Betracht kommen. Bei Art. 6 Abs. 1 lit. f DS-GVO ist ausdrücklich festgehalten, dass das Kindeswohl besonders berücksichtigt werden muss.[779]

Insgesamt lässt sich damit durch eine konditionale Verknüpfung von Leistung und Gegenleistung bei Verträgen, in denen personenbezogene Daten die Gegenleistung darstellen, eine partielle Konvergenz zwischen datenschutzrechtlicher Einwilligungsfähigkeit und zivilrechtlicher Vertragsabschlusskompetenz herstellen. Konflikte bestehen jedoch weiterhin bei Minderjährigen zwischen sieben und 16 Jahren, was mit Blick auf die erhöhten datenschutzrechtlichen Risiken jedoch hinzunehmen ist.

dd) Sensitive Daten, Art. 9 DS-GVO

Schließlich ist als weitere besondere Schutzvorschrift Art. 9 DS-GVO zu nennen, der sich sensiblen Daten widmet. Er ist auch *lex specialis* zu Art. 8 DS-GVO.[780] Die Sonderbehandlung sensitiver Daten legitimiert sich aus dem mit den genannten Daten einhergehenden Diskriminierungspotenzial und dem Umstand, dass diese Daten besonders nah an für die Persönlichkeitsentfaltung zentralen Lebensbereichen liegen oder diese ausmachen.[781] Sie ist damit Teil des (hier abstrakt typisierenden) risikobasierten Ansatzes der DS-GVO.[782]

(1) Regelungsstruktur

Art. 9 Abs. 1 DS-GVO installiert dabei ein eigenes Verbotsprinzip[783] hinsichtlich der Verarbeitung personenbezogener Daten, „aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person".

---

[779] Zu Interpretationsmöglichkeiten etwa *Joachim*, ZD 2017, 414 (416); zum Fall Facebook instruktiv *Buchner*, WRP 2019, 1243 (1248).

[780] Dies zeigt bereits der Wortlaut von Art. 8 Abs. 1 S. 1 DS-GVO, der vom Grundtatbestand des Art. 6 Abs. 1 lit. a DS-GVO ausgeht. *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 8 DS-GVO Rn. 17.

[781] Siehe den 51. und 71. Erwägungsgrund der DS-GVO; *Weichert*, DuD 2017, 538 (539); *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 9 DS-GVO Rn. 10; *Weichert*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 9 DS-GVO Rn. 15–17.

[782] 51. Erwägungsgrund der DS-GVO; *Veil*, ZD 2015, 347 (349).

[783] Siehe nur *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 9 DS-GVO Rn. 2; *Roßnagel*, NJW 2019, 1 (4).

Der zweite Absatz der Schutzvorschrift nennt dann abschließend Erlaubnistatbestände, welche nach der im 51. Erwägungsgrund angelegten Lesart zusätzlich zu Art. 6 Abs. 1 DS-GVO hinzutreten.[784] Dies ist insbesondere deshalb von Belang, weil die vertragserforderliche Datenverarbeitung (Art. 6 Abs. 1 lit. b DS-GVO) und die Datenverarbeitung aufgrund überwiegender Verarbeiterinteressen (Art. 6 Abs. 1 lit. f DS-GVO) hier keine Entsprechung finden. Im Rahmen der digitalen Wirtschaft sind Verarbeiter daher faktisch auf eine ausdrückliche Einwilligung nach Art. 9 Abs. 2 lit. a DS-GVO angewiesen.

(2) Unmittelbar und mittelbar sensitive Daten

Angesichts der bei einer Einwilligung in Anbetracht der bereits diskutierten Voraussetzungen aus Art. 4 Nr. 11 und Art. 7 DS-GVO, die auch im Rahmen von sensitiven Daten beachtet werden müssen, bestehenden Rechtsunsicherheit hinsichtlich der Wirksamkeit der Einwilligung kommt der Feststellung, ob Daten zu den besonders geschützten, sensitiven Kategorien gehören, erhebliche Bedeutung zu. Diese Subsumtion wird jedoch dadurch erschwert, dass mithilfe von Techniken maschinellen Lernens auch an sich unverdächtige Daten (Aussehen, Facebook Likes) genutzt werden können, um mit signifikanter Wahrscheinlichkeit auf das Vorliegen der genannten Merkmale zu schließen.[785] Daher stellt sich die Frage, ab welchem Korrelationswert nicht primär sensitive Daten zu solchen werden.

Hier könnte man zunächst zwischen unterschiedlichen Typen von sensitiven Merkmalen unterscheiden.[786] Denn nach dem Wortlaut von Art. 9 Abs. 1 DS-GVO genügt es einerseits, wenn aus personenbezogenen Daten „rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit *hervorgehen*“ [Hervorhebung des Verfassers; engl. Fassung: *reveal*]. Dagegen geht es anderseits unmittelbar um die Verarbeitung *von* „genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“ (engl. Fassung: *concerning*). Dass jedoch bei dieser zweiten Gruppe

[784] *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 9 DS-GVO Rn. 2; *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 9 DS-GVO Rn. 5. Dies führt jedoch teilweise zu einer unnötigen Doppelung der Voraussetzungen (z. B. Art. 9 Abs. 2 lit. a und Art. 6 Abs. 1 lit. a DS-GVO); daher aA *Jandt*, DuD 2016, 571 (573) (Abs. 2 lit. c, lit. d, lit. e und lit. f. als abschließende Erlaubnistatbestände; wohl auch lit. a, wenngleich hier Ausschlussmöglichkeit durch Unionsrecht oder nationales Recht nach dem Wortlaut). Richtigerweise wird jeweils im Einzelfall zu entscheiden sein, ob eine zusätzliche Prüfung von Art. 6 Abs. 1 DS-GVO Sinn macht (z. B. Art. 9 Abs. 2 lit. e DS-GVO) oder nicht (z. B. Art. 9 Abs. 2 lit. a DS-GVO).

[785] *Kosinski/Stillwell/Graepel*, 110 Proceedings of the National Academy of Sciences 2013, 5802; *Wang/Kosinski*, 114 Journal of Personality and Social Psychology 2018, 246; siehe auch *Schneider*, ZD 2017, 303 (306).

[786] So *Schneider*, ZD 2017, 303 (303 f.).

von sensitiven Merkmalen ein engerer Zusammenhang zwischen Daten und Merkmal bestehen muss, vermag aus teleologischer Sicht nicht einzuleuchten, da Diskriminierung und andere Nachteile bei diesen Merkmalen ebenso zu befürchten sind wie bei in der ersten Gruppe. Daher ist die Schwelle für alle sensitiven Daten einheitlich zu bestimmen.[787] Eine feste quantitative Grenze wird dabei jedoch kaum etabliert werden können.

Letztlich wird man sich damit behelfen müssen, dass nicht unmittelbar sensitive Daten (z. B. Facebook Likes, Bewegungsprofile) dann keine mittelbar sensitiven Daten darstellen und daher nicht unter Art. 9 Abs. 1 DS-GVO fallen, wenn in dem konkreten Kontext der Datenverarbeitung nicht damit zu rechnen ist, dass der Verantwortliche eine (statistisch signifikante) Zuordnung zu sensitiven Kriterien vornimmt.[788] Angesichts der rapide fortschreitenden Möglichkeiten der Korrelation von nicht unmittelbar sensitiven Daten mit sensitiven Merkmalen würde andernfalls Art. 9 DS-GVO den eigentlich als Grundnorm konzipierten Art. 6 DS-GVO faktisch ersetzen, was nicht der Intention des Verordnungsgebers entspräche.[789] Hierfür spricht auch, dass, anders als bei der Definition personenbezogener Daten, bei denen eine indirekte Identifizierbarkeit (z. B. durch Techniken maschinellen Lernens) nach Art. 4 Nr. 1 DS-GVO grundsätzlich genügt,[790] eine indirekte Gewinnung der Merkmale nicht ausdrücklich im Wortlaut von Art. 9 Abs. 1 DS-GVO erwähnt wird. Schließlich zeigt dies auch die Behandlung von Lichtbildern (Fotos, Videos) im 51. Erwägungsgrund, denen dort sensitive Merkmale nur zugeschrieben werden, wenn sie eine „eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen" – obgleich damit typischerweise die Hautfarbe und korrelativ auch die „rassische und ethnische Herkunft" bestimmt werden kann.

Dass Dritte vom Verantwortlichen veröffentlichte, nicht unmittelbar sensitive Daten nutzen können, um Korrelationen zu sensitiven Merkmalen zu etablieren, ist zwar nicht ausgeschlossen. Allerdings müssen Verarbeitungen, die jene Korrelationen zum Ziel haben, dann eben selbst den Vorgaben von Art. 9 DS-GVO entsprechen – aber nicht jene Verarbeitungen, die Daten betreffen, denen lediglich ein derartiges Korrelationspotenzial innewohnt. So lassen sich das Schutzbedürfnis der betroffenen Personen einerseits und das Verarbeitungsbedürfnis von Anbietern andererseits in schonenden Ausgleich bringen.

---

[787] Im Ergebnis ebenso *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 9 DS-GVO Rn. 2.

[788] So auch *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 9 DS-GVO Rn. 13; *Weichert*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 9 DS-GVO Rn. 22–24; ähnlich *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 211 f. (Sensibilitätsprognose); aA *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 9 DS-GVO Rn. 12 (hinreichende Korrelationshöhe hinreichend); *Schneider*, ZD 2017, 303 (305).

[789] *Schneider*, ZD 2017, 303 (307).

[790] Siehe oben, § 4 A.II.2.a)aa)(2).

c) Allgemeine Wirksamkeitsvoraussetzungen nach dem BGB

Die soeben diskutierten besonderen Wirksamkeitsvoraussetzungen der Einwilligung nach Art. 7–9 DS-GVO sind elementarer Bestandteil des unionalen Datenschutzrechts. Bereits hier zeigte sich aber, insbesondere bei den Rechtsfolgen des Widerrufs der Einwilligung und der Einwilligung von Minderjährigen, ein signifikanter Koordinierungsbedarf mit dem allgemeinen Zivilrecht. Dieser verstärkt sich noch bei der Beantwortung der Frage, ob die allgemeinen Wirksamkeitsvoraussetzungen für Rechtsgeschäfte nach dem BGB auch für die datenschutzrechtliche Einwilligung gelten sollen. Dieser Fragestellung geht ein eigener Teil der Arbeit nach, im Rahmen der das Datenprivatrecht betreffenden Ermöglichungsstrukturen des Zivilrechts.[791]

4. Cookies und andere Geräte-Identifier: Von der ePrivacy-Richtlinie über die DS-GVO zur ePrivacy-VO

Damit verbleibt noch ein letztes, für den hiesigen Kontext besonders bedeutsames Sonderregime der Einwilligung zu besprechen, welches das Datenprivatrecht in erheblicher Weise prägt, insbesondere mit Blick auf den zweiten Leitfall (*third-party tracking*): die Einwilligung in die Verwendung von Cookies und anderen Tracking-Tools. Die technischen Grundlagen von Tracking-Instrumenten wurden bereits im ersten Teil der Arbeit dargestellt.[792] Daher soll hier nur noch einmal in Erinnerung gerufen werden, dass sich diese Instrumente in drei unterschiedliche Gruppen einteilen lassen: Cookies, *fingerprinting* und geräteeigene *unique strings*.[793] Alle gemeinsam werden als Geräte-Identifier bezeichnet.[794]

Ihre rechtliche Analyse folgt einem Dreischritt an Normgefügen: Zunächst kommt die ePrivacy-Richtlinie in den Blick (a)), sodann die DS-GVO (b)) und, als Ausblick, schließlich die ePrivacy-Verordnung (c)).

a) Regelung nach der ePrivacy-Richtlinie

Jedenfalls bis zum Geltungsbeginn der DS-GVO war für die Nutzung dieser Instrumente in datenschutzrechtlicher Hinsicht die ePrivacy-Richtlinie maßgeblich. Ursprünglich aus dem Jahr 2002,[795] wurde sie gerade in Bezug auf die Regelung zu Tracking-Instrumenten durch die Richtlinie 2009/136/EG[796] neu gefasst.

---

[791] Siehe unten, § 5 B.II.

[792] Siehe oben, § 2 A.

[793] *Hanloser*, ZD 2018, 213 (213).

[794] *Hanloser*, ZD 2018, 213.

[795] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. 2002 L 201/37.

[796] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. No-

aa) Gesetzliche Grundlagen

Die gesetzlichen Grundlagen wurzeln daher im Unionsrecht und wurden durch das TMG in deutsches Recht (unzureichend) umgesetzt.

(1) Art. 5 Abs. 3 ePrivacy-Richtlinie

Die Nutzung von Tracking-Instrumenten ist in Art. 5 Abs. 3 ePrivacy-Richtlinie geregelt. In der Fassung von 2002 war hier nur ein Widerspruchsrecht der Nutzer vorgesehen. Durch die Neufassung im Jahr 2009 wurde die Vorschrift jedoch auf einen Einwilligungsvorbehalt umgestellt. Ihr erster Satz lautet nunmehr:

„Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie 95/46/EG u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat."

Diese Regelung der ePrivacy-Richtlinie beansprucht als *lex specialis* Vorrang vor der DSRL, sofern die Speicherung von Informationen auf einem Endgerät oder Zugang zu diesen betroffen sind. Ein Rückgriff auf Erlaubnistatbestände aus der DSRL, etwa das überwiegende Verarbeiterinteresse, verbietet sich daher.[797] *Zusätzlich* müssen die Vorgaben der (Umsetzung der) DSRL jedoch beachtet werden, wenn eine über den Zugriff auf Endgeräteinformationen hinausgehende Verarbeitung von so gewonnenen personenbezogenen Daten stattfindet.[798] Entscheidend für die Abgrenzung ist mithin der Begriff der Information, die auf einem Endgerät gespeichert ist. Grund für die gesonderte Regelung dieser Informationen ist der Eingriff in die Privatsphäre des Nutzers, die nach Vorstellung des Gesetzgebers nicht davon abhängt, ob die Informationen personenbezogene Daten darstellen oder nicht.[799] Wie gesehen, greifen Geräte-Identifier auf derartige Daten zu, um eine eindeutige Erkennung von Geräten vorzunehmen und unterfallen damit der Regelung von Art. 5 Abs. 3 S. 1 ePrivacy-Richtlinie.[800] Dabei gelten nicht nur Computer,

vember 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, ABl. 2009 L 337/11.

797 EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 89.

798 *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 17.

799 Siehe den 24. Erwägungsgrund der Richtlinie 2002/58/EG.

800 *Dieterich*, ZD 2015, 199 (200f.); *Article 29 Data Protection Working Party*, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, WP 224, 2014, 7,

sondern auch Smartphones und IoT-Geräte als Endgeräte im Sinne der Vorschrift.[801]

Sie trägt jedoch auch dem Umstand Rechnung, dass bestimmte Typen von Geräte-Identifiern (essenzielle Cookies) für die Funktionsfähigkeit einer Webseite oder App erforderlich sein können. Daher formuliert Art. 5 Abs. 3 S. 2 ePrivacy-Richtlinie:

„Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann."

Das Einwilligungserfordernis bezieht sich daher lediglich auf nicht-essenzielle Geräte-Identifier;[802] Marketing-Tools unterliegen immer einem Einwilligungsvorbehalt.[803] Hinsichtlich des Begriffs der Einwilligung verweist Art. 2 S. 2 lit. f ePrivacy-Richtlinie auf die Legaldefinition der DSRL. Damit wurde an sich ein einheitliches Einwilligungsregime für personenbezogene Daten nach der DSRL einerseits und für den Zugriff auf Endgerätdaten mittels Geräte-Identifiern andererseits eingeführt.

(2) Deutsches Recht

In Deutschland hat diese Vereinheitlichung jedoch schon in legislatorischer Perspektive keinen Niederschlag gefunden. Art. 5 Abs. 3 ePrivacy-Richtlinie wurde nach Ansicht der Bundesregierung umgesetzt in §§ 12 ff. TMG.[804] Die Vorgabe der ePrivacy-Richtlinie erfasst dabei ohne weitere Binnendifferenzierung personenbezogene und nicht personenbezogene Informationen auf dem Endgerät.[805] Die deutsche Umsetzung hingegen differenziert hier.[806] Für nicht personenbezogene Informationen gilt lediglich das Transparenzerfordernis

11; *Article 29 Data Protection Working Party*, Opinion 04/2012 on Cookie Consent Exemption, WP 194, 2012, 2; *Schmidt/Babilon*, K&R 2016, 86 (87).

[801] Zu letzteren siehe *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 16.

[802] Siehe auch den 25. Erwägungsgrund der Richtlinie 2002/58/EG; ferner *Article 29 Data Protection Working Party*, Opinion 04/2012 on Cookie Consent Exemption, WP 194, 2012, 4; *Kosta*, 21 International Journal of Law and Information Technology 2013, 380 (393); *Moos/Rothkegel*, MMR 2019, 736 (737).

[803] GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 54 Fn. 32; *Schmidt/Babilon*, K&R 2016, 86 (87).

[804] *Bundesregierung*, Questionnaire on the implementation of the Article 5(3) of the ePrivacy Directive, KommDok. COCOM11–20 vom 4.10.2011, 3 ff.; kritisch wegen mangelndem konkreten Umsetzungswillens *Rauer/Ettig*, ZD 2016, 423 (424); *Schmidt/Babilon*, K&R 2016, 86 (89); *Hanloser*, ZD 2018, 213 (214).

[805] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 70 f.; *Kosta*, 21 International Journal of Law and Information Technology 2013, 380 (386); *Hanloser*, ZD 2018, 213 (214).

[806] Dazu *Bundesregierung*, Questionnaire on the implementation of the Article 5(3) of the ePrivacy Directive, KommDok. COCOM11–20 vom 4.10.2011, 3 ff.

nach § 13 Abs. 1 S. 2 TMG.[807] Danach muss bei einem „automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet", der Nutzer zu Beginn des Verfahrens unterrichtet werden. Ein Einwilligungserfordernis ist hier jedoch nicht explizit vorgesehen. Für personenbezogene Daten hingegen gilt zwar ein grundsätzlicher Einwilligungsvorbehalt nach § 12 Abs. 1 TMG, der die Erhebung und Verwendung personenbezogener Daten zur Bereitstellung von Telemedien (jeglichen Onlinediensten) umfasst. Nach § 15 Abs. 3 S. 1 TMG darf der Anbieter jedoch ohne Einwilligung des Nutzers „für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien" pseudonyme[808] Nutzerprofile erstellen, die lediglich einem Widerspruchsrecht unterliegen, wie es die Fassung der ePrivacy-Richtlinie von 2002 vorgesehen hatte. Für diesen Fall und für nicht personenbezogene Daten sieht das deutsche Recht daher keinen ausdrücklichen Einwilligungsvorbehalt vor.[809] Auch § 12 Abs. 1 TMG greift jedoch erst, wenn personenbezogene Daten verarbeitet werden und noch nicht, bevor der Geräte-Identifier gesetzt oder erzeugt wird, wie es Art. 5 Abs. 3 ePrivacy-Richtlinie vorsieht.[810]

bb) Voraussetzungen der Cookie-Einwilligung

Aufgrund dieser verzweigten und defizitären Umsetzung war in Deutschland lange Zeit umstritten, ob überhaupt eine Einwilligung, und wenn ja in welcher Form, für die Verwendung von Geräte-Identifiern notwendig ist.

(1) Das Erfordernis aktiver und gesonderter Einwilligung

Obwohl das Einwilligungserfordernis bereits 2009 unionsrechtlich verankert wurde und die Umsetzungsfrist 2011 ablief, konnte sich die deutsche Rechtsprechung erst im Jahr 2017 zu einer Vorlage der Frage an den EuGH durchringen.[811]

(a) Rechtsprechung und Literatur bis 2019

Bis zur Entscheidung des EuGH in der Rechtssache *Planet49* im Jahr 2019 wurde eine aktive Einwilligung von der deutschen Rechtsprechung bei Geräte-Identifiern nicht verlangt.[812] Diese Auffassung fand immerhin eine gewisse Stütze im 66. Erwägungsgrund der Richtlinie 2009/136/EG. Dessen S. 3 spricht lediglich von einem Ablehnungsrecht. Nach S. 5 des 66. Erwägungsgrunds soll-

[807] *Hanloser*, ZD 2018, 213 (214).
[808] Zum Personenbezug pseudonymer Daten bereits oben, § 4 A.II.2.a)aa)(2).
[809] *Hanloser*, ZD 2018, 213 (214 f.); *Schmidt/Babilon*, K&R 2016, 86 (89).
[810] *Rauer/Ettig*, ZD 2016, 423 (424); *Hanloser*, ZD 2018, 213 (214 f.); vgl. auch *Kosta*, 21 International Journal of Law and Information Technology 2013, 380 (392 f.).
[811] BGH ZD 2018, 79.
[812] OLG Frankfurt a. M. MMR 2016, 245 (246 f.).

te die Einwilligung „über die Handhabung der entsprechenden Einstellungen eines Browsers oder einer anderen Anwendung ausgedrückt werden" können. Dies wurde teilweise so interpretiert, dass auch die Beibehaltung von cookiefreundlichen Browservoreinstellungen eine hinreichende Einwilligung darstellen sollte.[813] Allerdings formulierte auch der genannte fünfte Satz des 66. Erwägungsgrunds eindeutig, dass eine derartige Browserhandhabung nur dann eine wirksame Einwilligung darstellen kann, wenn sie „im Einklang mit den entsprechenden Bestimmungen der [DSRL]" erfolgt. Dies zeigt noch einmal, dass kein Sondereinwilligungsregime mit von der DSRL abweichenden Maßstäben durch die ePrivacy-Richtlinie in der Fassung von 2009 etabliert werden sollte.

(b) Die Rechtssache *Planet49*

So entschied denn auch der EuGH in der Rechtssache *Planet49*.[814] Dieses Unternehmen hatte ein Gewinnspiel veranstaltet und dabei auf die Setzung von Cookies auf dem Computer des Nutzers hingewiesen. Dieser Hinweistext[815] wiederum war mit einem vorangekreuzten Kästchen versehen, dessen Häkchen entfernt werden konnte.[816] In zeitlicher Hinsicht war jedenfalls für einen Teil des Sachverhalts die Rechtslage vor Geltungsbeginn der DS-GVO maßgeblich.[817] Der EuGH entschied, dass auch für diesen Zeitraum eine aktive Einwilligung in das Setzen eines Cookies notwendig ist nach Art. 2 lit. h DSRL i. V. m. Art. 5 Abs. 3, Art. 2 S. 2 lit. f ePrivacy-Richtlinie.[818] Diese kann jedoch nicht in der aktiven Eingabe von Informationen auf der Website (zum Beispiel Adresseingabe zur Teilnahme am Gewinnspiel oder Betätigung der Schaltfläche zur Teilnahme) gesehen werden, sondern muss gesondert, also von der inhaltlichen Nutzung der Webseite getrennt, abgegeben werden.[819] Solches kann etwa durch das aktive Setzen eines Häkchens,[820] nicht aber durch das Nicht-

[813] *Hanloser*, ZD 2018, 213 (215); dagegen überzeugend *Kosta*, 21 International Journal of Law and Information Technology 2013, 380 (397 f.).

[814] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*).

[815] Der Text lautete: „Ich bin einverstanden, dass der Webanalysedienst Remintrex bei mir eingesetzt wird. Das hat zur Folge, dass der Gewinnspielveranstalter, die Planet49 GmbH, nach Registrierung für das Gewinnspiel Cookies setzt, welches Planet49 eine Auswertung meines Surf- und Nutzungsverhaltens auf Websites von Werbepartnern und damit interessengerichtete Werbung durch Remintrex ermöglicht. Die Cookies kann ich jederzeit wieder löschen. Lesen Sie Näheres hier."

[816] GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 1.

[817] Vgl. EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 42.

[818] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 56 f., 65; siehe auch GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 60 f.

[819] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 58; GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 63–66, 89; zum Kriterium der gesonderten Einwilligung bereits oben, Text bei § 4, Fn. 458.

[820] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 49.

entfernen eines bereits vorangekreuzten Häkchens geschehen.[821] Damit ist evident, dass ein reines Widerspruchsrecht nicht den Anforderungen an eine Einwilligung genügt, genauso wenig wie die Möglichkeit eines Opt-Out. Letztlich werden damit die Anforderungen an die Unmissverständlichkeit der Einwilligung, welche die DS-GVO ausdrücklich eingeführt hat,[822] bereits für die Geltung der DSRL, und damit auch der ePrivacy-Richtlinie, implementiert.

(c) Folgen für das deutsche Recht

Damit ist zugleich klar, dass im deutschen Recht ein Umsetzungsdefizit bestand.[823] Dieses muss künftig, für Altfälle, für welche noch die ePrivacy-Richtlinie i. V. m. der DSRL maßgeblich ist, durch richtlinienkonforme Auslegung ausgeglichen werden.[824] Der Wortlaut der nationalen Norm bildet dafür nach herrschender Meinung keine feste Grenze.[825] Ferner erfasst die richtlinienkonforme Auslegung das gesamte nationale Recht[826] und damit auch Normen, die – wie die einschlägigen Paragraphen des TMG – vor Geltungsbeginn der Richtlinie erlassen wurden.[827] Hätte sich der BGH jedoch durch einen fehlenden konkreten Umsetzungswillen des Gesetzgebers an einer richtlinienkonformen Auslegung gehindert gesehen,[828] würde die BRD im Sinne der *Francovich*-Rechtsprechung geschädigten Nutzern aus Staatshaftungsrecht auf

[821] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 52; GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 88.

[822] Siehe oben, § 5 D.2.a)aa).

[823] So auch bereits zuvor *Schmitz*, in: Spindler/Schmitz/Liesching, TMG, 2. Aufl. 2018, § 15 Rn. 4–7, 95–98; *Dieterich*, ZD 2015, 199 (202); *Schmidt/Babilon*, K&R 2016, 86 (90); EuGH, Urt. v. 19.10.2016 – Rs. C-582/14 (*Breyer*) – Rn. 64; GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 109.

[824] Siehe dazu unten, Text bei § 5, Fn. 882 f.

[825] EuGH, Urt. v. 4.7.2006 – Rs. C-212/04 (*Adeneler*) – Rn. 110 f.; dies für das deutsche Recht umsetzend BGH NJW 2009, 427 Rn. 21 – Quelle; zur Problematik umfassend *Grundmann*, ZEuP 1996, 399 (408 ff.); *Canaris*, in: Festschrift Bydlinski, 2002, 47 (61, 91 ff.); *Herresthal*, Rechtsfortbildung im europarechtlichen Bezugsrahmen, 2006, 317 ff.; *Auer*, NJW 2007, 1106 (1108 f.).

[826] Siehe nur EuGH, Urt. v. 14.7.1994 – Rs. C-91/92 (*Faccini Dori*) – Rn. 26; Urt. v. 5.10.2004 – verb. Rs. C-397/01 bis C-403/01 (*Pfeiffer*) – Rn. 113–116. Dafür sind Unbedingtheit und hinreichende Bestimmtheit keine Voraussetzungen, EuGH, Urt. v. 10.4.1984 – Rs. 14/83 (*von Colson und Kamann*) – Rn. 26; siehe im Einzelnen *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 176; *Craig/de Búrca*, EU Law, 2015, 209 f.; *Streinz/W. Michl*, EuZW 2011, 384 (386); *Roth/Jopen*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 263 (271 Rn. 15).

[827] EuGH, Urt. v. 13.11.1990 – Rs. C-106/89 (*Marleasing*) – Rn. 8; *Everling*, ZGR 1992, 376 (378 f.); *Roth/Jopen*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 263 (288 Rn. 52); *Canaris*, in: Festschrift Bydlinski, 2002, 47 (73 f.).

[828] Diesen betonen für den konkreten Fall *Rauer/Ettig*, ZD 2016, 423 (424); *Schmidt/Babilon*, K&R 2016, 86 (89); *Hanloser*, ZD 2018, 213 (214); Wortlaut und *telos* der nationalen Norm als gemeinsame Grenze betonen auch *Canaris*, in: Festschrift Bydlinski, 2002, 47 (92); *Suhr*, Richtlinienkonforme Auslegung im Privatrecht und nationale Auslegungsmethodik, 2011, 241.

Schadensersatz haften.[829] Man durfte daher mit Spannung dem Urteil des BGH zur Umsetzung der EuGH-Entscheidung in Sachen *Planet49* entgegensehen. Der BGH entschied jedoch,[830] dass dem deutschen Gesetzgeber ein hinreichender Umsetzungswille unterstellt werden kann, da dieser die bestehende Rechtslage als richtlinienkonform eingestuft hatte. Auch der Wortlaut sei einer richtlinienkonformen Auslegung noch zugänglich. Ein Widerspruch im Sinne des § 15 Abs. 3 S. 1 TMG liege vor, wenn eine wirksame Einwilligung fehle. Das Bemühen des BGH, trotz der klar defizitären Formulierung der genannten Norm einen Staatshaftungsanspruch zu vermeiden, ist mit Händen zu greifen. In der Sache jedenfalls ist damit auch für deutsche Altfälle Rechtssicherheit geschaffen worden, auch wenn die Debatte über die methodische Zulässigkeit der richtlinienkonformen Auslegung in diesem Fall wohl anhalten wird.

(2) Informiertheit der Einwilligung

Die Informiertheit der Cookie-Einwilligung ist, wie die der allgemeinen Einwilligung bei Art. 4 Nr. 11 DS-GVO, eng mit den allgemeinen Informationspflichten bei Datenverarbeitungsvorgängen verknüpft, die für die DSRL in Art. 10 und 11 festgehalten sind. Nach Art. 5 Abs. 3 der ePrivacy-Richtlinie muss die Einwilligung auf der Grundlage von klaren und umfassenden Informationen erteilt werden. Wiederum ist hier auf einen Durchschnittsnutzer abzustellen,[831] von dem jedoch kein Vorverständnis hinsichtlich der Funktionsweise und der unterschiedlichen Typen von Cookies zu erwarten ist.[832] Daher muss unter der Geltung der ePrivacy-Richtlinie in Verbindung mit der DSRL, aber auch nach der DS-GVO,[833] sowohl über die Funktionsdauer der Cookies als auch über Zugriffsmöglichkeiten von Dritten und deren Identität klar und verständlich informiert werden.[834] Gleiches gilt für den Zeitraum, über den die durch die Cookies gesammelten Daten gespeichert werden.[835]

(3) Freiwilligkeit der Einwilligung

Schließlich ist wichtig zu sehen, dass die Regelungen der ePrivacy-Richtlinie, auch in Verbindung mit der DSRL, kein Art. 7 Abs. 4 DS-GVO vergleichbares Kopplungsverbot beinhalten. Auch das deutsche Recht kannte ein solches für

---

[829] EuGH, Urt. v. 19.11.1991 – verb. Rs. C-6/90 und C-9/90 (*Francovich*) – Rn. 44–46; Urt. v. 14.7.1994 – Rs. C-91/92 (*Faccini Dori*) – Rn. 29; Urt. v. 5.3.1996 – Rs. C-46/93 (*Brasserie du Pêcheur*) – Rn. 17 ff.

[830] BGH GRUR 2020, 891 Rn. 52–55 – Cookie-Einwilligung II.

[831] GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 113.

[832] GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 114.

[833] Vgl. EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 60.

[834] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 75–81; GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 117–120.

[835] GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 118.

Geräte-Identifier nicht. Die Einwilligung muss lediglich freiwillig sein. Dies wirft die Frage auf, ob Webseitenanbieter und App-Entwickler den Zugang zu ihren Produkten von der Einwilligung in das Setzen von Cookies oder die Verwendung anderer Geräte-Identifier abhängig machen können (sog. *tracking wall*). Die Antwort ist für die ePrivacy-Richtlinie i. V. m. der DSRL umstritten;[836] letztlich dürfte die Frage aber *de lege lata* zu bejahen sein, sofern nicht Produkte der Daseinsvorsorge oder der Kern der Ausübung von Grundrechten betroffen ist.[837] Dies zeigt insbesondere der letzte Satz des 25. Erwägungsgrunds der ursprünglichen Fassung der ePrivacy-Richtlinie.[838] Umso bedeutsamer ist die Frage, ob mit Geltungsbeginn der DS-GVO diese abschließend die Einwilligung in Geräte-Identifier regelt oder weiterhin auf die ePrivacy-Richtlinie i. V. m. der DSRL zurückgegriffen werden kann. Dem widmet sich der folgende Abschnitt.

b) Maßgeblichkeit der DS-GVO bis zum Inkrafttreten der ePrivacy-VO

Die ursprüngliche Planung auf europäischer Ebene sah vor, die DS-GVO zeitgleich mit der ePrivacy-VO in Kraft treten zu lassen.[839] Da jedoch die Kompromisssuche bei der ePrivacy-VO erheblich mehr Zeit in Anspruch nahm, wurde die DS-GVO vorweg verabschiedet und erlangt am 23. Mai 2018 Geltung, ohne dass auch nur das Trilogverfahren zur ePrivacy-VO begonnen worden wäre. Damit stellt sich für die Zeit zwischen dem Inkrafttreten der DS-GVO und dem Inkrafttreten der ePrivacy-VO die Frage, nach welchen Regeln sich die Einwilligung in Cookies und andere Geräte-Identifier richtet. Denkbar ist einerseits eine Fortgeltung der alten Regelungen nach der ePrivacy-Richtlinie und ihrer nationalen Umsetzung sowie andererseits eine Behandlung der Cookie-Einwilligung nach dem Regime der DS-GVO.

---

[836] Für eine Unfreiwilligkeit im Fall von *tracking walls Kosta*, 21 International Journal of Law and Information Technology 2013, 380 (396); dagegen *Article 29 Data Protection Working Party*, Working Document 02/2013 providing guidance on obtaining consent for cookies, WP 208, 2013, 5.

[837] Im Ergebnis ähnlich *Zuiderveen Borgesius et al.*, 3 European Data Protection Law Review 2017, 1 (8).

[838] *Article 29 Data Protection Working Party*, Working Document 02/2013 providing guidance on obtaining consent for cookies, WP 208, 2013, 5. Der betreffende Satz lautet: „Der Zugriff auf spezifische Website-Inhalte kann nach wie vor davon abhängig gemacht werden, dass ein Cookie oder ein ähnliches Instrument von einer in Kenntnis der Sachlage gegebenen Einwilligung abhängig gemacht wird, wenn der Einsatz zu einem rechtmäßigen Zweck erfolgt."

[839] Art. 29 Abs. 2 des Kommissionsentwurfs zur ePrivacy-Verordnung: *Europäische Kommission*, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, COM(2017) 10 final.

aa) Die DS-GVO als Maßstab für Einwilligungen

Die DS-GVO selbst enthält eine Regelung dieser Frage in Art. 95, dessen Gehalt jedoch in der Literatur umstritten ist.[840] Danach erlegt die DS-GVO

„natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen".

Damit wird ein Vorrang der Altregelungen vor den verschärften Anforderungen der DS-GVO insoweit statuiert, als in der ePrivacy-Richtlinie besondere Pflichten aufgestellt wurden und diese dasselbe Ziel wie die Regelungen der DS-GVO verfolgen. Unter Berufung auf Art. 95 DS-GVO hat der BGH nunmehr auch die Fortgeltung von § 15 Abs. 3 S. 1 TMG als Umsetzung von Art. 5 Abs. 3 S. 1 der ePrivacy-Richtlinie angeordnet.[841]

(1) Anwendbarkeit der DS-GVO

Nach hier vertretener Auffassung fehlt es jedoch bereits an einer besonderen Regelung der Cookie-Einwilligung in der ePrivacy-Richtlinie.[842] Zwar enthält, wie gesehen, Art. 5 Abs. 3 ePrivacy-Richtlinie spezifische Vorgaben für die Zulässigkeit von Cookies und anderen Tracking-Tools, die auf dem Endgerät des Nutzers installiert werden oder Informationen von dort abrufen. Allerdings verweist bereits die Ursprungsfassung von Art. 5 Abs. 3 ePrivacy-Richtlinie hinsichtlich der Informationspflichten unmittelbar auf die DSRL. Selbiges gilt für die Einwilligung nach Art. 2 S. 2 lit. f ePrivacy-Richtlinie. Allenfalls könnte argumentiert werden, dass Art. 5 Abs. 3 ePrivacy-Richtlinie in der Ursprungsfassung von 2002 gar keine Einwilligung als Voraussetzung für die Erhebung von Daten mittels eines Cookies forderte, sondern lediglich ein qualitativ von einer Einwilligung verschiedenes Ablehnungsrecht statuierte.

Entscheidend jedoch ist, dass, wie gesehen, die Richtlinie 2009/136/EG den Art. 5 Abs. 3 der ePrivacy-Richtlinie abgeändert hat und nunmehr in S. 1 ausdrücklich eine Einwilligung des Betroffenen für Cookies und andere Tracking Tools gefordert ist. Ausgenommen sind, wie gesehen, lediglich Konstellationen der alleinigen Übertragung einer Nachricht in einem Kommunikationsnetz-

[840] Für eine Weitergeltung der ePrivacy-Richtlinie und deren Umsetzungsnormen etwa *Hanloser*, ZD 2019, 264 (265); *Hanloser*, ZD 2018, 213 (217); für eine Geltung der DS-GVO GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 77; *Kühling/Raab*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 95 DS-GVO Rn. 7; *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 95 DS-GVO Rn. 18.

[841] BGH GRUR 2020, 891 Rn. 60 – Cookie-Einwilligung II.

[842] So auch GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 77; *Kühling/Raab*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 95 DS-GVO Rn. 7; *Karg*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 95 DS-GVO Rn. 18.

werk oder der unbedingten Erforderlichkeit der Datenerhebung für die Zurverfügungstellung des Dienstes. Weiterhin verweist der unveränderte Art. 2 S. 2 lit. f der ePrivacy-Richtlinie auf die Einwilligung nach der DSRL. Auch der 66. Erwägungsgrund von Richtlinie 2009/136/EG benennt nun klar die Notwendigkeit einer Einwilligung, ohne jedoch dafür gesonderte, vom allgemeinen Datenschutzrecht verschiedene Maßstäbe aufzustellen. Nach Art. 94 Abs. 2 S. 1 DS-GVO gilt der Verweis auf die Bestimmungen der DSRL als Verweis auf die Bestimmungen der DS-GVO.[843] Da jedoch die Richtlinie 2009/136/EG die ePrivacy-Richtlinie lediglich abänderte, und nicht ersetzte, bezieht sich die Vorrangregelung in Art. 95 DS-GVO auf die jeweils geltende Fassung der ePrivacy-Richtlinie, die wiederum in Art. 2 S. 2 lit. f i. V. m. Art. 94 Abs. 2 S. 1 DS-GVO auf das nunmehr geltende Einwilligungserfordernis nach der DS-GVO verweist. Damit findet sich in der ePrivacy-Richtlinie richtigerweise schon kein von der DS-GVO abweichendes Einwilligungsregime für Cookies.

Sofern man entgegen dem deutschen Wortlaut Art. 95 DS-GVO so liest, dass sich die Regelung auf abweichendes mitgliedstaatliches Umsetzungsrecht bezieht,[844] liegt auch keine deutsche abweichende Regelung mit selber Zielsetzung vor: § 12 Abs. 1 TMG weicht mangels spezifischen Einwilligungsregimes nicht ab,[845] und die bloße Information nach § 13 Abs. 1 S. 2 TMG und das Widerspruchsrecht, das in § 15 Abs. 3 S. 1 TMG verortet ist, haben, sofern man die Regelungen nicht ohnehin richtlinienkonform auslegt (dazu oben, § 4 B.I.4.a) bb)(1)(c)), nicht dieselbe Zielsetzung wie die Einwilligung nach Art. 4 Nr. 11 DS-GVO.[846] Denn durch die Aufnahme des neuen Kriteriums der Unmissverständlichkeit soll gerade die aktive Beteiligung des Nutzers an der Datenerhebung auf privatautonomer Basis gefördert und eingefordert werden. Dies steht in diametralem Gegensatz zu einer rein passiven Hinnahme der Implantierung eines Tracking-Tools. Wie verhaltensökonomische Studien belegen, wird das Wahlverhalten von betroffenen Personen typischerweise erheblich dadurch beeinflusst, welche Voreinstellung (Zulässigkeit oder Unzulässigkeit der Datenerhebung) gewählt wird (*default*-Effekt/*status quo bias*).[847] Bei der Frage, ob ein aktives Tun notwendig ist oder eine passive Hinnahme reicht, handelt es sich daher nicht um ein marginales Detail, sondern eine der zentralen Weichen-

[843] Dies erkennt auch der BGH an, siehe BGH GRUR 2020, 891 Rn. 29, 63 – Cookie-Einwilligung II; dazu genauer im übernächsten Absatz.

[844] Dazu *Hanloser*, ZD 2018, 213 (216 Fn. 40); so auch *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, 3; aA die Nachweise in § 4, Fn. 842.

[845] *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, 4.

[846] *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, 6; aA wohl *Hanloser*, ZD 2018, 213 (217); *Gierschmann*, ZD 2018, 297 (299).

[847] Siehe *Hacker*, Verhaltensökonomik und Normativität, 2017, 85 f.; *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 264 ff.; *Baumgartner/Gausling*, ZD 2017, 308 (312); *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (9).

stellungen eines auf Datensouveränität ausgerichteten Einwilligungsregimes. Der Wechsel von Einwilligungsvorbehalt zu Widerspruchsrecht bringt mithin eine echte Zielverschiebung mit sich, welche den Vorrang der Regelungen der ePrivacy-RL nach Art. 95 DS-GVO entfallen ließe, sofern man weiterhin auf einem bloßen Widerspruchsrecht nach dem TMG beharren wollte.

Im Ergebnis hat sich dem auch der BGH angeschlossen. Bereits in seine EuGH-Vorlage vom Oktober 2017 zur Cookie-Einwilligung hatte er eine Frage zur Behandlung von Opt-Out-Einwilligungen nach Art. 6 Abs. 1 lit. a DS-GVO aufgenommen.[848] Dies konnte jedoch nur dann entscheidungserheblich und damit vorlagefähig sein, wenn das Einwilligungsregime der DS-GVO auch tatsächlich bis zur Geltung der ePrivacy-VO auf die Cookie-Einwilligung anwendbar ist. Dies hat implizit, wenngleich ohne Berücksichtigung von Art. 95 DS-GVO, auch GA *Szpunar* so gesehen.[849] Der EuGH hat sich zu der Frage nicht ausdrücklich verhalten, aber jedenfalls klargestellt, dass zumindest über den Verweis in Art. 2 S. 2 lit. f. der ePrivacy-RL auf die Cookie-Einwilligung die Einwilligungsregeln der DS-GVO Anwendung finden, da Verweise auf die DSRL nach Art. 94 Abs. 2 DS-GVO nunmehr als Verweise auf die DS-GVO zu lesen sind.[850] Dieser Lesart hat sich der BGH angeschlossen.[851]

(2) Konsequenzen (*tracking walls*)

Konsequenz dieser Rechtslage ist, dass, wie bereits in den Ausführungen zur Einwilligung nach der DS-GVO zugrunde gelegt,[852] die Einwilligung in die Nutzung von Geräte-Identifiern nunmehr allen Anforderungen der DS-GVO entsprechen muss.[853] Dies betrifft insbesondere das Kriterium der Unmissverständlichkeit, sodass stets eine aktive Einwilligung erforderlich ist. Ferner ist damit auch das Kopplungsverbot des Art. 7 Abs. 4 DS-GVO anwendbar, sodass *tracking walls*, sofern sie für die Vertragsdurchführung nicht essenzielle Cookies betreffen, grundsätzlich eine Einwilligung unwirksam machen,[854] es sei denn, es besteht ein funktional äquivalentes Angebot am Markt ohne *tracking wall*.[855]

bb) Rückgriff auf andere Erlaubnistatbestände der DS-GVO

Zuletzt lässt sich danach fragen, ob der Vorrang der revidierten Fassung der ePrivacy-Richtlinie insoweit erhalten bleibt, als, von den Ausnahmen in Art. 5 Abs. 3 S. 2 der revidierten ePrivacy-Richtlinie abgesehen, Art. 5 Abs. 3 S. 1 der

[848] BGH ZD 2018, 79 Rn. 13 – Cookie-Einwilligung.
[849] GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 47, 93.
[850] EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 42, 60 ff.
[851] BGH GRUR 2020, 891 Rn. 29, 63 – Cookie-Einwilligung II.
[852] Siehe oben, § 5 D.I.3.
[853] So im Ergebnis auch *Weidert/Klar*, BB 2017, 1858 (1860, 1862).
[854] So *Zuiderveen Borgesius et al.*, 3 European Data Protection Law Review 2017, 1 (9).
[855] Siehe im Einzelnen oben, § 4 B.I.3.a)dd)(3) und (5)(b).

revidierten ePrivacy-Richtlinie die Einwilligung zum alleinigen Erlaubnistatbestand erhebt. Art. 5 Abs. 3 S. 1 der revidierten ePrivacy-Richtlinie kennt, ebenso wenig wie die deutsche Umsetzung, eine Parallele zu Art. 6 Abs. 1 lit. b-f DS-GVO. Dies hätte zur Folge, dass bei Nichtvorliegen einer Einwilligung eine Datenerhebung und -verarbeitung nur nach Art. 5 Abs. 3 S. 2 der revidierten ePrivacy-Richtlinie erlaubt sein könnte, ein Rückgriff auf Art. 6 Abs. 1 lit. b-f DS-GVO jedoch gesperrt wäre. Damit wären ohne Einwilligung lediglich reine Nachrichtenübertragungen in Kommunikationsnetzwerken sowie das Setzen essenzieller Cookies möglich, nicht aber die Nutzung von Cookies oder anderer Tracking-Tools zu Marketingzwecken.

Jedenfalls grundsätzlich steht jedoch Art. 95 DS-GVO, der das Verhältnis von ePrivacy-Richtlinie zur DS-GVO regelt, einer Anwendung der gesetzlichen Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO nicht im Weg. Denn deren Einschlägigkeit neben der Einwilligung erlegt den Verantwortlichen keine weiteren Pflichten i. S. d. Art. 95 DS-GVO auf; vielmehr werden diese dadurch begünstigt. Insbesondere über die Interessensabwägungsklausel von Art. 6 Abs. 1 lit. f DS-GVO soll letztlich ein angemessener, schonender Ausgleich der verschiedenen beteiligten Interessen ermöglicht werden, ein Ziel, das jedenfalls in dieser Form in der revidierten Fassung von Art. 5 Abs. 3 ePrivacy-Richtlinie nicht greifbar wird.[856] Daher ist nach hier vertretener Auffassung das gesamte Erlaubnisregime von Art. 5 Abs. 3 ePrivacy-Richtlinie durch Art. 6 Abs. 1 DS-GVO abgelöst worden,[857] auch wenn die Wertungen von Art. 5 Abs. 3 weiter zu berücksichtigen sind (s. S. 281).

Für nicht personenbezogene Daten müssen die Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO dann konsequenterweise analog gelten (und kann nicht etwa Art. 5 Abs. 3 ePrivacy-Richtlinie fortgelten[858]), da sonst (eine korrekte Umsetzung von Art. 5 Abs. 3 ePrivacy-Richtlinie vorausgesetzt) eine Verarbeitung personenbezogener Daten leichter möglich wäre als jene nicht personenbezogener Daten.

c) Ausblick: Die Regelung der ePrivacy-VO

Die Reform der ePrivacy-Regelungen steht in der Wahrnehmung der Öffentlichkeit im Schatten der bereits vollzogenen DS-GVO-Reform. Dabei werden mit der neuen ePrivacy-Verordnung die Weichen für große Teile der digita-

---

856 Im Ergebnis ebenso *Hanloser*, ZD 2018, 213 (217).

857 *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, 7 ff.

858 So aber *Hanloser*, ZD 2018, 213 (215 f.). Dies kann jedoch nur für das deutsche Recht überzeugen, da hier die Vorschriften von Art. 5 Abs. 3 ePrivacy-Richtlinie bei nicht personenbezogenen Daten gerade nicht umgesetzt wurden und insofern eine strengere Regelung von nicht personenbezogenen Daten entfällt. Auf europäischer Ebene jedoch, die für Art. 95 DS-GVO maßgeblich ist, ist die deutsche Rechtslage nach hiesiger Auffassung irrelevant.

len Wirtschaft möglicherweise neu gestellt.[859] Denn die dort als *lex specialis*[860] zur DS-GVO angedachten Regelungen haben potenziell weitreichende Folgen für große Teile des digitalen Datenaustauschs. Der neue Kerntatbestand für Tracking-Technologien, Art. 8 Abs. 1 des Kommissionsentwurfs der ePrivacy-Verordnung (ePrivacy-VO-KommE[861]), gilt für

„[j]ede vom betreffenden Endnutzer nicht selbst vorgenommene Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer, auch über deren Software und Hardware".

Damit sind einerseits klar jegliche Formen von Geräte-Identifiern, auch technisch komplexere Formen von *fingerprinting*, erfasst.[862] Diese stellen jedoch den Nukleus der Datenerhebung im digitalen Austausch dar: *first-party* und *third-party tracking*, auf denen weite Teile der personalisierten Werbung basieren. Nicht erfasst sind im Onlinebereich lediglich aktive Nutzertätigkeiten (zum Beispiel ein spezifischer Like auf Facebook), wobei die passive Messung dieser Nutzertätigkeit, wenn sie über das Endgerät des Nutzers erfolgt, wiederum unter die ePrivacy-Verordnung fällt. Hinzu kommt, dass unter die genannten Endeinrichtungen der Nutzer auch IoT-Geräte fallen.[863] Auch *tracking*-Formen über WLAN- oder Bluetooth Signale (*beacons*[864]) werden geregelt (Art. 8 Abs. 2 ePrivacy-VO-KommE).[865] Damit wird die ePrivacy-Verordnung zu einem zentralen Instrument der Regulierung gegenwärtiger und künftiger Formen des Datenaustauschs im Onlinebereich und Internet der Dinge.

Bislang liegt neben dem Kommissionsentwurf von 2017 auch die Stellungnahme des Europäischen Parlaments aus demselben Jahr vor (ePrivacy-VO-EP[866]). Insgesamt zeichnen sich dabei drei zentrale Reformvorhaben ab,[867]

---

[859] *Engeler/Felber*, ZD 2017, 251 (251).

[860] *Engeler/Felber*, ZD 2017, 251 (253), auch zu Konkurrenzproblemen.

[861] *Europäische Kommission*, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, COM(2017) 10 final; siehe dazu etwa die umfassende Stellungnahme *Article 29 Data Protection Working Party*, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 2017; ferner *Engeler/Felber*, ZD 2017, 251; *Maier/Schaller*, ZD 2017, 373.

[862] 20. Erwägungsgrund ePrivacy-VO-KommE.

[863] 12. Erwägungsgrund ePrivacy-VO-KommE.

[864] Siehe dazu oben, § 3, Fn. 181.

[865] Dazu mit Recht kritisch hinsichtlich der Details *Engeler/Felber*, ZD 2017, 251 (255 f.).

[866] Europäisches Parlament, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, A8–0324/2017, vom 20.10.2017.

[867] Zur hier nicht thematischen Regelung von Kommunikationsdaten in der ePrivacy-Verordnng, die eventuell auch Metadaten aus dem Internet der Dinge erfassen werden, siehe *Heun/Assion*, BB 2018, 579 (583); zur Rechtslage vor deren Geltungsbeginn *Heun/Assion*, CR 2015, 812 (815 f.).

deren endgültige Verabschiedung zwar noch nicht abschließend abgesehen werden kann, die hier jedoch kurz vorgestellt werden sollen: erstens eine spezifische Regelung der Einwilligung durch Browsereinstellungen; zweitens eine zwingend in Software vorzuhaltende Möglichkeit der Deaktivierung von *third-party tracking*; und schließlich drittens ein Recht auf die Nutzung von Onlinediensten ohne *tracking walls*.

aa) Einwilligung durch Browsereinstellungen, Art. 9 Abs. 2 ePrivacy-VO-KommE

Nach Art. 8 Abs. 1 lit. b. ePrivacy-VO-KommE stellt die wirksame Einwilligung weiterhin einen Erlaubnistatbestand für die Verwendung von Geräte-Identifiern dar. Hinsichtlich der Voraussetzungen der Einwilligung verweist Art. 9 Abs. 1 ePrivacy-VO-KommE zwar auf die DS-GVO, Art. 9 Abs. 2 ePrivacy-VO-KommE regelt jedoch spezifisch, dass eine Einwilligung „in den passenden technischen Einstellungen einer Software, die den Zugang zum Internet ermöglicht, gegeben werden" kann. Damit soll die Notwendigkeit obsolet werden, bei jeder einzelnen Webseite stets auf Neue eine spezifische Einwilligung in bestimmte Formen von Cookies oder anderen Geräte-Identifiern zu erteilen. Dieser Vorschlag ist daher an sich zu begrüßen. Er muss jedoch gekoppelt werden mit einem sinnvollen Regime der verständlichen und einfach navigierbaren Möglichkeit, diese Browsereinstellungen auch vorzunehmen.[868] Unklar bleibt ferner, ob die passive Hinnahme der Voreinstellungen eine wirksame Einwilligung darstellen kann.[869] Zudem rückt damit die Frage der Ausrichtung der Voreinstellungen (*tracking* oder *privacy by default*) in den Mittelpunkt.[870] Dies steht im Zentrum der zweiten wichtigen Reformvorschrift.

bb) Möglichkeit der Verhinderung von *third-party tracking*, Art. 10 ePrivacy-VO-KommE

Einerseits soll nach dem neuen Art. 8 Abs. 1 lit. d ePrivacy-VO-KommE die Messung des Webpublikums durch den Anbieter von Onlinediensten (und damit ein Teil von *first-party analytics*: die Webanalyse und die Reichweitenmessung[871]) einwilligungsunabhängig ermöglicht werden.[872] Schärfer geregelt wird im Kommissionsentwurf andererseits *third-party tracking*. Art. 10 Abs. 1

[868] Vgl. *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (4) (57 % der populärsten Webseiten der EU steuern Nutzer durch ihr Design aktiv zu datenschutzfeindlichen Optionen); *Forbrukerrådet*, Deceived by Design, Bericht, 2018, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf; *Conti/Sobiesk*, Proceedings of the 19th International Conference on World Wide Web 2010, 271.

[869] Siehe zum Parallelproblem des Widerspruchs durch Voreinstellungen insoweit noch unten, § 6 C.I.3.c)aa)(3).

[870] Zu *privacy by default* noch eingehend unten, § 6 E.III.

[871] Zu den Begriffen *Schleipfer*, ZD 2017, 460 (461).

[872] Dazu *Schleipfer*, ZD 2017, 460 (464).

ePrivacy-VO-KommE implementiert eine zwingend in Software bereitzuhaltende Möglichkeit, *third-party tracking* zu verhindern. Dies betrifft jegliche elektronische Kommunikationssoftware und damit insbesondere auch Internetbrowser oder Messengerplattformen (OTT-Dienste),[873] aber auch die Software für IoT-Geräte.[874] Abs. 2 enthält dann die Verpflichtung, dem Nutzer bei der Installation eine Wahl hinsichtlich der Einstellung abzuverlangen. Allerdings muss diese Wahl nach dem Wortlaut nicht notwendig „auf einem weißen Blatt" erfolgen, sondern kann auch in einer Bestätigung einer Voreinstellung liegen. Die verhaltensökonomische Literatur zu *default*-Effekten[875] suggeriert dabei jedoch, dass die spezifische Form der Voreinstellung, die im Kommissionsentwurf nicht geregelt ist, entscheidende Bedeutung haben wird. Wenn alle Kategorien von Cookies vorangekreuzt sind, akzeptieren nach einer Studie (aus dem Jahr 2018/19) 83 % der Nutzer alle Kategorien; wenn keine Kategorie vorangekreuzt ist, nur 0,2 %.[876] Eine andere Auswertung aus dem Jahr 2019 kommt auf 99 % Akzeptanz bei Vorselektion gegenüber knapp 6 % Akzeptanz bei mangelnder Vorselektion.[877]

Die Stellungnahme des Europäischen Parlaments fordert daher richtigerweise eine Implementierung von *privacy by default* (Art. 10 Abs. 1 lit. a ePrivacy-VO-EP) und dies nicht lediglich mit Blick auf *third*, sondern auch auf *first-party tracking*,[878] was dem Gedanken von Art. 25 Abs. 2 DS-GVO entspricht.[879] Danach muss die Voreinstellung nicht funktional essenzielles *tracking* verhindern. Nach der Installation der Software soll der Nutzer nach dem Parlamentsvorschlag aufgefordert werden, die Voreinstellungen zu bestätigen

---

[873] *Europäische Kommission*, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, COM(2017) 10 final, 2; kritisch zur begrifflichen Unklarheit *Engeler/Felber*, ZD 2017, 251 (254).

[874] 12. Erwägungsgrund ePrivacy-VO-KommE.

[875] Siehe dazu *Hacker*, Verhaltensökonomik und Normativität, 2017, 85 f.; *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 264 ff.; *Baumgartner/Gausling*, ZD 2017, 308 (312); *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (9).

[876] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (10).

[877] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (10).

[878] Die Reichweite von Art. 8 Abs. 1 lit. d ePrivacy-VO-KommE wird daher in der Stellungnahme des Parlaments auch erheblich eingeschränkt auf die Reichweitenmessung im öffentlichen Interesse.

[879] Europäisches Parlament, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, A8–0324/2017, vom 20.10.2017, 102; *Article 29 Data Protection Working Party*, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 2017, 14; *Engeler/Felber*, ZD 2017, 251 (256); *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 56.

oder zu ändern (Art. 10 Abs. 1 lit. b ePrivacy-VO-EP). Die gewählten Voreinstellungen sollen dann für alle anderen Parteien (die Verantwortlichen) bindend sein (Art. 10 Abs. 1a UAbs. 1 ePrivacy-VO-EP). An nicht umfänglicher Bindungswirkung kranken heutige *do not track*-Einstellungen in der Tat gerade.[880] Zugleich muss die Software es jedoch dem Nutzer ermöglichen, seine gewählten Voreinstellungen hinsichtlich einzelner Onlinedienste durch ausdrückliche Einwilligung abzuändern (*override*, Art. 10 Abs. 1b ePrivacy-VO-EP). Angesichts der erwähnten *default*-Effekte und des zentralen Grundsatzes von *privacy by default*[881] stellt dieser Vorschlag ein sinnvoll abgestimmtes Regime aus datenschutzfreundlicher Voreinstellung, Möglichkeit der Abänderung generell sowie des Opt-Out aus den Voreinstellungen im Einzelfall dar.

cc) Regelung von *tracking walls*, Art. 8 Abs. 1a ePrivacy-VO-EP

Noch weiter in Richtung effektivem Datenschutz und Stärkung von Wahlfreiheit der Nutzer geht das Parlament in seiner Stellungnahme mit Art. 8 Abs. 1a ePrivacy-VO-EP. Darin enthalten ist ein striktes Kopplungsverbot:

„Unabhängig davon, ob es sich um einen vergüteten Dienst handelt, darf keinem Nutzer der Zugang zu einem Dienst oder einem Funktionselement der Informationsgesellschaft mit der Begründung verweigert werden, er habe seine Einwilligung in die Verarbeitung personenbezogener Daten bzw. in die zur Bereitstellung dieses Dienstes oder dieses Funktionselements nicht erforderliche Nutzung von Verarbeitungs- oder Speicherkapazitäten seiner Endeinrichtung nach Artikel 8 Absatz 1 Buchstabe b nicht gegeben."

Das Kopplungsverbot hat zwei Anknüpfungspunkte. Erstens kann der Zugang zu Onlinediensten gar nicht von der Einwilligung in die Verarbeitung personenbezogener Daten abhängig gemacht werden. Dies geht über Art. 7 Abs. 4 DS-GVO hinsichtlich der Rechtsfolge hinaus, da hier nicht lediglich eine Vermutung für die Unfreiwilligkeit der Einwilligung, sondern ein striktes Zugangsrecht installiert wird. Insbesondere marktbezogene Faktoren, etwa das Vorhandensein funktional äquivalenter Dienste, wären dann irrelevant. Die Verarbeitung könnte dementsprechend, sofern eine Einwilligung nicht erteilt wird, nur nach Art. 6 Abs. 1 lit. b-f DS-GVO legitimiert werden. Die Verarbeitung von personenbezogenen Daten für personalisierte Werbung wäre daher, sofern mit der hier vertretenen Auffassung eine Erfassung durch Art. 6 Abs. 1 lit. b und f DS-GVO grundsätzlich abgelehnt wird, nicht mehr möglich, wenn

[880] Siehe dazu im Einzelnen unten, § 6 C.I.3.c)aa)(2); ferner zur mangelnden Bindungswirkung *Libert*, Proceedings of the 2018 World Wide Web Conference, 207 (213); *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 9; Europäisches Parlament, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, A8–0324/2017, vom 20.10.2017, 102; *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (421).

[881] Dazu im Einzelnen unten, § 4 C.III.

der Nutzer seine Einwilligung verweigert. Anders als nach dem Kopplungsregime der DS-GVO hätte der Nutzer aber dennoch einen Anspruch auf die Nutzung des Dienstes.

Zweitens gilt dieselbe Zugangslogik für nicht essenzielle Geräte-Identifier, unabhängig davon, ob diese personenbezogene Daten darstellen oder nicht. Dies würde das Ende von *tracking walls* bedeuten:[882] Nutzer müssten auf Onlinedienste oder IoT-Geräte zugreifen können, auch wenn eine Einwilligung in die Nutzung von nicht essenziellen Geräte-Identifiern nicht erteilt wird.[883] Problematisch wird dann zwar, inwieweit erforderliche von nicht erforderlichen Geräte-Identifiern abgegrenzt werden können.[884] Allerdings wird diese Auswahlmöglichkeit von einigen Diensten bereits jetzt in der Praxis vorgehalten, die es ermöglichen, Marketing- und Performance-Cookies gezielt auszuschalten:[885] Laut einer Studie, welche im August 2018 die populärsten Webseiten der EU untersuchte (n > 5000), ermöglichten die Webseiten in zwar geringer, aber nicht völlig vernachlässigbarer Proportion (8,5 %) das Blockieren von spezifischen Kategorien von Cookies.[886] Insofern ist nicht ersichtlich, dass hier keine pragmatische und technisch umsetzbare Lösung erzielt werden kann. Jedenfalls hinsichtlich klarerweise im Schwerpunkt auf Marketing ausgerichteter Tracking-Tools (z. B. Google Analytics,[887] Google Ads,[888] *fingerprinting* oder Werbe-IDs) wird man die funktionale Erforderlichkeit unproblematisch verneinen können. Sofern sich Zweifelsfälle häufen, muss der Weg notfalls über eine technische Standardisierung gegangen werden.[889]

Die betroffenen Personen hätten damit ein echtes Wahlrecht zwischen einer Nutzung der Dienste mit oder ohne nicht vertrags-/funktionserforderliche Daten. Zugleich würde es Anbietern erlauben, bei Verweigerung der Einwilligung einen monetären Preis zu verlangen. Die Regelung würde damit einen erheblichen Schritt in Richtung eines Rechts auf eine datenschonende Alterna-

---

[882] Europäisches Parlament, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, A8–0324/2017, vom 20.10.2017, 102.

[883] Dafür auch *Article 29 Data Protection Working Party*, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, 2017, 15.

[884] Darauf weisen zu Recht *Engeler/Felber*, ZD 2017, 251 (255); *Engeler*, ZD 2018, 55 (61) hin.

[885] So z. B. von www.doodle.com (zuletzt abgerufen am 4.9.2019); von der mobilen Version der Webseite https://de.flightaware.com (zuletzt abgerufen am 20.8.2019); von https://www.axa.com/en/cookies (zuletzt abgerufen am 13.11.2019).

[886] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (6): 434 von 5087 Webseiten; siehe auch die Auswertung einer Stichprobe, ebd., 4.

[887] Siehe https://marketingplatform.google.com/intl/de/about/analytics/ (zuletzt abgerufen am 8.8.2019).

[888] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (7).

[889] *Engeler/Felber*, ZD 2017, 251 (255 Fn. 48).

tive für die Nutzung von Onlinediensten, auch im Rahmen des IoT, darstellen. Dies wäre, wie unten im Einzelnen erläutert wird, ein erheblicher Fortschritt für die wirksame Wahrnehmung von Privatautonomie im digitalen Umfeld.[890] Insgesamt zeigt sich damit an den Diskussionen um die ePrivacy-Verordnung die Möglichkeit von Technikgestaltung durch Recht in besonderer Schärfe.

5. Eine kurze Kritik der Einwilligung

Die Reformbemühungen der ePrivacy-Verordnung sind jedoch noch nicht Realität, und es ist unklar, ob sie es jemals sein werden. Die bestehenden Regelungen der Einwilligung nach der DS-GVO (und vergleichbaren oder schwächeren Regimen) hingegen stoßen weithin auf berechtigte Kritik.[891] Da diese bereits vielerorts beschrieben wurde, soll hier ein knapper Überblick genügen, der zeigt, warum das Einwilligungsregime der DS-GVO die gerade im Bereich des Datenprivatrechts so zentrale wirksame Inanspruchnahme materieller Privatautonomie nicht verbürgen kann (a)). Allein auf diesen positiven Regelungsbestand kann ein Datenermöglichungsrecht daher nicht gegründet werden.

Dennoch wäre es verfrüht, die Einwilligung vollkommen *ad acta* zu legen. Denn einerseits liefern die auf sie bezogenen Datenschutzerklärungen wertvolle Hinweise für den Markt und darauf aktive Informationsintermediäre (b)). Andererseits kann eine *technologische Einwilligung*, die durch Techniken maschinellen Lernens auf Seiten der Einwilligenden unterstützt wird, im Verbund mit spezifischen regulatorischen Strukturen womöglich den Schlüssel zu einer so weit als möglich gewährleisteten informationellen Selbstbestimmung in hochvernetzten Kontexten wie dem *Internet of Everything* darstellen. Daraus erwachsen zugleich Reformbedürfnisse, die im Einzelnen später, in § 6 C., aufgegriffen werden.[892]

a) Mangelnder direkter Nutzen für Betroffene

Zunächst ist jedoch zu konstatieren, dass der individuelle Nutzen des bestehenden Einwilligungsregimes für Betroffene aufgrund der bereits diskutierten Phänomene rationaler Ignoranz und verhaltensökonomischer Effekte äußerst begrenzt ist. Das Ziel, über die Einwilligung Kontrolle und Datensouveränität

---

[890] Siehe unten, § 6 C.II.

[891] *Richards/Hartzog*, 96 Washington University Law Review 2019, 1461 (1476 ff.); *Efroni et al.*, 5 European Data Protection Law Review 2019, 352 (355 ff.); *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (448–451); *Koops*, 4 International Data Privacy Law 2014, 250 (251 f.); *Blume*, 2 International Data Privacy Law 2012, 26 (29); *Zuiderveen Borgesius*, 13 IEEE Security & Privacy 2015, 103; *Zuiderveen Borgesius*, Improving Privacy Protection in the Area of Behavioural Targeting, 2015, Kapitel 7; *Lynskey*, The Foundations of EU Data Protection Law, 2015, 229 ff.; *Calo*, 87 Notre Dame Law Review 2012, 1027 (1050 ff.); *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 227 ff.; *Hacker*, 7 International Data Privacy Law 266 (274); siehe auch die Nachweise unten in § 6, Fn. 195.

[892] Siehe unten, § 6 C.I.3.

herzustellen,[893] wird damit in der Praxis, wenngleich nicht immer, so doch zumeist verfehlt.

aa) Rationale Ignoranz

Neuere Studien zeigen übereinstimmend, dass Datenschutzerklärungen, welche die informatorische Grundlage für Einwilligungen abgeben, von fast allen Nutzern vollständig ignoriert werden, selbst wenn die Erklärungen hinsichtlich Lesbarkeit und Übersichtlichkeit nach den gegenwärtigen *best practices* optimiert werden.[894] Wie bereits erläutert, hat dies häufig rationale Gründe, da der Erwartungsnutzen unter dem Erwartungsaufwand für die Lektüre und die kognitive Verarbeitung der Informationen liegt.[895] Neben der Länge der Erklärungen[896] und ihrer wenig nutzerfreundlichen Zugänglichkeit[897] liegt dies auch daran, dass Datenschutzerklärungen in der EU zumeist, nach gängigen Metriken, für Laien kaum lesbar sind.[898] Dies verstößt zwar gegen das Verständlichkeitsgebot in Art. 12 Abs. 1 S. 1 DS-GVO, ist jedoch bislang gängige Marktpraxis und schon aufgrund der Vielzahl der nach Art. 4 Nr. 11 und Art. 13 f. DS-GVO erforderlichen Informationen nur schwer zu korrigieren.[899]

Ein Ansatz zur Überwindung derartiger rationaler Ignoranz findet sich daher in Formen verpflichtender aktiver Wahl (*required active choosing*),[900] wie sie in Art. 10 Abs. 2 ePrivacy-VO-KommE im Nukleus angelegt ist. Sie zwingen die Betroffenen dazu, sich (jedenfalls kursorisch) mit einer Entscheidung über Privatsphäreeinstellungen zu beschäftigen. Dies kann jedoch nur dann fruchten, wenn die Entscheidung auch hinreichend informiert ist.

bb) Verhaltensökonomische Effekte

Allerdings beeinträchtigen Informationsüberlastung[901] sowie eine Reihe von weiteren verhaltensökonomischen Effekten, wie dargelegt, die rationale Information von Nutzern und ihre Entscheidung über die Abgabe einer Einwil-

[893] Vgl. den 7. Erwägungsgrund der DS-GVO.

[894] Nachweise oben in § 3, Fn. 80.

[895] Vgl. *McDonald/Cranor*, 4 I/O Journal of Law and Policy for the Information Society 2008, 543.

[896] *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (449).

[897] *Forbrukerrådet*, Deceived by Design, Bericht, 2018, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[898] Empirische Studie bei *Becher/Benoliel*, in: Mathis/Tor (Hrsg.), Consumer Law & Economics, 2020, (im Escheinen); siehe ferner *Policy and Research Group of the Office of the Privacy Commissioner of Canada*, Consent and privacy – A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act, 2016, 11 f.; *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (448).

[899] Zu *multi-layered notices* unten, § 6 C.I.1.a)aa)(2).

[900] Zu diesem aus der verhaltensökonomischen Theorie stammenden Instrument ausführlich *Hacker*, Verhaltensökonomik und Normativität, 2017, 488 ff.

[901] Siehe oben, Text bei § 3, Fn. 69.

ligungserklärung.[902] Dies steht in diametralem Gegensatz zur Annahme eines durchschnittlich informierten, situationsadäquat aufmerksamen und verständigen Durchschnittsnutzers, der in Anlehnung an das (zumindest tendenziell) rationale Verbraucherleitbild[903] auf unionaler Ebene propagiert wird.[904]

Eine verhaltensökonomische Perspektive verdeutlicht demgegenüber einmal mehr die Wichtigkeit von Voreinstellungen, wie sie wiederum Art. 10 ePrivacy-VO-EP in den Blick nimmt. Insofern ist es zu begrüßen, dass die DS-GVO mit dem Kriterium der Unmissverständlichkeit[905] und Art. 25 Abs. 2 DS-GVO[906] die Weichen nun klar gegen datenschutzfeindliche Voreinstellungen als Grundlage der Einwilligung gestellt hat. Nichtsdestoweniger bleiben die weiteren verhaltensökonomischen Effekte wie Informationsüberlastung, Risikofehleinschätzungen und Präsenzeffekte (*present bias*) relevant. Nimmt man rationale Ignoranz hinzu, so ist daher festzustellen, dass auf Grundlage der DS-GVO die eigenverantwortliche und informierte Ausübung von Privatautonomie durch eine Einwilligung weitestgehend eine Illusion bleibt.

cc) Faktische Grenzen der Einwilligung im IoT-Kontext

Dies gilt verschärft, wie bereits erwähnt,[907] für den Kontext des Internets der Dinge. Hier ist es gerade hinsichtlich der Erhebung und Verarbeitung von Daten Dritter, mit denen kein primäres Nutzungsverhältnis hinsichtlich des Geräts besteht, faktisch kaum möglich, vor dem Kontakt mit dem IoT-Gerät eine informierte und unmissverständliche Einwilligung einzuholen. Der Fokus verschiebt sich in diesen Konstellationen klar auf die Ordnungsstrukturen des Datenschutzrechts. Die privatautonome Gestaltungsfähigkeit gelangt an eine Grenze, wenn sich die Einwilligung nicht für neue Erscheinungsformen, etwa eine technologische Einwilligung für vernetzte Umgebungen, öffnet.[908]

b) Nutzen für Informationsintermediäre

Dennoch ist nicht in Abrede zu stellen, dass die Einwilligung und die damit verbundenen Informationspflichten aus Art. 12 ff. DS-GVO einen residualen Nutzen, wenn schon nicht unmittelbar für die typischen betroffenen Personen, so doch für Dritte und damit indirekt auch für Nutzer haben.[909] Dies wird bei

---

[902] Siehe oben, § 3, Fn. 84.

[903] Dazu etwa *Klinck/Riesenhuber* (Hrsg.), Verbraucherleitbilder: interdisziplinäre und europäische Perspektiven, 2015; *Hacker*, 11 European Review of Contract Law 2015, 299 (311 ff.).

[904] GA *Szpunar*, Schlussanträge v. 21.3.2019 – Rs. C-673/17 (*Planet49*) – Rn. 113.

[905] Siehe oben, § 4 B.I.3.a)aa).

[906] Siehe unten, § 4 C.III.

[907] Siehe oben, Text bei § 4, Fn. 477 und 519.

[908] Dazu unten, § 6 C.I.3.

[909] Vgl. *Helberger/Zuiderveen Borgesius/Reyna*, 54 Common Market Law Review 2017, 1427 (1442).

der generellen Kritik von Einwilligung und Pflichtinformationen häufig übersehen. Denn die am Markt befindlichen Informationen ermöglichen es Informationsintermediären wie Privacy Watchdogs, Analysten, Wissenschaftlern und Datenschutzbehörden, die Datenverarbeitung durch Anbieter zu einem gewissen Maße nachzuvollziehen und auf Rechtmäßigkeit zu überprüfen.[910]

Ein ganz ähnlicher Effekt ist aus dem Kapitalmarktrecht bekannt, wo die für private Durchschnittsanleger häufig zu komplexen Pflichtinformationen[911] ebenfalls die Grundlage für professionelle Analysen und Aufbereitungen darstellen, die dann wiederum von den Durchschnittsanlegern oder ihren Anlageberatern rezipiert werden können.[912]

Dieser Umstand spricht entscheidend dafür, die Einwilligung als Rechtsinstitut in rechtspolitischer Hinsicht nicht vollständig aufzugeben, sie aber kontinuierlich mit Blick auch auf diese Zielrichtung zu verbessern und als Instrument gegen Marktversagen auf individueller Ebene mit anderen Mitteln sinnvoll zu ergänzen (dazu im Einzelnen § 6 C. und § 7 B.I.).[913]

6. Zusammenfassung zur Einwilligung

Durch die DS-GVO wurden die Anforderungen an die Einwilligung gegenüber der DSRL noch einmal verschärft. Insbesondere die explizite Aufnahme des Kriteriums der Unmissverständlichkeit in Art. 4 Nr. 11 DS-GVO und das neu eingeführte Kopplungsverbot in Art. 7 Abs. 4 DS-GVO sorgen dafür, dass eine wirksame Einwilligung in der Praxis nicht mehr leicht zu erlangen ist. So hat die Analyse gezeigt, dass in allen drei Leitfällen die Einwilligung häufig an einer ihrer Voraussetzungen scheitert.

(1) Die Datenweiterleitung an Dritte umfasst sowohl die Nutzung von personenbezogenen Daten für personalisierte Werbung im Rahmen des Geschäftsmodells mit Daten als Gegenleistung als auch die zwischen verschiedenen Akteuren aufgeteilte Datenverarbeitung im Internet der Dinge. Bezüglich personalisierter Werbung sind einerseits die Informationen hinsichtlich der Partner, an welche die Daten zu diesem Zweck weitergeleitet werden, häufig nicht hinreichend präzise; andererseits greift grundsätzlich das Kopplungsverbot, wenn nicht funktionsäquivalente Angebote ohne diesbezügliche Einwil-

---

[910] Siehe etwa die Untersuchungen bei *Bischhoff*, Comparing the privacy policy of internet giants side-by-side, comparitech (20.3.2017), https://www.comparitech.com/blog/vpn-privacy/we-compared-the-privacy-policies-of-internet-giants-side-by-side/; *Forbrukerrådet*, Deceived by Design, Bericht, 2018, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf; *Becher/Benoliel*, in: Mathis/Tor (Hrsg.), Consumer Law & Economics, 2020, (im Escheinen); *McDonald/Cranor*, 4 I/O Journal of Law and Policy for the Information Society 2008, 543.

[911] Dazu etwa *Hacker*, Verhaltensökonomik und Normativität, 2017, 423 und § 12.

[912] Umfassend *Leyens*, Informationsintermediäre des Kapitalmarkts, 2017, 47 ff.; ferner *Schwarcz*, 61 UCLA Law Review 2014, 394 (409); *Merkt*, zfbf Sonderheft 55/06, 24 (29 f.).

[913] Ebenso *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (452).

ligung am Markt bestehen. Dies gilt ebenso für das Internet der Dinge, wobei hier die Datenweiterleitung gegenüber dem Primärnutzer in der Regel insoweit auf eine wirksame Einwilligung gestützt werden kann, als die Verarbeitung außerhalb des Endgeräts selbst funktional erforderlich ist. Auch hier muss jedoch auf präzise Informationen geachtet werden, die allerdings jedenfalls grundsätzlich gegenüber dem Primärnutzer des Geräts durchaus vor der ersten Nutzung erteilt werden können.

(2) Die Datenerhebung durch Dritte vollzieht sich vor allem im Wege des *third-party tracking*. Eine diesbezügliche Einwilligung muss jedenfalls nach der DS-GVO, in der Sache nach aber auch für Altfälle nach der ePrivacy-Richtlinie (in der Interpretation der Rechtssache *Planet49*), unmissverständlich erteilt werden, woran es häufig mangelt. Ferner werden hier häufig Informationspflichten verletzt. Schließlich greift das Koppelungsverbot, sofern *tracking walls* bei Nichtakzeptanz nicht essenzieller Cookies oder anderer Geräte-Identifier den Zugriff auf Dienste verhindern.

(3) Auch die im Rahmen des Internets der Dinge vermehrt auftretende Datenerhebung bei Dritten lässt sich kaum über ein Einwilligungsmodell lösen. Schon aus faktischen Gründen wird es hier häufig an der Möglichkeit, hinreichende Informationen bereitzustellen, fehlen. Zudem haben Dritte zumeist weder eine Gelegenheit noch ein Interesse daran, in stark vernetzten Umgebungen in hoher Frequenz unmissverständliche Einwilligungserklärungen abzugeben.

In rechtlicher Hinsicht liegt eine mögliche Lösung für Verantwortliche darin, die Anwendbarkeit des Kopplungsverbots durch eine monetär finanzierte datenschonende Alternative auszuhebeln. Ferner können Verträge so gestaltet werden, dass die Datenverarbeitung vertragserforderlich wird. Bei Zugrundelegung eines subjektiven Erforderlichkeitsmaßstabs scheidet die Anwendbarkeit des Kopplungsverbots dann aus. Umso bedeutender wird zugleich eine Wirksamkeitskontrolle der betreffenden Vertragsklauseln im Rahmen des allgemeinen Zivilrechts. Auch sonst bestehen erhebliche Verschränkungen zwischen dem Einwilligungstatbestand und dem allgemeinen Zivilrecht, insbesondere hinsichtlich der Folgen eines Widerrufs und der noch eigens zu besprechenden allgemeinen Wirksamkeitsvoraussetzungen der Einwilligung nach dem BGB.

Der Blick auf die reale Ausübung der Einwilligung zeigt jedoch, dass ihre schwindende rechtliche Bedeutung als wirksames datenschutzrechtliches Legitimationsinstrument einhergeht mit einem empirischen Bedeutungsverlust, der auch durch die DS-GVO bislang nicht aufgehalten werden konnte. Für die betroffenen Personen hat sie einen deutlich limitierten Nutzen in reellen Entscheidungssituationen, da auch unter Geltung der DS-GVO rationale Ignoranz infolge langer und komplexer Datenschutzerklärungen sowie verhaltensökonomische Beschränkungen an der Tagesordnung sind. Die mit der

Einwilligung einhergehenden Informationspflichten entfalten daher vor allem einen indirekten Nutzen für Informationsintermediäre, weshalb auf die Einwilligung als Rechtsinstrument in rechtspolitischer Hinsicht nicht verzichtet werden sollte. Nichtsdestoweniger zeigen gerade die Schwierigkeiten der Kompatibilisierung des Einwilligungsmodells mit dem Internet der Dinge, dass das in der DS-GVO angelegte Modell privatautonomer Gestaltungsmacht und einwilligungsbasierter Datensouveränität zunehmend an faktische Grenzen stößt. Dies macht deutlich, dass zur Förderung der privatautonomen Gestaltung der digitalen Lebenswelt jedenfalls in Teilen neue Wege, hin zu einer technologischen Einwilligung, beschritten werden müssen (siehe § 6, besonders § 6 C.I.3 und § 6 C.II.). Nur so lässt sich ein effektives Datenermöglichungsrecht schaffen.

II. Vertragserforderliche Datenverarbeitung, Art. 6 Abs. 1 lit. b DS-GVO

Eine weitere, auf privatautonomer Gestaltung basierende Möglichkeit der rechtmäßigen Datenverarbeitung sieht Art. 6 Abs. 1 lit. b DS-GVO vor. Es wird sich jedoch zeigen, dass hier ebenfalls signifikante rechtliche und faktische Grenzen für die Legitimation der Datenverarbeitung bestehen.

1. Ermöglichungs- bzw. Permissivitätscharakter

Dem Erlaubnistatbestand in Art. 6 Abs. 1 lit. b DS-GVO wohnt ein Ermöglichungscharakter inne, der dem der Einwilligung durchaus verwandt, mit ihm aber nicht identisch ist. Im Rahmen der allgemeinen Grenzen der Privatautonomie sind die Parteien frei, ihre Verträge zu gestalten und damit die Voraussetzungen für Art. 6 Abs. 1 lit. b DS-GVO zu schaffen. Insofern ließe sich von der „Permissivität" dieser Regelung sprechen:[914] Sie kann von den Parteien privatautonom auch zur Gestaltung der datenschutzrechtlichen Erlaubniswirkung genutzt werden, ohne zugleich aktiv die Wahrnehmung von Privatautonomie unterstützend zu fördern.

Allerdings bezieht sich die privatautonome Regelung, im Gegensatz zur Einwilligung, ohnehin stets nur indirekt auf die Datenverarbeitung. Vielmehr muss die betroffene Person den Schluss von der Vereinbarung vertraglicher Pflichten auf die Erlaubnis diesbezüglicher Datenverarbeitung selbst tätigen. Inwiefern diese Ableitung der datenschutzrechtlichen Erlaubnis aus einer beliebigen Vertragspflicht unmittelbar gilt, ist zudem wie im Rahmen des Kopplungsverbots des Art. 7 Abs. 4 DS-GVO umstritten.[915] Dabei ist klar, dass ein wie auch immer geartetes objektives, vom subjektiven Parteiwillen abstrahier-

[914] Ich danke Herrn Professor *Stefan Grundmann* für diese Anregung.
[915] Siehe unten, § 4 B.II.2.b)bb).

tes Verständnis der Vertragserforderlichkeit sowohl die privatautonomen Gestaltungsmöglichkeiten der Parteien mit Blick auf die Datenverarbeitung als auch die Deduzierbarkeit der erlaubten Datenverarbeitung aus dem vertraglichen Regelwerk für den einzelnen Nutzer erheblich reduziert.[916] Schließlich ist zu beachten, dass im Kontext sensitiver Daten eine Art. 6 Abs. 1 lit. b DS-GVO vergleichbare Regelung in Art. 9 Abs. 2 DS-GVO fehlt, so dass auch insofern der vertragsautonomen Gestaltung der Datenverarbeitung Grenzen gesetzt sind.

Anders als die datenschutzrechtliche Einwilligung unterliegt jedoch der Abschluss des eine Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO legitimierenden Vertrags keinen spezifischen, in der DS-GVO vorgehaltenen Voraussetzungen, welche die strengen Anforderungen von Art. 4 Nr. 11 DS-GVO spiegeln würden. Dies impliziert zugleich, dass die genuine *Förderung* privatautonomer Gestaltungsmacht, die zumindest, wie dargestellt, auch ein Zielpunkt der Wirksamkeitsvoraussetzungen der Einwilligung ist,[917] im Rahmen der vertragserforderlichen Datenverarbeitung nur sehr reduziert durch das Datenschutzrecht selbst geleistet wird. Vielmehr muss insofern auf die Ermöglichungsstrukturen des allgemeinen Privatrechts rekurriert werden, die Art. 6 Abs. 1 lit. b DS-GVO als Scharniernorm, über das Erfordernis der Wirksamkeit des Vertrags,[918] gleichermaßen ins Datenschutzrecht importiert. Lediglich die Informationspflichten aus Art. 12 ff. DS-GVO, die ohne Weiteres auch die Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO erfassen, bieten mit Blick auf die vertragserforderliche Datenverarbeitung Ansatzpunkte für eine echte Förderung informierter Entscheidungen im Rahmen der DS-GVO – auch wenn sie in diesem Kontext hinsichtlich ihrer tatsächlichen Effektivität denselben empirischen Bedenken wie im Rahmen der Einwilligung ausgesetzt sind.[919]

2. *Tatbestand*

Art. 6 Abs. 1 lit. b DS-GVO erlaubt die Datenverarbeitung, wenn sie für eine von zwei Tatbestandsalternativen erforderlich ist: für die Erfüllung eines Vertrags mit der betroffenen Person oder für die Durchführung vorvertraglicher Maßnahmen auf Anfrage dieser Person. Die zweite Tatbestandsalternative soll Vorgänge erfassen, bei denen die betroffene Person vor dem Vertragsabschluss die Initiative ergreift und personenbezogenen Daten überlässt, etwa um zu testen, ob ein Produkt an ihrem Wohnsitz lieferbar ist.[920] Dass die Initiative für vorvertragliche Maßnahmen vom Nutzer ausgeht, wird jedoch eher selten der

[916] Vgl. auch *Sattler*, in: Ochs et al. (Hrsg.), Die Zukunft der Datenökonomie, 2019, 1 (18).
[917] Siehe oben, § 4 B.I.1.
[918] Siehe unten, § 4 B.II.2.a).
[919] Siehe oben, § 4 B.I.5. sowie unten, § 4 B.II.4.
[920] *European Data Protection Board*, Guidelines 2/2019 on the processing of personal

Fall sein. Im Zentrum der Fragestellung, welche Rahmenbedingungen Art. 6 Abs. 1 lit. b DS-GVO für die drei Leitfälle bereithält, steht mithin die erste Alternative, die Erforderlichkeit für die Erfüllung eines Vertrags mit der betroffenen Person.

a) Zivilrechtliche Wirksamkeit des Vertrags

Ungeschriebenes Tatbestandsmerkmal von Art. 6 Abs. 1 lit. b DS-GVO ist zunächst die zivilrechtliche Wirksamkeit des Vertrags.[921] Denn wenn der Vertrag unwirksam ist, besteht auch kein legitimes Interesse des Anbieters an der Datenverarbeitung. Insofern kommt Art. 6 Abs. 1 lit. b DS-GVO der Charakter einer Scharniernorm zwischen dem Datenschutzrecht und dem allgemeinen Zivilrecht zu. Insbesondere dann, wenn wie hier ein subjektiver Erforderlichkeitsmaßstab gewählt wird, sind die Wirksamkeitsvoraussetzungen nach dem BGB von entscheidender Bedeutung (siehe dazu eingehend § 5 B.III.).[922]

b) Erforderlichkeit

Ist der Vertrag wirksam abgeschlossen, so muss die Datenverarbeitung für die hier besonders interessierende erste Tatbestandsvariante von Art. 6 Abs. 1 lit. b DS-GVO dem Wortlaut zufolge also für die Erfüllung des Vertrags erforderlich sein.

aa) Vertragserfüllung

Die Erforderlichkeit selbst bezieht sich nach dem Wortlaut von Art. 6 Abs. 1 lit. b DS-GVO lediglich auf die Vertragserfüllung und nicht den Vertragsabschluss oder die Vertragsbeendigung. Dass der Vertragsabschluss nicht pauschal erfasst sein kann, zeigt die zweite Tatbestandsalternative von Art. 6 Abs. 1 lit. b DS-GVO, wonach vorvertragliche Maßnahmen nur dann legitimierende Wirkung entfalten, wenn sie von der betroffenen Person selbst angefordert wurden.[923]

---

data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8.10.2019, 13 Example 5.

[921] *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3749); *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8.10.2019, Rn. 26; *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 31; *Indenhuck/Britz*, BB 2019, 1091 (1093); *Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder*, Bericht vom 15. Mai 2017, 2017, 218.

[922] Ebenso *Indenhuck/Britz*, BB 2019, 1091 (1093 f.).

[923] So im Ergebnis auch *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8.10.2019, Rn. 38; der weitergehende 44. Erwägungsgrund der DS-GVO kann angesichts des klaren Wortlauts von Art. 6 Abs. 1 lit. b DS-GVO

Damit stellt sich vor allem die Frage, inwiefern Scoring-Tätigkeiten (z. B. Bonitätsprüfungen) im vorvertraglichen Bereich nach Art. 6 Abs. 1 lit. b DS-GVO gerechtfertigt werden können. Richtigerweise dürften schon der klare Wortlaut und der Vergleich mit der zweiten Tatbestandsalternative einer Öffnung für vorvertragliches Scoring entgegenstehen. Insbesondere wäre dies auch mit dem Zweck der Regelung, den Parteien Möglichkeiten zur *gemeinsamen* privatautonomen Gestaltung ihrer Rechtsverhältnisse und indirekt der Datenverarbeitung zu geben,[924] nicht vereinbar.[925] Denn sofern das Scoring nicht von der betroffenen Person selbst angefordert wird – was die Rechtfertigung nach der zweiten Tatbestandsalternative nach sich zöge[926] –, findet es auch hinsichtlich des „Ob" außerhalb des Einflussbereichs der betroffenen Person statt. Soweit eine Rechtsverpflichtung zur Durchführung von Scoring besteht (§ 505a BGB), ist jedoch Art. 6 Abs. 1 lit. c DS-GVO einschlägig.

Der deutsche Gesetzgeber hat lediglich für den Beschäftigtendatenschutz spezifische Regelungen dahingehend erlassen, dass hier eine Datenverarbeitung erlaubt ist, die für die Vertragsanbahnung, die Vertragsdurchführung oder die Vertragsbeendigung erforderlich ist (§ 26 Abs. 1 S. 1 BDSG). Daher kann ein hier ein Scoring in gewissen Grenzen erlaubt sein.[927]

bb) Erforderlichkeitsmaßstab

Wie bei Art. 7 Abs. 4 DS-GVO ist auch im Rahmen von Art. 6 Abs. 1 lit. b DS-GVO der Erforderlichkeitsmaßstab umstritten.

(1) Subjektiver Erforderlichkeitsmaßstab

Auch hier werden die drei bereits beim Kopplungsverbot angesprochenen Lesarten vertreten: eine ökonomische, eine objektive und eine subjektive Variante des Erforderlichkeitsmaßstabs.[928] Mit denselben Argumenten wie oben erscheint auch hier der subjektive Erforderlichkeitsmaßstab letztlich vor-

keine Berücksichtigung finden; aA *Albers/Veit*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2019, Art. 6 DS-GVO Rn. 31.

[924] *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 26.

[925] *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO Rn. 42; aA *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 47.

[926] *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 35.

[927] Im Einzelnen *Betz*, ZD 2019, 148 (149 ff.).

[928] Siehe oben, § 5 D.I.3.a)dd)(3)(a)(bb); die objektive Variante fordert eine teleologische Reduktion von Art. 6 Abs. 1 lit. b DS-GVO, wenn die Verarbeitung der Befriedigung eines über die zentrale Vertragserfüllung hinausgehenden kommerziellen Interesses des Verantwortlichen dient, siehe *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3747); ähnlich *Graf von Westphalen/Wendehorst*, BB 2016, 2179 (2185); dem folgend *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 40.

zugswürdig, da er am klarsten dem Wortlaut entspricht, am besten operationalisierbar ist und auch die privatautonome Gestaltungsmacht der Parteien am stärksten zur Geltung bringt. Abzulehnen ist insbesondere auch die Unanwendbarkeit von Art. 6 Abs. 1 lit. b DS-GVO bei einseitig gestellten Vertragsbedingungen,[929] da dies jeglichen normativen Anhaltspunkts in der DS-GVO entbehrt.

(2) Relevanz von Nutzerpflichten?

Dies wirft jedoch wiederum die Folgefrage auf, inwiefern die Erfüllung von Pflichten der betroffenen Person legitimierend wirken kann.[930] Hier wäre es zumindest denkbar, anders als bei Art. 7 Abs. 4 DS-GVO die Nutzerpflichten zu berücksichtigen, da der bei Art. 7 Abs. 4 DS-GVO enthaltene explizite Verweis auf die Erbringung einer Dienstleistung bei Art. 6 Abs. 1 lit. b DS-GVO fehlt. Nach hier vertretener Auffassung entfaltet diese Differenz jedoch nur klarstellende Wirkung für Art. 7 Abs. 4 DS-GVO; hätten abweichend von Art. 7 Abs. 4 DS-GVO bei Art. 6 Abs. 1 lit. b DS-GVO auch Nutzerpflichten Berücksichtigung finden sollen, so wäre vielmehr im Rahmen dieser Norm ein Hinweis auf derartige Verpflichtungen zu erwarten gewesen. Letztlich spricht daher die semantische Identität und die systematische Nähe der beiden Formulierungen entscheidend für eine einheitliche Auslegung,[931] sodass Nutzerpflichten auch im Rahmen von Art. 6 Abs. 1 lit. b DS-GVO keine Erlaubniswirkung entfalten. Diese Fokussierung auf die Pflichten des Verarbeiters findet sich im Übrigen auch in Art. 3 Abs. 1 UAbs. 2 DIDD-Richtlinie.

3. Konsequenzen für das Verhältnis zu Art. 7 Abs. 4 DS-GVO und für die drei Leitfälle

Damit gelten für die drei Leitfälle die gleichen Beschränkungen wie unter dem Kopplungsverbot: Lediglich dann, wenn die Datenweiterleitung oder das *third-party tracking* der Erfüllung von wirksam zwischen der betroffenen Person und dem Verantwortlichen vereinbarten Vertragspflichten dient, greift der Erlaubnistatbestand des Art. 6 Abs. 1 lit. b DS-GVO. Anders als bei der Wirksamkeit der Einwilligung nach dem Kopplungsverbot ist es jedoch bei Art. 6 Abs. 1 lit. b DS-GVO irrelevant, ob funktionsäquivalente Angebote am Markt bestehen. Ferner verhilft auch der Umstand, dass die Vertragserfüllung nicht von der dafür nicht erforderlichen Datenverarbeitung abhängig gemacht wird,

[929] So aber *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, 2014, 21 f.; *Artikel-29-Datenschutzgruppe*, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, WP 259 rev. 1, 2018, 14; dem folgend Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 668 ff.

[930] Dazu eingehend oben, Text bei § 4, Fn. 599.

[931] Siehe bereits oben, Text bei § 4, Fn. 530.

Art. 6 Abs. 1 lit. b DS-GVO nicht zur Einschlägigkeit. Dessen rechtliche Grenzen sind insofern enger gezogen als jene der Einwilligung nach dem Kopplungsverbot. Andererseits kann Art. 6 Abs. 1 lit. b DS-GVO auch dann Wirkung entfalten, wenn eine zusätzlich eingeholte Einwilligung aufgrund anderer Wirksamkeitsmängel nichtig ist, verweigert oder widerrufen wird.[932] Hier behält dieser Erlaubnistatbestand seine gegenüber der Einwilligung eigenständige Funktion.

Für den ersten und zweiten Leitfall lässt sich jedoch festhalten, dass, sofern keine ausdrücklichen Verpflichtungen des Verantwortlichen zur Personalisierung von Produkt oder Werbung festgehalten werden, zu diesem Zweck betriebene Datenweiterleitung oder erfolgtes Tracking nicht unter Art. 6 Abs. 1 lit. b DS-GVO fallen. Hinsichtlich der Datenerhebung bei unbeteiligten Dritten, etwa im IoT-Kontext, kommt Art. 6 Abs. 1 lit. b DS-GVO schon deshalb tatbestandlich nicht in Betracht, weil hier kein Vertragsverhältnis mit dem Anbieter des IoT-Geräts besteht.[933] Allenfalls bei bewusster, bestimmungsgemäßer Nutzung des Geräts durch nicht primär Nutzungsberechtigte kann ein Vertragsverhältnis mit legitimierenden Pflichten der Anbieter entstehen.[934]

4. Eine kurze Kritik der vertragserforderlichen Datenverarbeitung

Aus empirischer Warte treten jedoch im Rahmen der vertragserforderlichen Datenverarbeitung ganz ähnliche Probleme wie bei der Einwilligung auf, die den Nutzen dieses Erlaubnistatbestands für die wirksame Ausübung von Privatautonomie durch die betroffenen Personen grundlegend infrage stellen. Denn einerseits machen rationale Ignoranz und verhaltensökonomische Effekte vor Vertragsbedingungen keinen Halt. Eine Studie ergab vielmehr, dass lediglich etwa einer von 1000 Internetnutzern die Nutzungsbedingungen von im Internet verfügbarer Software, und damit die vertragliche Grundlage der Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO, zur Kenntnis nahm.[935] Wie bei der Einwilligung ist die Veröffentlichung der Nutzungsbedingungen daher im Ergebnis lediglich für Analysten und andere Informationsintermediäre, aber natürlich auch die Gerichte im Rahmen der Klauselkontrolle, förderlich, wovon freilich indirekt auch die Nutzer profitieren.[936] Dies zeigt zugleich, dass wie auch im Rahmen von Art. 7 Abs. 4 DS-GVO[937] der zivilrechtlichen Kontrolle der Vertragsbedingungen im Wege der positivrechtlichen Grenzen der Privatautonomie gesteigerte Bedeutung zukommt.[938] Denn wie

[932] Zur Möglicheit des Rückgriffs auf andere Tatbestände bei Widerruf der Einwilligung oben, Text bei § 4, Fn. 639.
[933] *Steege*, MMR 2019, 509 (511).
[934] Dazu im Einzelnen unten, § 5 B.III.2.b)aa).
[935] *Bakos/Marotta-Wurgler/Trossen*, 43 The Journal of Legal Studies 2014, 1.
[936] Siehe zu diesem Befund im Rahmen der Einwilligung oben, § 4 B.I.5.b).
[937] Siehe oben, Text bei § 4, Fn. 546.
[938] Siehe unten, § 5 C.II.

erwähnt enthält die DS-GVO selbst praktisch keine wirksamen Schutzmechanismen gegen die Auferlegung unangemessener Vertragsbedingungen und die Verarbeitung von personenbezogenen Daten auf deren Grundlage nach Art. 6 Abs. 1 lit. b DS-GVO.[939]

Andererseits ist, wie gesehen, die vertragliche Bindung bei Dritten, zu denen kein Vertragsverhältnis besteht und auch keine vertragliche Bindung beabsichtigt ist (Nicht-Primärnutzer von IoT-Geräten), in der Regel kein geeignetes Instrument für privatautonome Gestaltung.[940] Dies macht neue Möglichkeiten der wirksamen Inanspruchnahme materieller Privatautonomie im digitalen Umfeld nur umso dringlicher.[941]

III. Datenübertragung, Art. 20 DS-GVO

Mit dem Recht auf Datenübertragung gemäß Art. 20 DS-GVO wurde schließlich ein neuer Eckpfeiler für die Ermöglichung der Ausübung von Privatautonomie im digitalen Kontext geschaffen. Ziel ist die Erhöhung der Kontrolle der Nutzer über die eigenen Daten bei automatischer Verarbeitung.[942] Komplementär dazu statuiert nunmehr auch Art. 16 Abs. 4 DIDD-Richtlinie ein (limitiertes) Portabilitätsrecht hinsichtlich nicht personenbezogener Daten, „welche vom Verbraucher bei der Nutzung der vom Unternehmer bereitgestellten digitalen Inhalte oder digitalen Dienstleistungen bereitgestellt oder erstellt wurden".[943] Allerdings sind diese Rechte vor allem für die Abmilderung kartellrechtlich relevanter Probleme (*lock-in*-Effekte[944]) bedeutsam und umgekehrt auf funktionierenden Wettbewerb, insbesondere funktional äquivalente Alternativen, auf welche die Daten übertragen werden können, angewiesen. Aufgrund dieser primär kartellrechtlichen Ausrichtung soll hier nur ein kurzer Überblick, mit einem Fokus auf Art. 20 DS-GVO, gegeben werden.[945]

---

[939] Vgl. bereits oben, Text bei § 4, Fn. 546 f.

[940] Dazu eingehend § 5 B.III.2.a).

[941] Siehe unten, § 6 C.I.3. und § 6 C.II.

[942] 68. Erwägungsgrund der DS-GVO; *Article 29 Data Protection Working Party*, Guidelines on the right to data portability, WP 242 rev. 01, 2017, 3 f.

[943] Zu den Unterschieden dieses Rechts zu Art. 20 DS-GVO, siehe *Metzger et al.*, 9 JIPITEC 2018, 90 Rn. 52 (basierend auf dem Kommisionsentwurf der DIDD-Richtlinie).

[944] *Schweitzer*, GRUR 2019, 569 (574); *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter III.2.

[945] Zur kartellrechtlichen Dimension von Zugangsrechten insbesondere *Schweitzer*, GRUR 2019, 569; *Drexl*, NZKart 2017, 339 (344); *Drexl, Josef, et al.*, Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate, Max Planck Institute for Innovation & Competition Research Paper No. 16–10, 2016, https://ssrn.com/abstract=2833165; *Graef/Verschakelen/Valcke*, 4 Law: The Journal of the Higher School of Economics, Annual Review 2013, 53.

1. Ermöglichungscharakter

Das Recht auf Datenübertragung soll Nutzern den Wechsel zu anderen Anbietern bzw. die parallele Nutzung mehrerer Anbieter ermöglichen und die Wechselkosten (*switching costs*) senken.[946] Denn die betroffene Person hat nunmehr nicht nur das Recht, ihre von ihr selbst bereitgestellten[947] personenbezogenen Daten herauszuverlangen (vgl. auch Art. 15 Abs. 3 DS-GVO) und ohne Behinderung durch den bisherigen Verantwortlichen einem anderen Anbieter zur Verfügung zu stellen; sie kann zudem verlangen, dass die Daten in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden (Art. 20 Abs. 1 DS-GVO).[948] Damit soll die unmittelbare Wiederverwendbarkeit der Daten für andere Dienste gefördert werden. Dies ist nicht nur für die Plattform-Ökonomie wichtig, sondern auch für das Internet der Dinge, in welchem gleichermaßen eigene Daten und Präferenzen für neue Geräte relevant sind.[949] Damit wird zugleich materielle Privatautonomie, in der Erscheinungsform der Sicherstellung einer effektiven Wahlfreiheit zwischen verschiedenen Angeboten,[950] zumindest gestärkt. Dies macht den Ermöglichungscharakter von Art. 20 DS-GVO aus.

2. Tatbestand

Das Recht auf Datenübertragung besteht jedoch nur dann, wenn die Verarbeitung auf einer Einwilligung (Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DS-GVO) oder auf einem Vertrag (Art. 6 Abs. 1 lit. b DS-GVO) beruht und die Verarbeitung zudem durch automatisierte Verfahren erfolgt. Das Recht auf Datenübertragung ist damit unmittelbar an konsensualen Austausch gebunden: Nur wenn der Nutzer schon zu Beginn der Datenverarbeitung eine eigenständige Wahl durch Einwilligung oder Vertrag ausgeübt hat, soll er auch die Möglichkeit erhalten, den *exit* nicht nur durch Löschung seiner Daten (Art. 17 DS-GVO), sondern auch durch einen erleichterten Anbieterwechsel, also die erneute Ausübung von Wahlfreiheit, zu gestalten. Ferner ist das Portierungsrecht nach Art. 20 Abs. 4 DS-GVO durch Rechte Dritter beschränkt, wobei die genaue Implementierung dieser Schranke durch den EuGH zu klären sein wird.[951]

---

[946] *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf, ZEW Discussion Paper No. 17–043, 2017, http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf, 45, 50.

[947] Dazu etwa *Article 29 Data Protection Working Party*, Guidelines on the right to data portability, WP 242 rev. 01, 2017, 9 f.; *Martinelli*, in: Reins (Hrsg.), Regulating New Technologies in Uncertain Times, 2019, 133 (148 f.); *De Hert et al.*, 34 Computer Law & Security Review 2018, 193 (199 f.).

[948] *De Hert et al.*, 34 Computer Law & Security Review 2018, 193 (201).

[949] *Urquhart/Sailaja/McAuley*, 22 Personal and Ubiquitous Computing 2018, 317.

[950] Zum Verhältnis von Wahlfreiheit und Privatautonomie genauer unten, § 6 A.

[951] Siehe für Vorschläge *Article 29 Data Protection Working Party*, Guidelines on the

Das Portierungsrecht nach Art. 20 DS-GVO wird ergänzt durch ein Recht auf Datenübertragung hinsichtlich nicht personenbezogener Daten aus Art. 16 Abs. 4 DIDD-Richtlinie. Dieses ist gekoppelt an die in der Richtlinie geregelte Vertragsbeendigung. Angesichts des weiten Begriffs personenbezogener Daten kommt diesem weiteren Recht jedoch neben Art. 20 DS-GVO aller Voraussicht nach keine entscheidende Bedeutung zu. Weitere spezialgesetzliche Portierungsrechte finden sich im Energierecht und dem Zahlungsdiensterecht.[952]

3. Limitationen

Das Recht auf Datenübertragung ist in der Tat zentral, um funktionierenden Wettbewerb durchzusetzen,[953] setzt ihn jedoch zugleich insofern voraus, als ein Wechsel aus Sicht der Nutzer nur dann sinnvoll erscheinen wird, wenn funktional zumindest äquivalente Angebote am Markt bestehen. Sonst überwiegen die (wenngleich durch das Recht gesenkten) Wechselkosten den marginalen Erwartungsnutzen aus dem Wechsel. Dies impliziert zugleich, dass das Recht auf Datenübertragung faktisch wertlos ist, wenn signifikante Netzwerkeffekte bestehen[954] und daher funktionell vergleichbare Anbieter mit ähnlicher Nutzergruppenabdeckung nicht bestehen (zum Beispiel Facebook, WhatsApp).[955] Ferner muss eine hinreichende Interoperabilität zwischen den von den jeweiligen Diensten verwendeten Datenformaten bestehen, was ebenfalls nicht selbstverständlich ist.[956]

Ferner ist aus anderen Bereichen des Verbraucherrechts bekannt, dass individuelle Nutzer dazu neigen, rationale Wechsel zu unterlassen.[957] Dies kann eine Reihe von verhaltensökonomischen Gründen haben, von Prokrastination

---

right to data portability, WP 242 rev. 01, 2017, 11 f.; *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf, ZEW Discussion Paper No. 17–043, 2017, http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf, 46.

[952] *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf, ZEW Discussion Paper No. 17–043, 2017, http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf, 48 f.

[953] *Martinelli*, in: Reins (Hrsg.), Regulating New Technologies in Uncertain Times, 2019, 133 (139); *Metzger et al.*, 9 JIPITEC 2018, 90 Rn. 50; *Metzger*, in: Festschrift Basedow, 2018, 131 (144 ff.).

[954] Dazu bereits oben, Text bei § 4, Fn. 559.

[955] Vgl. auch die kritische Perspektive bei *Schweitzer*, GRUR 2019, 569 (574).

[956] Siehe den zweiten Satz des 68. Erwägungsgrunds der DS-GVO; *Urquhart/Sailaja/McAuley*, 22 Personal and Ubiquitous Computing 2018, 317 (325); *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf, ZEW Discussion Paper No. 17–043, 2017, http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf, 46 f.; *Article 29 Data Protection Working Party*, Guidelines on the right to data portability, WP 242 rev. 01, 2017, 17 f.; *De Hert et al.*, 34 Computer Law & Security Review 2018, 193 (201).

[957] *Shui/Ausubel*, Time inconsistency in the credit card market, 14th Annual Utah Winter Finance Conference, 2004, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=586622; *Financial Conduct Authority*, Stimulating interest: Reminding savers to act when rates decrease, Occasional Paper No.7, 2015, 6.

über *default*-Effekte und *present bias* bis hin zu faktischer Ignoranz.[958] Diese beiden Gesichtspunkte, verhaltensökonomische Effekte und Marktstrukturvoraussetzungen, suggerieren, dass das Recht auf Datenübertragung unter den gegenwärtigen Bedingungen der digitalen Wirtschaft, die in vielen Bereichen von erheblichen Marktkonzentrationen und Netzwerkeffekten geprägt ist, nur von eingeschränkter Bedeutung ist. Gleiches kann für das Portabilitätsrecht aus Art. 16 Abs. 4 DIDD-Richtlinie gesagt werden.[959] Derartige Regelungen können daher für sich genommen eine wirksame Ausübung von Privatautonomie nicht ermöglichen, da sie von wettbewerblichen Voraussetzungen leben, die sie selbst nicht garantieren können.[960] Hier zeigt sich einmal mehr die besondere Bedeutung des Kartellrechts, auf die hier jedoch nicht weiter eingegangen werden kann.

IV. Zusammenfassung zu den Ermöglichungsstrukturen im Datenschutzrecht

Insgesamt muss daher mit Blick auf die Ermöglichungsstrukturen im Datenschutzrecht eine ernüchternde Bilanz gezogen werden. Die Anforderungen an die Einwilligung wurden zwar mit dem Kriterium der Unmissverständlichkeit und dem Kopplungsverbot in rechtlicher Hinsicht in sinnvoller Weise verschärft. Sie können jedoch die vielfältigen Defizite der Einwilligung im empirischen Bereich nicht überwinden.[961] Rationale Ignoranz und verhaltensökonomische Effekte lassen wirksame Selbstbestimmung über die eigenen Daten zu dem Privileg einer informierten und aufmerksamen Minderheit werden. Dies ist insofern unbefriedigend, als diese Gruppe mit denjenigen Nutzern, die hohe Datenschutzpräferenzen haben, keineswegs notwendig identisch ist. Insofern stellt die Einwilligung in ihrer in der DS-GVO verankerten Form kein wirksames Mittel dar, um angesichts von heterogenen Datenschutzpräferenzen die Ausübung materieller Privatautonomie signifikant zu fördern. Im Rahmen des Internets der Dinge sind zudem erhebliche externe Effekte in Form der Datenerhebung bei Dritten zu berücksichtigen, die mit den Mitteln der Einwilligung kaum in den Griff zu bekommen sind.

---

[958] *Financial Conduct Authority*, Stimulating interest: Reminding savers to act when rates decrease, Occasional Paper No.7, 2015, 6 f.

[959] *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter III.2.; vgl. auch *Metzger et al.*, 9 JIPITEC 2018, 90 Rn. 50.

[960] In Abwandlung des bekannten Zitats von Böckenförde, dazu etwa *Mangold*, Das Böckenförde-Diktum, VerfBlog (9.5.2019), https://verfassungsblog.de/das-boeckenfoerde-diktum/.

[961] Ähnliches Ergebnis bei *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf, ZEW Discussion Paper No. 17–043, 2017, http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf, 44.

Ein ähnliches Schicksal ist der Datenverarbeitung auf Grundlage eines wirksamen Vertrags beschieden. Schon grundsätzlich liegt hier ein lediglich indirektes Verhältnis zwischen privatautonomer Gestaltung und Kontrolle der erlaubten Datenverarbeitung vor, da in inhaltlicher Hinsicht typischerweise die Vertragsklauseln selbst, nicht jedoch die Datenverarbeitung Gegenstand des Verhandlungsprozesses sind. Hinzu kommt jedoch, dass praktisch ausnahmslos die Vertragsbedingungen, ebenso wie die Einwilligung, mit rationaler Ignoranz gestraft werden. Damit zeigt sich insbesondere deutlich, dass die beiden Hauptinstrumente für Datensouveränität auf der Grundlage von privatautonomer Gestaltung, Einwilligung und Vertrag, nicht nur für beschränkt rationale, sondern gerade auch für rationale Nutzer nur von äußerst limitiertem Wert sind.

Ein ähnliches Bild ergibt sich mit Blick auf das Recht für Datenübertragung. Auch diesem stehen in empirischer Hinsicht verschiedene verhaltensökonomische Effekte im Wege, welche Nutzer tendenziell von einem Anbieterwechsel abhalten. Vor allem jedoch ist auch für stark rationale Betroffene ein Wechsel nur bei funktional äquivalenten Alternativen am Markt sinnvoll, welche in wichtigen Bereichen der digitalen Wirtschaft durch signifikante Netzwerkeffekte verhindert werden.

Dieser Befund deutet auf zwei wichtige Konsequenzen hin. Einerseits kommt angesichts der geringen Belastbarkeit der Ermöglichungsstrukturen im Datenschutzrecht den regulatorischen Strukturen im Datenschutzrecht, aber auch im allgemeinen Zivilrecht, eine erhöhte Bedeutung zur wirksamen Ausbalancierung der beteiligten Interessen, Grundrechte und Grundfreiheiten zu. Dies wird in den folgenden Abschnitten untersucht. Andererseits stellt sich die Frage, auf welche Weise privatautonome Gestaltung, gerade mit Blick auf die drei Leitfälle, stärker als bislang verwirklicht werden könnte. Dies ist die Leitfrage für § 6.

C. Regulatorische Strukturen im Datenschutzrecht

Die Analyse der Ermöglichungsstrukturen des Datenschutzrechts hat gezeigt, dass diese eine wirksame Kontrolle personenbezogener Daten durch Nutzer, mithin eine effektive informationelle Selbstbestimmung, kaum garantieren können. Umso wichtiger sind die in diesem Abschnitt zu behandelnden regulatorischen Strukturen des Datenschutzrechts. Wie bereits bemerkt, eignet den meisten Normkomplexen sowohl eine ermöglichende als auch eine ordnende Dimension. Unter die hier behandelten Ordnungsstrukturen fallen daher solche Normgebilde, die ihrem Schwerpunkt nach regulatorischen Charakter haben und der Entfaltung der Privatautonomie der beteiligten Parteien keinen nennenswerten Raum einräumen. Diese sollen wiederum mit Blick auf die Vernetzungsproblematik, insbesondere hinsichtlich der drei Leitfälle, behandelt werden.

Mit Blick auf die digitale Wirtschaft ist hier vor allem der Erlaubnistatbestand des Art. 6 Abs. 1 lit. f DS-GVO zu nennen (I.), ferner die besondere Regelung für Zweckänderungen in Art. 6 Abs. 4 DS-GVO (II.). Schon etwas vager, aber immer noch als klare Rechtspflicht, tritt *privacy by design and default* nach Art. 25 DS-GVO auf (III.). Am wenigsten interveniert schließlich die sanfte Regulierung (regulierte Selbstregulierung), die in Art. 35 f. und 40 ff. DS-GVO verortet ist, der jedoch als Rahmenbedingung für die digitale Wirtschaft und letztlich auch die Ausübung von Privatautonomie eine signifikante Rolle zukommen kann (IV.).

I. Erlaubnistatbestand, Art. 6 Abs. 1 lit. f DS-GVO

Von den Erlaubnistatbeständen des Art. 6 Abs. 1 DS-GVO sind im Bereich der digitalen Wirtschaft faktisch gegenwärtig nur die Buchstaben a, b und f relevant. Wie gesehen, stellen die Einwilligung (lit. a) und die vertragserforderliche Datenverarbeitung (lit. b) zwei in ihrer konkreten Ausprägung defizitäre, aber grundsätzlich zumindest theoretisch vorhandene Ermöglichungsstrukturen dar. Art. 6 Abs. 1 lit. f DS-GVO enthält demgegenüber mit der zentralen Interessenabwägungsklausel ein Ordnungselement, das jedenfalls vordergründig auf jeglichen Rekurs auf privatautonome Gestaltung verzichtet. Negativ vermag sich diese allenfalls durch das Widerspruchsrecht, Art. 21 Abs. 1 S. 1, Abs. 2 DS-GVO, zu manifestieren. Demgegenüber soll hier der Vorschlag gemacht werden, auch bei der Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO stärker die Belange privatautonomer Gestaltung zu berücksichtigen.

1. Relevanz

Die in den letzten Abschnitten geschilderten Defizite der Einwilligung und der vertragsbasierten Datenverarbeitung werden unter der Geltung der DS-GVO aller Voraussicht nach zu einer stetig steigenden Relevanz der Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO führen. Sie ist Ausdruck der Multirelationalität personenbezogener Daten[962] und enthält zugleich den Auftrag zur hierarchischen Ordnung dieser Relationen. Ihre Grundsätze finden im hier untersuchten Kontext lediglich dann keine Anwendung, wenn wegen der Verarbeitung sensitiver Daten (Art. 9 Abs. 2 lit. a DS-GVO[963]) oder der Direktwerbung mittels Telefon oder E-Mail (§ 7 Abs. 2 Nr. 2/3 UWG) eine ausdrückliche Einwilligung notwendig ist.[964]

---

[962] Siehe oben, § 3 A.III.

[963] Art. 6 Abs. 1 lit. f DS-GVO kann lediglich dann zur Anwendung kommen, wenn ein anderer Tatbestand aus Art. 9 Abs. 2 DS-GVO einschlägig ist, der jedoch nicht alleine die Datenverarbeitung legitimiert, siehe *Herfurth*, ZD 2018, 514 (516).

[964] *Drewes*, ZD 2019, 296 (297).

a) Ökonomische Relevanz

In ökonomischer Hinsicht haben die Ausführungen zur Einwilligung und zur vertragserforderlichen Datenverarbeitung gezeigt, dass beide Instrumente zentrale Gründe des Marktversagens im Bereich digitaler Austauschprozesse (rationale Ignoranz, verhaltensökonomische Effekte und negative Externalitäten) nicht ausräumen können. Insofern kommt Art. 6 Abs. 1 lit. f DS-GVO eine zentrale Rolle für den Ordnungsrahmen der digitalen Wirtschaft zu. Über die Abwägung kann nicht nur der intrinsisch unscharfe „Datenpreis" für Dienste im Rahmen des Geschäftsmodells der Daten als Gegenleistung reguliert werden,[965] sondern können auch Drittinteressen in die Abwägung einfließen, für die im Rahmen der Einwilligung und der vertragsbasierten Datenverarbeitung im Rahmen der DS-GVO keine Anknüpfungspunkte bestehen.

b) Rechtliche Relevanz

Diese ökonomische Steuerungsfunktion kann Art. 6 Abs. 1 lit. f DS-GVO jedoch nur erfüllen, wenn kein anderer Erlaubnistatbestand einschlägig ist. Dann ist die Interessenabwägung auch für die Berücksichtigung der Position der Verantwortlichen von entscheidender Bedeutung. Diese Relevanz steigt in dem Maße, in dem mit Verabschiedung der DS-GVO die Rechtsunsicherheit hinsichtlich einer wirksamen Einwilligung (noch einmal) zugenommen hat.[966] Im privatrechtlichen Bereich ist dies insbesondere in zwei Fallkonstellationen zu gewärtigen.

Erstens ist dies dann der Fall, wenn (bei den ersten beiden Leitfällen: Datenweiterleitung an und Datenerhebung durch Dritte) die Einwilligung und die vertragserforderliche Datenverarbeitung strengen Voraussetzungen unterworfen werden. Hier ist in erster Linie der (nach hiesiger Auffassung abzulehnende) objektive Erforderlichkeitsmaßstab im Rahmen von Art. 6 Abs. 1 lit. b und Art. 7 Abs. 4 DS-GVO zu nennen. Ein ähnliches Ergebnis wird jedoch auch dann erzielt, wenn ein subjektiver Erforderlichkeitsmaßstab einerseits mit einer engen zivilrechtlichen Wirksamkeitskontrolle und andererseits mit dem Fokus auf Verarbeiterpflichten, wie hier vorgeschlagen, kombiniert wird. Dann entfaltet das Kopplungsverbot eine hinreichende Schärfe und die Reichweite der vertragserforderlichen Datenverarbeitung wird begrenzt. Hinzu kommt die Interpretation des Kriteriums der Unmissverständlichkeit, welches zusätzliche signifikante Grenzen für eine wirksame Einwilligung zieht.

Eine zweite, äußerst bedeutsame Kategorie der Relevanz der Interessenabwägung ist mit dem dritten Leitfall (Datenerhebung bei Dritten) angespro-

[965] *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf, ZEW Discussion Paper No. 17–043, 2017, http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf, 44; *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (281 ff.).

[966] *Veil*, NJW 2018, 3337 (3343); *Buchner*, WRP 2019, 1243 (1246).

chen. Hier kommt eine rechtsgeschäftliche Grundlage für die Datenverarbeitung ohnehin kaum in Betracht (dazu § 5 B.III.2.b)), sodass von vornherein lediglich Art. 6 Abs. 1 lit. f DS-GVO eine datenschutzkonforme Verarbeitung zu gewährleisten vermag.

2. *Tatbestand*

Der Tatbestand des Art. 6 Abs. 1 lit. f DS-GVO enthält nach der Rechtsprechung des EuGH (zu Art. 7 lit. f DSRL) drei kumulativ notwendige Kriterien:

„berechtigtes Interesse, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden (1), Erforderlichkeit der Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses (2) und kein Überwiegen der Grundrechte und Grundfreiheiten der betroffenen Person (3).“[967]

a) Berechtigte Interessen

Berechtigte Interessen können somit nicht nur Verantwortliche, sondern auch Dritte geltend machen, was für die Kollektivdimension des Datenschutzes von entscheidender Bedeutung ist.

aa) Interessen des/der Verantwortlichen

Berechtigt sind zunächst alle rechtlich gebilligten Interessen des Verantwortlichen.[968] Für den ersten und zweiten Leitfall ist insbesondere relevant, dass ausweislich des 47. Erwägungsgrunds der DS-GVO das Werbeinteresse als solches anerkannt ist,[969] auch hinsichtlich Dritter, an welche die Daten zu Werbezwecken weitergeleitet werden sollen.[970] Gerade im Bereich der Datenerhebung durch Dritte (*third-party tracking*) hat der EuGH jedoch für die initiale Erhebung eine gemeinsame Verantwortung etwa der Anbieter einer Webseite oder App und der Anbieter des einzubindenden Tracking-Instruments angenommen.[971] Bei derartiger gemeinsamer Verantwortlichkeit müssen die berechtig-

[967] EuGH, Urt. v. 4.5.2017 – Rs. C-13/16 (*Rīgas satiksme*) – Rn. 28; bestätigt in EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 95.

[968] GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (Fashion ID) – Rn. 122; *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, 2014, 32; *Herfurth*, ZD 2018, 514 (514); *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 57; *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, 12; *Robrahn/Bremert*, ZD 2018, 291 (291 f.); *Tavanti*, RDV 2016, 295 (296).

[969] *Drewes*, ZD 2019, 296 (298); *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, 11 f.; *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Anhang 3 zu Artikel 6: Datenverarbeitung für Zwecke der Werbung Rn. 25; *Weidert/Klar*, BB 2017, 1858 (1860); *Tavanti*, RDV 2016, 295 (296 f.).

[970] GA *Bobek*, Schlussanträge v. 19.12.2018 – Rs. C-40/17 (Fashion ID) – Rn. 123; *Drewes*, ZD 2019, 296 (300).

[971] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 84 f.; dazu eingehend oben, § 4 A.III.1.b)dd)(1).

ten Interessen separat vorliegen: Jeder Verantwortliche muss ein eigenes berechtigtes Interesse vorweisen können, das die Datenverarbeitung durch diesen Verarbeiter rechtfertigt.[972]

Bei dem dritten Leitfall, der Datenerhebung bei Dritten im Rahmen des Internets der Dinge, wird man als berechtigtes Interesse des Verantwortlichen das Angebot und den Vertrieb des Produkts selbst, inklusive der Datenerhebung bei Dritten als Folgeerscheinung, in Rechnung stellen müssen, da gerade bei unbeabsichtigter Erhebung von Drittdaten (z. B. Gespräche mit Kindern) typischerweise kein berechtigtes Interesse des Verantwortlichen an der Erhebung gerade dieser funktionsirrelevanten Daten besteht.

bb) Interessen Dritter

Ferner sind berechtigte Drittinteressen in Rechnung zu stellen. Nach dem Wortlaut kommt dies jedoch nur zugunsten einer Verarbeitung (im Rahmen des ersten Kriteriums des EuGH), nicht zulasten einer Verarbeitung (im Rahmen des dritten Kriteriums), in Betracht. Bliebe man hierbei stehen, so müsste zwar einerseits z. B. dem Interesse der Nutzer mit gering ausgeprägten Datenschutzpräferenzen, die ein Tracking aus Komfortgründen oder zur Erweiterung ihrer Budget-Restriktionen gerne in Kauf nehmen, Rechnung getragen werden.[973] Andererseits könnte jedoch das Interesse Dritter mit hohen Datenschutzpräferenzen, die durch externe Effekte wie adverse oder ähnlichkeitsbasierte Inferenz betroffen wären,[974] keine Berücksichtigung finden.

Dies erscheint jedoch bei teleologischer und primärrechtskonformer Auslegung unhaltbar.[975] Denn es ist im Lichte von Art. 20 GRCh kein sachlicher Grund ersichtlich, aus dem Drittinteressen die Interessen, Grundrechte und Grundfreiheiten des Verantwortlichen verstärken können, jedoch für die Wertung des Datenschutzgrundrechts des Betroffenen irrelevant sein sollen. Wenn schon eine Ausdehnung auf Drittinteressen stattfindet, so muss diese richtigerweise symmetrisch vorgenommen werden.

Dafür streitet nunmehr auch die Rechtsprechung des EuGH zur horizontalen Direktwirkung der Chartagrundrechte.[976] Diese Rechtsprechung dürfte auf das Datenschutzgrundrecht aus Art. 8 GRCh übertragbar sein.[977] Inwiefern mittelbare Auswirkungen wie adverse Inferenz (*unraveling*) tatsächlich eine Verletzung des Datenschutzgrundrechts Dritter bewirken können, harrt

[972] EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 96 f.

[973] Vgl. *Hanloser*, ZD 2019, 287 (289).

[974] Siehe zu solchen negativen Externalitäten oben, Teil § 3 B.II.1.c).

[975] Im Ergebnis ebenso *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (282).

[976] Siehe nur EuGH, Urt. v. 17.4.2018 – Rs. C-414/16 (*Egenberger*) – Rn. 76; Urt. v. 11.9.2018 – Rs. C-68/17 (*IR*) – Rn. 69; Urt. v. 6.11.2018 – verb. Rs. C-569/16 und C-570/16 (*Bauer und Willmeroth*) – Rn. 89 f., 92; EuGH, Urt. v. 22.1.2019 – Rs. C-193/17 (*Cresco Investigation*) – Rn. 79 f.; weitere Nachweise unten, § 5, Fn. 1074.

[977] Dazu unten, § 5 C.III.4.a)aa).

noch einer eingehenden Untersuchung. Als Minimalfolge der horizontalen Direktwirkung müssen jedoch Auswirkungen auf Datenschutzgrundrechte Dritter auch im privatrechtlichen Kontext jedenfalls im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO Beachtung finden. Damit wird diese Norm zum entscheidenden Einfallstor für die Berücksichtigung der Kollektivdimension des Datenschutzes.[978]

b) Erforderlichkeit der Datenverarbeitung zur Interessenwahrung

In einem zweiten Schritt ist zu eruieren, ob die Datenverarbeitung zur Wahrung der Interessen des Verantwortlichen oder Dritter, deren Interessen ebenfalls für die Verarbeitung sprechen, erforderlich ist. Gleichwertige, zumutbare Alternativen verhindern daher die Berufung auf Art. 6 Abs. 1 lit. f DS-GVO.[979] Dabei handelt es sich der Sache nach um eine Ausprägung des Datenminimierungsgrundsatzes aus Art. 5 Abs. 1 lit. c DS-GVO.[980]

c) Abwägung

Die berechtigten Interessen des Verantwortlichen oder von Dritten legitimieren schließlich die Datenverarbeitung, wenn, wie die DS-GVO formuliert, die Interessen, Grundrechte oder Grundfreiheiten der betroffenen Person nicht überwiegen. Dies bedingt eine umfassende Interessenabwägung, in welche richtigerweise, wie ausgeführt, auch die Interessen Dritter, die durch negative Externalitäten betroffen sind, einzustellen sind. Auf Seiten der betroffenen Person sind dabei vor allem das Datenschutzgrundrecht aus Art. 8 GRCh, aber auch die Achtung der Privatsphäre und die Vertraulichkeit der Kommunikation gem. Art. 7 GRCh[981] oder mögliche wirtschaftliche Nachteile in die Waagschale zu werfen.[982]

aa) Überwiegen

Die Formulierung der DS-GVO dahingehend, dass berechtigte Interessen des Verantwortlichen oder Dritter eine Verarbeitung erlauben, wenn die Interessen der betroffenen Person nicht überwiegen, begründet keine Vermutung zu-

---

978 Siehe auch *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (282).

979 *Herfurth*, ZD 2018, 514 (515).

980 *Robrahn/Bremert*, ZD 2018, 291 (292); ähnlich *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Anhang 3 zu Artikel 6: Datenverarbeitung für Zwecke der Werbung Rn. 28.

981 Zum Verhältnis von Art. 7 und 8 GRCh ausführlich *Lynskey*, The Foundations of EU Data Protection Law, 2015, 91 ff.; *W. Michl*, DuD 2017, 349.

982 *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 148; *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, 13.

gunsten der Verarbeitung. Jedoch ist bei einem *non liquet* die Verarbeitung zulässig.[983]

bb) Wertungskriterien

Die Abwägung selbst ist hochgradig einzelfallabhängig und kann daher hier nicht umfassend für alle im Rahmen der Leitfälle denkbaren Konstellation geleistet werden (siehe aber sogleich den Überblick unter 3.). Allerdings lassen sich im Einklang mit der Literatur grundsätzliche Wertungskriterien für die Abwägung angeben.[984] Für die Belange des Datenschutzprivatrechts soll hier zudem der Vorschlag gemacht werden, der privatautonomen Gestaltung eine Residualwirkung zukommen zu lassen.

(1) Grundsätzliche Wertungskriterien

Die maßgeblichen Wertungskriterien können drei Kategorien zugeordnet werden: den Daten, den Akteuren und der Verarbeitung selbst.[985] Hinsichtlich der Daten ist zum Beispiel ihre Art und insbesondere die Nähe zu sensitiven Daten, sowie daraus folgend die Stärke der Implikation des Datenschutzgrundrechts, zu beachten.[986] Neben der Qualität spielt freilich auch die Quantität der Daten eine Rolle.[987] Schließlich kann die Stärke der Pseudo- oder Anonymisierung (d. h. eine geringe Wahrscheinlichkeit der Re-Identifikation) die Belastung für die betroffene Person reduzieren.[988]

Besonders wichtig ist zweitens der Blick auf die Akteure. Denn der 47. Erwägungsgrund der DS-GVO formuliert ausdrücklich, dass die vernünftigen Erwartungen der betroffenen Person hinsichtlich der Datenverarbeitung maßgeblich zu berücksichtigen sind. Ein Überraschungseffekt spricht daher klar gegen eine Zulässigkeit im Rahmen der Interessenabwägung.[989] Umgekehrt

[983] *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 58; *Robrahn/Bremert*, ZD 2018, 291 (293); *Tavanti*, RDV 2016, 295 (298); aA *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Anhang 3 zu Artikel 6: Datenverarbeitung für Zwecke der Werbung Rn. 35 (im Zweifel für die betroffene Person).

[984] Siehe die exemplarischen Anleitungen bei *DSK*, Orientierungshilfe für Anbieter von Telemedien, 2019, 11 ff.; *Herfurth*, ZD 2018, 514 (516 ff.); *Robrahn/Bremert*, ZD 2018, 291 (293 ff.); *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 298 ff.

[985] *Herfurth*, ZD 2018, 514 (516 ff.).

[986] *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, 2014, 49; *Tavanti*, RDV 2016, 295 (298).

[987] *Herfurth*, ZD 2018, 514 (516); *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, 20.

[988] *Drewes*, ZD 2019, 296 (299); *Herfurth*, ZD 2018, 514 (516); *Hanloser*, ZD 2019, 287 (289); *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO Rn. 114; *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, 2014, 54; *Tavanti*, RDV 2016, 295 (299); aA *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, 14.

[989] *Tavanti*, RDV 2016, 295 (299).

sind jedoch nicht alle Verarbeitungen, die den vernünftigen Erwartungen entsprechen, legitim,[990] da sonst die Kenntnis von ubiquitärer und weitreichender Datenverarbeitung zu einem Entfallen des datenschutzrechtlichen Schutzes führen, Faktizität damit unmittelbar normativ würde. Die vernünftigen Erwartungen sind nach hier vertretener Auffassung nicht mit den Pflichtinformationen gem. Art. 13 f. DS-GVO identisch,[991] da typischerweise mit deren Erfassung gerade nicht gerechnet werden kann und im 47. Erwägungsgrund sonst auch einfach auf diese hätte verwiesen werden können. Vielmehr ist hier in einer gemischt normativ-empirischen Analyse[992] der tatsächliche Wissensstand eines Durchschnittsnutzers,[993] angereichert durch besonders salient kommunizierte Informationen, deren Kenntnisnahme daher normativ zu erwarten ist,[994] zugrunde zu legen. Ferner ist das Verhältnis der beiden Akteure von Relevanz, etwa auch die Marktstellung des Verantwortlichen.[995] Schließlich enthält bereits der Wortlaut von Art. 6 Abs. 1 lit. f DS-GVO den Hinweis, dass die Verarbeitung gegenüber Kindern besonders streng zu prüfen ist und ihre Interessen regelmäßig überwiegen werden.[996]

Zuletzt ist auch die Art der Verarbeitung für die Interessenabwägung in Rechnung zu stellen.[997] Der Zweck und die Umstände der Verarbeitung sind hier maßgeblich.[998] Insbesondere muss hier auf Grundlage des risikobasierten Regimes der DS-GVO untersucht werden, ob Anhaltspunkte für erhöhte datenschutzrechtliche Risiken bestehen. Diese können sich etwa in einer systematischen Überwachung, welche mit erhöhten Risiken von *chilling*-Effekten, Diskriminierung und Datenmissbrauch einhergeht, einer langen Speicherdauer sowie der Weiterleitung ins EU-Ausland manifestieren.[999]

---

[990] *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Anhang 3 zu Artikel 6: Datenverarbeitung für Zwecke der Werbung Rn. 31.

[991] So aber *Drewes*, ZD 2019, 296 (298); *Tavanti*, RDV 2016, 295 (299); wohl auch *Herfurth*, ZD 2018, 514 (518); wie hier *DSK*, Orientierungshilfe für Anbieter von Telemedien, 2019, 16; *Robrahn/Bremert*, ZD 2018, 291 (295).

[992] Ähnlich *Robrahn/Bremert*, ZD 2018, 291 (294); *Tavanti*, RDV 2016, 295 (299); aA *Hanloser*, ZD 2019, 287 (290): rein empirische Frage, wobei offenbleibt, wie der tatsächliche Wissensstand jeweils genau gemessen werden soll.

[993] Zur Bestimmung des Wissenstands etwa *Ayres/Schwartz*, 66 Stanford Law Review 2014, 545 (595 ff.); *Rao et al.*, Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016, 77.

[994] Vgl. insoweit auch *Tavanti*, RDV 2016, 295 (299 mit Fn. 30).

[995] *Herfurth*, ZD 2018, 514 (518); *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, 2014, 51.

[996] *Drewes*, ZD 2019, 296 (298); genauer *Robrahn/Bremert*, ZD 2018, 291 (294 f.).

[997] *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Anhang 3 zu Artikel 6: Datenverarbeitung für Zwecke der Werbung Rn. 36.

[998] *Drewes*, ZD 2019, 296 (298); *Herfurth*, ZD 2018, 514 (519).

[999] *Herfurth*, ZD 2018, 514 (518 f.); *Robrahn/Bremert*, ZD 2018, 291 (294); vgl. auch *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, 19; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO Rn. 105 f.

Keine Rolle kann jedoch spielen, ob die betroffene Person die Daten freiwillig veröffentlicht hat. Eine bisweilen vertretene analoge Anwendung von Art. 9 Abs. 2 lit. e DS-GVO[1000] scheitert bereits daran, dass diese Vorschrift nach hier vertretener Auffassung keinen Zulässigkeitstatbestand enthält, sondern lediglich das in Art. 9 Abs. 1 DS-GVO enthaltene Verbot aufhebt.[1001] Daher muss auch in diesem Fall ein Zulässigkeitstatbestand des Art. 6 Abs. 1 DS-GVO vorliegen. Denn auch freiwillig veröffentlichte Daten (etwa in sozialen Netzwerken hochgeladene Fotos) sind vom Betroffenen regelmäßig nicht für jegliche Form der Verwendung freigegeben.[1002] So enthält ein Post auf Facebook, der für alle Internetnutzer sichtbar ist, sicherlich keine konkludente Einwilligung dahingehend, dass er auch beliebig als Input für Big Data Analysen oder Techniken maschinellen Lernens verwendet werden darf. Dies folgt bereits aus dem Rechtsgedanken des Zweckbindungsgrundsatzes.

Ganz allgemein müssen auch die Grundsätze der Datenverarbeitung im Rahmen der Abwägung beachtet werden. Ferner ist darauf zu achten, dass der Heterogenität der Datenschutzpräferenzen präzise Rechnung getragen wird durch eine Berücksichtigung sowohl der Interessen derjenigen, die niedrige Datenschutzpräferenzen haben, als auch derjenigen, welche ein hohes Datenschutzniveau einfordern.

(2) Residualwirkung privatautonomer Gestaltung

Im Rahmen des Datenschutzprivatrechts ist nun insbesondere zu erwägen, einer privatautonomen Gestaltung jedenfalls in einigen Fällen eine Wirkung auf die Interessenabwägung zuzusprechen. Dies kann insbesondere dann wichtig werden, wenn die betroffene Person sich zunächst vertraglich zu einer Einwilligung in eine bestimmte Form der Datenverarbeitung als Gegenleistung für einen Dienst oder ein Produkt des Anbieters verpflichtet hat, die Einwilligung jedoch nach Erhalt des Dienstes oder Produkts widerruft. Eine Einschränkung der Widerruflichkeit der Einwilligung ist in diesen Fällen, wie gesehen, abzulehnen.[1003] Jedoch muss dann Folge der ursprünglichen vertraglichen Bindung sein, dass die Interessen des Verantwortlichen, sofern ein berechtigtes Interesse an weiterer Verarbeitung besteht, überwiegen, wenn die Bindung klar und salient (nicht lediglich in AGB) kommuniziert wurde und auf die Möglichkeit weiterer Verarbeitung nach Art. 6 Abs. 1 lit. f hingewiesen wurde. Denn dann liegt, trotz der Widerrufsmöglichkeit, kein Fall vor, in

[1000] So aber: *Golland*, MMR 2018, 130 (133): Verarbeitung dann stets zulässig; schwächer: *Herfurth*, ZD 2018, 514 (517): Berücksichtigung bei der Abwägung; ebenso *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Anhang 3 zu Artikel 6: Datenverarbeitung für Zwecke der Werbung Rn. 36; wie hier *Tavanti*, RDV 2016, 295 (297).

[1001] Siehe oben, § 4, Fn. 784.

[1002] *Robrahn/Bremert*, ZD 2018, 291 (295).

[1003] Siehe oben, § 4 B.I.3.b)bb)(2).

dem der Betroffene „vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss“ (47. Erwägungsgrund), da er auch über die weitere Verarbeitung zusätzlich noch nach Art. 13 DS-GVO informiert wird. Dies bietet eine Möglichkeit, einem etwaigen opportunistischen Einsatz des Widerrufsrechts durch die betroffene Person entgegenzutreten. Sofern der Widerruf zugleich als Widerspruch im Sinne des Abs. 21 Abs. 1 S. 1 DS-GVO gewertet wird[1004] – was allerdings Gründe voraussetzt, die sich aus der besonderen Situation der betroffenen Person ergeben[1005] –, können dann zumindest potenziell auch zwingende schutzwürdige Gründe des Verantwortlichen nach Abs. 21 Abs. 1 S. 2 DS-GVO angenommen werden. Diese Lösung der „Fortsetzung der privatautonomen Gestaltung mit anderen Mitteln“ versagt lediglich, wenn die Datenverarbeitung der Direktwerbung (auch: der personalisierten Werbung mithilfe von Geräte-Identifiern[1006]) dient, da der anlasslose Widerspruch nach Art. 21 Abs. 2 DS-GVO gem. Art. 21. Abs. 3 DS-GV nicht überwunden werden kann. Dies ist jedoch als klare gesetzliche Wertung *de lege lata* hinzunehmen.

Eine Residualwirkung privatautonomer Gestaltung scheidet ebenfalls aus, wenn die Einwilligung wegen Verstoßes gegen zwingende datenschutzrechtliche Vorschriften unwirksam ist. Dann kann kein grundsätzliches Überwiegen der Interessen des Verantwortlichen kraft privatautonomer Gestaltung angenommen werden, da gerade keine wirksame privatautonome Bindung eingetreten ist. Insofern kann etwa die Wirkung des Kopplungsverbots nach Art. 7 Abs. 4 DS-GVO nicht grundsätzlich durch die Hintertür der Interessenabwägung korrigiert werden. Allerdings ist andererseits auch nicht ausgeschlossen, dass trotz Einschlägigkeit des Kopplungsverbots die Interessen des Verantwortlichen im Einzelfall überwiegen.

3. Anwendung auf die drei Leitfälle

Diese Kriterien können wiederum auf die drei Leitfälle angewandt werden, indem die jeweiligen Wertungsparameter spezifisch gewichtet werden.

a) Datenweiterleitung an Dritte (*ad exchanges* und personalisierte Werbung)

Der erste Leitfall zur Datenweiterleitung an Dritte umfasst insbesondere die Frage der über *ad exchanges* abgewickelten personalisierten Werbung.[1007] Die

[1004] *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO Rn. 89.

[1005] Dazu *Robrahn/Bremert*, ZD 2018, 291 (296).

[1006] Diese fassen unter den Begriff der Direktwerbung ebenfalls: *Caspar*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 21 DS-GVO Rn. 21; *Tavanti*, RDV 2016, 295 (297 mit Fn. 18); *Piltz*, K&R 2016, 557 (565); wohl auch *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Anhang 3 zu Artikel 6: Datenverarbeitung für Zwecke der Werbung Rn. 18.

[1007] Zur personalisierter Werbung durch Facebook auf dem sozialen Netzwerk selbst,

wohl herrschende Meinung fordert hier eine ausdrückliche Einwilligung und lehnt eine Rechtmäßigkeit der Datenverarbeitung aufgrund der Interessenabwägung ab.[1008] Dies ist jedenfalls im Grundsatz zutreffend. Einerseits ist zwar anzuerkennen, dass der Verantwortliche, zur Finanzierung seines Geschäftsmodells, sowie Nutzer mit gering ausgeprägten Datenschutzpräferenzen ein signifikantes, zum Teil grundrechtlich über Art. 15 f. GRCh geschütztes, Interesse an der Zurverfügungstellung des Dienstes im Gegenzug für die Verarbeitung personenbezogener Daten zum Zwecke personalisierter Werbung hat. Jedoch ist andererseits zu beachten, dass personalisierte (oder zielgruppenorientierte) Werbung typischerweise mit einer systematischen Sammlung von personenbezogenen Daten einhergeht (Profilbildung).[1009] Ferner werden die Daten zumeist an Drittverarbeiter weitergeleitet, was nicht nur die Zahl der Angriffspunkte mit Blick auf die IT-Sicherheit, sondern auch die genannten datenschutzrechtlichen Risiken und damit auch die Gefahr von *chilling*-Effekten erhöht.[1010] Daher ist das Datenschutzgrundrecht der Nutzer regelmäßig stark betroffen und sind die Interessen der Nutzer mit mittel bis stark ausgeprägten Datenschutzpräferenzen mit erheblichem Gewicht versehen.[1011]

aa) Grundsätzliche Abwägung

Grundsätzlich ist dabei von einem Überwiegen der Interessen der Nutzer mit mittel bis stark ausgeprägten Datenschutzpräferenzen gegenüber den Interessen des Verantwortlichen und der wenig an Datenschutz orientierten Grup-

siehe, ohne klare Aussage zur Zulässigkeit, *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Anhang 3 zu Artikel 6: Datenverarbeitung für Zwecke der Werbung Rn. 47 f.

[1008] LG Berlin, Urt. v. 16.1.2018, BeckRS 2018, 1060 Rn. 45; *Zuiderveen Borgesius*, 5 International Data Privacy Law 2015, 163 (167–170); *Article 29 Data Protection Working Party*, Opinion 03/2013 on purpose limitation, WP 203, 2013, 46; *DSK*, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, Positionsbestimmung, 2018, 3 Rn. 9; *European Data Protection Supervisor*, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 2017, 26 Fn. 84; *Langhanke*, Daten als Leistung, 2018, 103; *Golland*, MMR 2018, 130 (130, 133); *Schwenke*, Individualisierung und Datenschutz, 2006, 164–167; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO Rn. 106; *Metzger*, GRUR 2019, 129 (134); wohl auch *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Anhang 3 zu Artikel 6: Datenverarbeitung für Zwecke der Werbung Rn. 29, 36, 43; aA *Gierschmann*, ZD 2018, 297 (300); *Roßnagel*, DuD 2016, 561 (563); *Arning/Moos*, ZD 2014, 242 (245 f.); Zulässigkeit bei starker Pseudonymisierung bejahend *Tavanti*, RDV 2016, 295 (306); tendenziell für die Zulässigkeit der Bestandskundenwerbung auch mithilfe von Tracking-Instrumenten *Weidert/Klar*, BB 2017, 1858 (1862).

[1009] *Zuiderveen Borgesius*, 5 International Data Privacy Law 2015, 163 (164).

[1010] Dies gilt unter der Annahme, dass die datenschutzrechtlichen Risiken des zusätzlich eingeschalteten Verarbeiters (z. B. das Missbrauchsrisiko) nicht bei null liegen, wovon jedoch – gerade im Rahmen von personenbezogener Werbung durch Verwendung großer Datenmengen – realistischerweise nicht ausgegangen werden kann.

[1011] Vgl. *Schwenke*, Individualisierung und Datenschutz, 2006, 165.

pe auszugehen. Zwei Gründe sind hierfür entscheidend. Erstens steht es dem Verantwortlichen frei, das Geschäftsmodell so abzuwandeln, dass das Datenschutzgrundrecht derjenigen, die hohe Datenschutzpräferenzen aufweisen, stärker respektiert wird. Dies kann etwa, wie bereits ausgeführt, durch die Eröffnung einer datenschonenden Alternative, für welche monetär statt durch Daten für personenbezogene Werbung gezahlt wird, geschehen.[1012] Dies ist, da das Geschäftsmodell im Übrigen nicht tangiert wird, dem Verantwortlichen auch in aller Regel zumutbar. Da in diesem Fall weiterhin eine datenintensive Alternative, finanziert über personalisierte Werbung, angeboten wird, werden auch die Präferenzen der datenschutzaversen Gruppe respektiert.

Zweitens ist in jenen Fällen, in denen Daten mithilfe von Tracking-Instrumenten erhoben werden,[1013] die Wertung von Art. 5 Abs. 3 ePrivacy-Richtlinie bis zur Geltung einer künftigen ePrivacy-Verordnung nach hier vertretener Auffassung in der Interessenabwägung zu berücksichtigen.[1014] Danach können derartige Instrumente, sofern sie nicht funktional essenziell sind, lediglich nach einer Einwilligung zum Einsatz gebracht werden. Dass statt der ePrivacy-Richtlinie oder der ePrivacy-Verordnung nunmehr, aufgrund der Verzögerung letzterer, die DS-GVO zur Anwendung kommt, darf nicht zu einer Absenkung des Schutzniveaus führen. Dem steht auch der 70. Erwägungsgrund der DS-GVO nicht entgegen.[1015] Danach muss eine betroffene Person Widerspruch gegen die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung einlegen können. Allerdings impliziert dies mitnichten, dass die Verarbeitung zu diesem Zweck damit grundsätzlich von Art. 6 Abs. 1 lit. f DS-GVO gedeckt wäre. Vielmehr will der 70. Erwägungsgrund lediglich klarstellen, dass jedenfalls und unentziehbar auch die Möglichkeit des Widerspruchs gem. Art. 21 Abs. 2 DS-GVO bleibt. Ferner kann Direktwerbung auch ohne Geräte-Identifier betrieben werden, sodass über die Wertung von Art. 5 Abs. 3 ePrivacy-Richtlinie insoweit nichts gesagt ist.

bb) Marktmacht

Verstärkt wird diese grundsätzliche Ausrichtung der Interessenabwägung zugunsten der betroffenen Person, wenn der Verantwortliche eine marktbeherrschende Stellung innehat. Denn dann kann die betroffene Person typischer-

[1012] Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, 2014, 60.

[1013] Dazu wiederum *Zuiderveen Borgesius*, 5 International Data Privacy Law 2015, 163 (164).

[1014] *Moos/Rothkegel*, MMR 2019, 736 (740); aA *Gierschmann*, ZD 2018, 297 (300); *Hanloser*, ZD 2018, 213 (217). Der bei *Hanloser* angeführte 66. Erwägungsgrund gibt für die Frage nichts her, da zwar von legitimer Verwendung von Cookies die Rede ist, aber nicht expliziert wird, ob damit essenzielle oder auch Marketing-Cookies gemeint sind. Auch der Verweis auf Art. 95 DS-GVO führt nicht weiter (s. o., § 4 B.I.4.b)).

[1015] So aber *Gierschmann*, ZD 2018, 297 (300).

weise (jedenfalls bei Vorliegen von Netzwerkeffekten) gerade nicht darauf verwiesen werden, dass sie funktional äquivalente Angebote am Markt wahrnehmen kann, die ohne eine entsprechende Datenverarbeitung auskommen.[1016] Dies verleiht dem Interesse derjenigen, die hohe Datenschutzpräferenzen aufweisen, eine noch stärkere Dringlichkeit. So hat auch das Bundeskartellamt im Fall des Datenaustauschs zwischen Facebook-Unternehmen ein Überwiegen der Interessen der Nutzer vor allem wegen der marktbeherrschenden Stellung von Facebook angenommen, welche nach dem Bundeskartellamt zu einem einseitigen Auferlegen von Datenverarbeitungskonditionen führt.[1017] Diese Abwägung im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO ist in der Literatur zu Recht auf Zustimmung gestoßen.[1018]

cc) Überraschungseffekt

Schließlich fällt ganz regelmäßig die Abwägung zugunsten der betroffenen Person aus, wenn sich ein Überraschungseffekt hinsichtlich der Nutzung gerade der spezifischen Daten für personalisierte Werbung einstellt. Dass überhaupt Daten für Werbeprofile verwendet werden, dürfte mittlerweile den vernünftigen Erwartungen der Nutzer entsprechen.[1019] Ein Überraschungseffekt kann jedoch hinsichtlich solcher, konkret verwendeter Daten auftreten, bei denen Nutzer mit einer Verwendung für personenbezogene Werbung nicht typischerweise rechnen. Eine empirische Studie legt dies etwa bei Facebook für eine Reihe der durch den Anbieter erhobenen Daten nahe.[1020] Ganz konkret hat auch der VGH München im Fall von Facebook Custom Audience entschieden, dass bei der Weiterleitung von gehashten E-Mail-Adressen an Facebook zu Zwecken der Überschneidungsanalyse, an welche sich eine zielgerichtete Werbung anschließt,

„die Interessenabwägung zwischen den schutzwürdigen Interessen der Betroffenen (insbes. dem Recht auf informationelle Selbstbestimmung gem. Art. 2 I GG iVm Art. 1 I GG bzw. dem in Art. 8 I GRCh garantierten Schutz personenbezogener Daten) und dem Interesse [eines Drittunternehmens] an der Übermittlung der E-Mail-Adressen an Facebook zu Werbezwecken zulasten [des Drittunternehmens ausfällt].“[1021]

Denn die Betroffenen würden typischerweise nicht damit rechnen, dass ihre im Rahmen eines Bestellvorgangs bei dem Drittunternehmen angegebene E-Mail-Adresse zu Zwecken der Werbung an Facebook übermittelt wird.[1022]

[1016] Siehe ausführlich unten, § 6 C.II.4.a) und b).
[1017] Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 783 ff., 858 f.
[1018] *Hoeren*, MMR 2019, 137 (138); *Buchner*, WRP 2019, 1243 (1248).
[1019] *DIVSI*, Daten – Ware und Währung, 2014, 16.
[1020] *Rothmann/Buchner*, DuD 2018, 342 (345).
[1021] VGH München, NVwZ 2019, 171 Rn. 27.
[1022] VGH München, NVwZ 2019, 171 Rn. 27.

Dies ist insbesondere auch wichtig für die Datenweiterleitung im Internet der Dinge. Gerade bei Geräten, die auch durch monetäre Zahlung erworben werden (data on top-Modell), rechnet der typische Nutzer vernünftigerweise eher nicht mit der Verwendung seiner Nutzungsdaten zu Zwecken personenbezogener Werbung. Anders kann die Abwägung jedoch, wie gesehen, dann ausfallen, wenn die wirksame Einwilligung in die Datenverarbeitung zu Werbezwecken seitens des Nutzers widerrufen wurde und er sich zuvor transparent zur Abgabe der Einwilligung verpflichtet hatte.[1023]

b) Datenerhebung durch Dritte

Wie soeben bereits angesprochen, überwiegt aufgrund der Wertung von Art. 5 Abs. 3 ePrivacy-Richtlinie grundsätzlich das Interesse des Nutzers an einer lediglich einwilligungsbasierten Nutzung von (insbesondere *third-party*) Tracking-Instrumenten. Zudem ist in Rechnung zu stellen, dass die Nutzer regelmäßig nicht erwarten, jedenfalls nicht erwarten müssen, in erheblichem Umfang einem Tracking durch Drittanbieter ausgesetzt zu werden.[1024] In diesem Sinne hat wiederum das Bundeskartellamt im Facebook-Fall hinsichtlich der Nutzung von Drittanbietercookies durch Social Plug-Ins entschieden.[1025] Auch hier kann jedoch wiederum die ursprüngliche, transparente Verpflichtung des Nutzers zur Abgabe einer Einwilligung zu einem anderen Ergebnis führen.[1026]

c) Datenerhebung bei Dritten

Auch bei der Datenerhebung bei Dritten ergeben sich erhebliche Interessenkonflikte, die in Ermangelung einer Einwilligung oder eines Vertrags typischerweise im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO bewältigt werden müssen.[1027] Zwar mag die versehentliche Erhebung von Daten Dritter bei manchen IoT-Geräten mit deren bestimmungsgemäßem Einsatz einhergehen. So mag es schwer zu verhindern sein, dass nach einer Aktivierung der Sprachsteuerung nicht nur Befehle des Geräteinhabers, sondern auch Sprachdaten Dritter verarbeitet werden.[1028] Jedenfalls im Grundsatz überwiegt jedoch das Daten-

[1023] Dazu oben, Text bei § 4, Fn. 1003.

[1024] *DSK*, Orientierungshilfe für Anbieter von Telemedien, 2019, 17 und Anhang, II.

[1025] Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 783 ff., 858 f.; zustimmend *Buchner*, WRP 2019, 1243 (1248).

[1026] Siehe nochmals oben, Text bei § 4, Fn. 1003.

[1027] Zu den – eingeschränkten – Möglichkeiten eines Vertragsschlusses in diesen Konstellationen noch unten, § 5 B.III.2.b).

[1028] *Wissenschaftliche Dienste – Deutscher Bundestag*, Zulässigkeit der Transkribierung und Auswertung von Mitschnitten der Sprachsoftware „Alexa" durch Amazon, WD 10 – 3000 – 032/19, Sachstand, 2019, 9; *Liptak*, Amazon's Alexa started ordering people dollhouses after hearing its name on TV, The Verge (7.1.2017), https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse.

schutzgrundrecht des Dritten. Dieser hätte sonst über die eigenen Daten in vernetzten Umgebungen, die bereits gegenwärtig bestehen und durch die Tendenz zum *Internet of Everything* eher noch umfassender werden,[1029] praktisch keine Kontrolle mehr. Dieser Abwägungsgrundsatz gilt umso mehr, wenn ein Mithören oder eine „manuelle" Verarbeitung der Daten durch menschliche Mitarbeiter des Anbieters erfolgt.[1030]

Das berechtigte Interesse des Verantwortlichen an Verkauf und Nutzbarkeit des Gerätes, sowie von bestimmten Nutzern an einer einfachen Handhabung des Geräts, kann richtigerweise nur dann überwiegen, wenn der Verantwortliche alle zumutbaren Anstrengungen unternimmt, um schon auf technischem Wege die Erhebung von Daten bei Dritten auszuschließen oder, wo dies nicht möglich ist, die Daten regelmäßig und proaktiv (zum Beispiel durch den Abgleich mit dem Sprachprofil des Geräteinhabers) untersucht und unmittelbar nach Erkenntnis der Dritteigenschaft löscht.[1031] Das Überwiegen der Interessen des Verantwortlichen gründet dann darauf, dass diesem, anders als in den beiden zuvor diskutierten Leitfällen, typischerweise keine Möglichkeiten des Ausweichens auf Art. 6 Abs. 1 lit. a oder b DS-GVO offenstehen. Soll die Legitimierung nach Art. 6 Abs. 1 lit. f DS-GVO gelingen, so dürfen jedoch auch in diesem Fall keine intensiven Eingriffe vorgenommen werden, insbesondere keine Daten mit Nähe zu besonders geschützten Kategorien i. S. d. Art. 9 Abs. 1 DS-GVO verarbeitet werden.

4. Rechtssichere Operationalisierung für die beteiligten Akteure

Trotz der Möglichkeit der Systematisierung der für die Interessenabwägung maßgeblichen Wertungskriterien stellt sich die rechtssichere Operationalisierung von Art. 6 Abs. 1 lit. f DS-GVO als besondere Herausforderung dar. Eine solche Konkretisierung ist aus Sicht der betroffenen Akteure, insbesondere auch der Anbieter, ein besonders dringliches Desiderat. Zwar kann, wie erwähnt, über Art. 6 Abs. 1 lit. f DS-GVO der „Datenpreis" effektiv und unter Berücksichtigung von Drittinteressen behördlich oder gerichtlich gesteuert werden.[1032] Andererseits ist nicht zu verkennen, dass die damit einhergehende Rechtsunsicherheit für den Aufbau innovativer Angebote am Markt nicht unbedingt förderlich ist. Insbesondere für kleine und mittlere Unternehmen sowie Start-ups, die nicht über erfahrene Rechtsabteilungen und nur über begrenzte Ressourcen zur Beauftragung von Rechtsbeistand verfügen, kann sich

---

[1029] Siehe oben, § 2 D.

[1030] Vgl. dazu *Day/Turner/Drozdiak*, Amazon Workers Are Listening to What You Tell Alexa, Bloomberg (11.4.2019), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

[1031] Etwas permissiver *Steege*, MMR 2019, 509 (512) hinsichtlich Daten beim autonomen Fahren.

[1032] *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (282 f.).

die Akzentverschiebung weg vom Einwilligungstatbestand und der vertragserforderlichen Datenverarbeitung hin zur Interessenabwägungsklausel als echtes Hindernis erweisen.

Gerade für diese Gruppen ist eine kontextsensible Konkretisierung daher essenziell. Zu Operationalisierungszwecken kommt ein Rückgriff auf die bisherigen, typisierten, bereichsspezifischen Interessenabwägungen der §§ 28, 28a, 30a BDSG aF jedoch lediglich als argumentative Materialsammlung in Betracht, da diese Normen nicht unionsrechtlich einheitlich galten.[1033] Darüber hinaus stehen *de lege lata* drei spezifische Instrumente zur Verfügung.

Erstens muss durch die Rechtsprechung letztlich eine Fallgruppenbildung, wie bei der Konkretisierung von Generalklauseln generell, vorgenommen werden.[1034] Dies wird jedoch erhebliche Zeit in Anspruch nehmen. Zeitnäher möglich sind zweitens Verhaltensregelungen nach Art. 40 DS-GVO.[1035] Darin kann insbesondere für bestimmte Situationen und Sektoren eine typisierende Interessenabwägung vorgenommen werden, die dann gemäß Art. 40 Abs. 5 DS-GVO von der Aufsichtsbehörde genehmigt und gemäß Art. 40 Abs. 9 DS-GVO sogar durch die Kommission für verbindlich erklärt werden kann. Schließlich vermögen drittens Leitlinien des Europäischen Datenschutzausschusses gem. Art. 70 Abs. 1 S. 2 lit. e DS-GVO eine gewisse Orientierungshilfe zu bieten,[1036] auch wenn ihnen freilich keine Bindungswirkung zukommt. Es steht zu hoffen, dass von diesen Instrumenten möglichst schnell umfangreich Gebrauch gemacht wird. Die Hinweise der Datenschutzkonferenz zur Interpretation von Art. 6 Abs. 1 lit. f DS-GVO sind insoweit prozedural ein Schritt in die richtige Richtung.[1037]

De lege ferenda erscheint es darüber hinaus sinnvoll, auf europäischer Ebene, ähnlich wie bei AGB oder unlauteren Geschäftspraktiken, eine schwarze Liste mit in keinem Fall (vgl. § 309 BGB, Anhang [zu § 3 Absatz 3] UWG) und eine graue Liste mit in der Regel (vgl. § 308 BGB) nicht nach Art. 6 Abs. 1 lit. f DS-GVO zu rechtfertigenden Datenverarbeitungen für typische Verarbeitungssituationen zu erstellen.[1038] Damit ließe sich für eine ganze Spannbreite von Ver-

---

[1033] *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 145.

[1034] Siehe etwa *Beater*, AcP 194 (1994), 82; *Bachmann*, in: MüKo, BGB, 8. Aufl. 2019, § 241 Rn. 55 f.; siehe auch *Röthel*, Normkonkretisierung im Privatrecht, 2004, 103.

[1035] *Schweitzer/Peitz*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf, ZEW Discussion Paper No. 17–043, 2017, http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf, 43; *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (282 f.); *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 145.

[1036] *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 145.

[1037] *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, 11 ff.

[1038] *Kring/Marosi*, K&R 2016, 773 (776); *Policy and Research Group of the Office of the Privacy Commissioner of Canada*, Consent and privacy – A discussion paper exploring po-

arbeitungen auf einen Schlag die Rechtssicherheit merklich erhöhen. Kandidaten für die Aufnahme auf eine schwarze Liste sind zum Beispiel *device fingerprinting*, da dies durch Nutzer kaum kontrollierbar ist und in der Regel unbemerkt geschieht;[1039] das Tracking von Minderjährigen;[1040] sowie schließlich die Nutzung genetischer Testergebnisse für nicht-medizinische Dienstleistungen.[1041]

5. Zusammenfassung zu Art. 6 Abs. 1 lit. f DS-GVO

Die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO ist letztlich immer eine Frage des Einzelfalls. Dennoch können gewisse Leitlinien für die Abwägung angegeben werden. Die relevanten Kriterien lassen sich drei unterschiedlichen Dimensionen zuordnen: den Daten, den Akteuren und der Verarbeitung selbst. Dabei ist letztlich insbesondere relevant, welche datenschutzrechtlichen Risiken von den spezifischen Typen der Daten, Verantwortlichen und dem Verarbeitungsmodus ausgehen.

Auf dieser Basis lassen sich die drei Leitfälle jedenfalls in typisierender Weise entscheiden. Eine Rechtfertigung personalisierter Werbung, die mit einer umfangreichen, systematischen Sammlung personenbezogener Daten zu Präferenzen einhergeht, scheidet danach grundsätzlich aus. Gleiches gilt für das, regelmäßig zudem mit einem Überraschungseffekt verbundene, Tracking durch Drittanbieter. Die Datenerhebung bei Dritten im Rahmen des Internets der Dinge wiederum kann gerechtfertigt sein, wenn besondere Schutzmaßnahmen ergriffen werden und kein intensiver Eingriff durch die Datenerhebung erfolgt. Denn während Geschäftsmodelle, die allein auf Tracking oder personalisierter Werbung beruhen, unschwer durch das Angebot einer datenschonenden Alternative in die Datenschutzrechtskonformität überführt werden können, ist eine gewisse Datenerhebung bei Dritten im Rahmen des Internets der Dinge technisch fast unvermeidlich. Dies beeinflusst die Interessenabwägung nach hier vertretener Auffassung entscheidend. Zur Erhöhung der Rechtssicherheit sollten auf europäischer Ebene letztlich eine schwarze und eine graue Liste mit Verarbeitungsformen erstellt werden, welche über die Interessenabwägungsklausel nie oder in der Regel nicht gerechtfertigt werden können.

---

tential enhancements to consent under the Personal Information Protection and Electronic Documents Act, 2016, 17 (no-go-zones); siehe auch *Kampert*, Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, 2016, 183 ff. zur Diskussion um ein „Rote-Linie-Gesetz" im Fall Google Street View.

[1039] *Policy and Research Group of the Office of the Privacy Commissioner of Canada*, Consent and privacy – A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act, 2016, 17.

[1040] *Policy and Research Group of the Office of the Privacy Commissioner of Canada*, Consent and privacy – A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act, 2016, 17.

[1041] *Policy and Research Group of the Office of the Privacy Commissioner of Canada*, Consent and privacy – A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act, 2016, 17.

II. Die Änderung der Verarbeitungszwecke, Art. 6 Abs. 4 DS-GVO

Eine weitere Ebene der datenschutzrechtlichen Regulierungsstruktur zieht Art. 6 Abs. 4 DS-GVO für die Änderung des Verarbeitungszwecks ein. Diese Regelung ist im Rahmen neuer Technologien ebenso relevant wie umstritten.

1. Relevanz

Die bisherigen Untersuchungen zu Art. 6 Abs. 1 DS-GVO haben gezeigt, dass werbe- und trackingbasierte Geschäftsmodelle ohne das Angebot einer datenschonenden Alternative nur äußerst schwer datenschutzrechtskonform realisiert werden können. Ein letzter Ausweg böte sich womöglich dann, wenn die Daten zu anderen Zwecken rechtmäßig gesammelt und anschließend im Wege einer Zweckänderung rechtmäßig für Werbung verwendet werden könnten. Dieser Umweg über eine Zweckänderung ist in der Tat denkbar und Gegenstand erheblicher Diskussionen in der Literatur. Ansatzpunkt ist, dass Art. 6 Abs. 4 DS-GVO eine eigenständige Regelung für die Zweckänderung beinhaltet, die diese scheinbar leichter ermöglicht als die originäre Datenerhebung. Diese Regelung ist insbesondere auch für Techniken maschinellen Lernens relevant, bei denen Daten neuen Nutzungsformen zugeführt werden (sog. *secondary use*[1042]), um aus bestehenden Daten neue Korrelationen zu gewinnen.[1043]

2. Kein eigener Erlaubnistatbestand

Art. 6 Abs. 4 DS-GVO stellt eine Reihe von Voraussetzungen für eine Zweckänderung auf. Tatbestandlich einschlägig ist die Vorschrift, wenn eine Zweckänderung gegenüber dem ursprünglichen Erhebungszweck vorgenommen wird und die Verarbeitung weder auf einer Einwilligung noch auf einer spezifischen unionalen oder mitgliedstaatlichen Rechtsvorschrift beruht.[1044] In diesem Fall muss der Verantwortliche feststellen, ob die Verarbeitung zu dem neuen Zweck mit dem ursprünglichen Zweck vereinbar ist. Bei diesem Kompatibilitätstest hat er gemäß Art. 6 Abs. 4 DS-GVO fünf Kriterien zu berücksichtigen: die Verbindung zwischen dem neuen und dem ursprünglichen Zweck; den Kontext der ursprünglichen Erhebung; die Art der personenbezogenen Daten, insbesondere sensitive Daten; die Folgen der Weiterverarbeitung für die betroffene Person; sowie das Bestehen geeigneter Schutzvorkehrungen wie etwa Verschlüsselung oder Pseudonymisierung.

[1042] Siehe dazu bereits oben, Text bei § 4, Fn. 395.

[1043] Zur Problematik der Zweckbindung in diesem Kontext *Roßnagel*, ZD 2013, 562 (564); *von Grafenstein*, DuD 2015, 789; *Buchner*, DuD 2016, 155 (156 f.); *Culik/Döpke*, ZD 2017, 226.

[1044] Dazu *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 199 f.

Streit ist nun um die Frage entbrannt, ob diese Kriterien zusätzlich zu oder anstelle von Art. 6 Abs. 1 DS-GVO erfüllt sein müssen, ob Art. 6 Abs. 4 DS-GVO mithin einen eigenen Erlaubnistatbestand darstellt. Dies suggeriert insbesondere der zweite Satz des 50. Erwägungsgrunds der DS-GVO, der explizit davon spricht, dass bei Erfüllung der Voraussetzungen von Art. 6 Abs. 4 DS-GVO keine weitere Rechtsgrundlage als jene der ursprünglichen Erhebung notwendig ist.

Nach hier vertretener Auffassung ist, unabhängig davon, ob die Fassung des 50. Erwägungsgrunds ein Redaktionsversehen darstellt, das einen früheren Verhandlungsstand abbildet,[1045] Art. 6 Abs. 4 DS-GVO lediglich als zusätzliche Konkretisierung des Zweckbindungsgrundsatzes, nicht als eigenständiger Erlaubnistatbestand zu verstehen.[1046] Denn die systematische Auslegung von Art. 6 DS-GVO ergibt keinen Anhaltspunkt dafür, dass Art. 6 Abs. 4 DS-GVO an die Stelle des ersten Absatzes treten soll.[1047] Dies wäre auch aus teleologischer Perspektive ein widersinniges Ergebnis, da sonst für alle Verarbeitungen *innerhalb* des ursprünglichen Zwecks die strengeren Anforderungen des Art. 6 Abs. 1 DS-GVO gälten, nicht aber für andere Zwecke, die freilich mit Blick auf den Grundsatz der Zweckbindung und der Datenminimierung sowie die Kontrolle der Betroffenen über ihre Daten, die ausweislich des siebten Erwägungsgrundes eine zentrale Zielsetzung der DS-GVO darstellt, gerade besonders problematisch erscheinen. Zudem ergäbe sich ein Wertungswiderspruch hinsichtlich rechtswidriger Verarbeitungspraktiken wie etwa typischen Konstellationen personalisierter Werbung. Bei Erhebung der Daten unmittelbar zu diesem Zweck wäre die Verarbeitung rechtswidrig. Werden jedoch Daten zu einem anderen, mit der rechtswidrigen Praxis zu vereinbarenden, rechtmäßigen Zweck erhoben und dann einer Zweckänderung unterworfen, wäre die bei direkter Verwendung rechtswidrige Praxis aufgrund des Umwegs über die Zweckänderung rechtmäßig.[1048] Dies stellt jedoch einen nicht hinnehmbaren Wertungswiderspruch dar. Diese systematischen und teleologischen Erwägungen zur Interpretation der Norm selbst sind insgesamt gewichtiger als die nicht bindenden Aussagen des 50. Erwägungsgrunds. Letztlich streitet für eine

---

[1045] So *Schantz*, NJW 2016, 1841 (1844).

[1046] *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 28 f.; *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 183; *Albers/Veit*, in: BeckOK DatenschutzR, 28. Ed. 1.5.2019, Art. 6 DS-GVO Rn. 75; *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 6 Rn. 48; aA *Ziegenhorn/von Heckel*, NVwZ 2016, 1585 (1590); *Kühling/Martini*, EuZW 2016, 448 (451); *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 4 DS-GVO Rn. 12; *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 210; *Monreal*, ZD 2016, 507 (510); *Culik/Döpke*, ZD 2017, 226 (230).

[1047] *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 183.

[1048] Vgl. *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 211, 78.

Trennung von Zweckbindung und Erlaubnistatbestand auch Art. 8 Abs. 2 S. 1 GRCh.[1049]

Schließlich ist hinsichtlich der Nutzung von in anderen Kontexten erhobenen Daten für die Zwecke maschinellen Lernens anzumerken, dass eine Rechtmäßigkeit der Verarbeitung über Art. 6 Abs. 1 lit. f DS-GVO durchaus möglich erscheint, wenn die Anwendung erheblichen Nutzen verspricht, Daten hinreichend pseudonymisiert werden und zum Beispiel ein Widerspruchsrecht anlassunabhängig angeboten wird. Damit werden insoweit innovative Verfahren nicht durch das Datenschutzrecht im Keim erstickt. Ist der Kompatibilitätstest erfüllt, so darf dann auf die bestehenden Daten zugegriffen werden; ist dies nicht der Fall, so müssen die Daten neu erhoben werden.[1050] Für die drei Leitfälle bleibt es jedoch dabei, dass Art. 6 Abs. 4 DS-GVO nichts am Ergebnis der Analyse von Art. 6 Abs. 1 DS-GVO ändern kann. Art. 6 Abs. 4 DS-GVO installiert gegenüber diesem Absatz lediglich eine weitere regulatorische Ebene mit zusätzlichen Kriterien.

III. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DS-GVO

Ausweislich des 78. Erwägungsgrunds der DS-GVO sollen der Datenschutz durch Technikgestaltung (*data protection by design*) und durch datenschutzfreundliche Voreinstellungen (*data protection by default*) die Grundrechte und Freiheiten der Nutzer sichern helfen. Diese Prinzipien sind schon seit langem in der datenschutzrechtlichen Diskussion unter dem Schlagwort *privacy by design* etabliert,[1051] in der DS-GVO jedoch erstmals auf unionaler Ebene, wenngleich in einer auf den unionalen Datenschutz zugespitzten Form,[1052] mit Rechtswir-

[1049] *Article 29 Data Protection Working Party*, Opinion 03/2013 on purpose limitation, WP 203, 2013, 12 Fn. 28.

[1050] *Buchner/Petri*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 6 DS-GVO Rn. 185; damit löst sich auch der vermeintliche Wertungswiderspruch einer Privilegierung der starken gegenüber der moderaten Zweckänderung, den *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 4 DS-GVO Rn. 12 ausmachen will.

[1051] Siehe etwa *Van Rossum et al.*, Privacy-Enhancing Technologies: The Path to Anonymity, 1995; *Borking*, DuD 1996, 654; *AK Technik der Datenschutzbeauftragten des Bundes und der Länder*, Arbeitspapier „Datenschutzfreundliche Technologien", 1997, http://www.datenschutz-bayern.de/technik/grundsatz/apdsft.htm; *Langheinrich*, in: Abowd et al. (Hrsg.), Ubicomp 2001: Ubiquitous Computing, 2001, 273; *Hoepman*, IFIP International Information Security Conference 2014, 446; Mitteilung der Kommission an das Europäische Parlament und den Rat über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre, KOM(2007) 228 endgültig; *Cavoukian*, Privacy by Design – The 7 Foundational Principles, 2009/2011; *International Conference of Data Protection and Privacy Commissioners*, Resolution on Privacy by Design, 2010; *Rubinstein*, 26 Berkeley Technology Law Journal 2011, 1409.

[1052] Zur Unterscheidung von *privacy by design* und *data protection by design Baumgartner/Gausling*, ZD 2017, 308 (309).

kung ausgestattet worden.[1053] Sie sind integraler Teil des risikobasierten Ansatzes der DS-GVO, da es für ihre Ausgestaltung ganz maßgeblich auf die Schwere und Eintrittswahrscheinlichkeit der datenschutzrechtlichen Risiken ankommt (Art. 25 Abs. 1 DS-GVO).[1054] Dabei kommt ihnen auch faktisch eine ganz erhebliche Relevanz zu, die sich vor allem aus den empirischen Defiziten des individuellen Kontrollregimes speist.

1. Relevanz

Art. 25 DS-GVO ähnelt in Konzeption und Bedeutung den Grundsätzen der Datenverarbeitung nach Art. 5 Abs. 1 DS-GVO. Auf zwei dieser Grundsätze, die Datenminimierung und den Zweckbindungsgrundsatz, nimmt er konkret Bezug, die anderen werden über die „Anforderungen dieser Verordnung" (Art. 25 Abs. 1 DS-GVO) angesprochen.[1055] Vor allem aber eignet ihm, wie den Grundsätzen nach Art. 5 Abs. 1 DS-GVO, einerseits eine tatbestandliche Vagheit, die andererseits mit einer weiten konzeptionellen Prägekraft einhergeht. Die in Art. 25 DS-GVO festgehaltenen Pflichten gelten für jegliche Form der Datenverarbeitung und sind auch bei der Auslegung spezifischer Pflichten, wie bereits gesehen, zu berücksichtigen.[1056] Insofern wäre eine Verortung im Rahmen der Grundsätze des Art. 5 Abs. 1 DS-GVO durchaus angezeigt gewesen. In der Sache jedenfalls handelt es sich bei den Anforderungen des Datenschutzes durch Technikgestaltung und durch Voreinstellungen um zentrale Grundsätze der Datenverarbeitung nach der DS-GVO.[1057]

In tatsächlicher Hinsicht ist Art. 25 DS-GVO besonders wichtig, wenn Datenverarbeitungsvorgänge notwendig komplex und daher die Voraussetzungen für einen selbstbestimmten Umgang der Nutzer mit Daten kaum gegeben sind. Dies ist etwa bei mehrstufigen Bearbeitungsprozessen durch verschiedene Verantwortliche im Rahmen des Internets der Dinge der Fall.[1058] Aber auch die bereits thematisierten empirischen Begrenzungen der Datensouveränität auf Grundlage der Einwilligung und der vertragserforderlichen Datenverarbeitung zeigen deutlich die Notwendigkeit auf, Datenschutz vom individuel-

---

[1053] Siehe aber die Vorläufer im 46. Erwägungsgrund und Art. 17 DSRL, dort jedoch vor allem auf die IT-Sicherheit bezogen; dazu *Bygrave*, 4 Oslo Law Review 2017, 105.

[1054] *Mantz*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 25 DS-GVO Rn. 21.

[1055] *Baumgartner/Gausling*, ZD 2017, 308 (310).

[1056] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 15.

[1057] Vgl. *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 15; siehe auch, zur allgemeinen Bedeutung für das Datenschutzrecht, *International Conference of Data Protection and Privacy Commissioners*, Resolution on Privacy by Design, 2010.

[1058] *Bolognini/Ziegler*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 93 (95); *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 22, 25.

len Kontrolldogma zu befreien und noch stärker als bisher auf die technische Ebene zu verlagern. Denn unter den Bedingungen von rationaler Ignoranz und verhaltensökonomischen Effekten ist es essenziell, dass an die Seite einer individuellen Kontrolle der Datenverarbeitung durch die betroffenen Personen, und partiell auch an deren Stelle, die Sicherstellung der Grundsätze der Datenverarbeitung bereits auf der technischen Ebene tritt. Nur so lässt sich informationelle Selbstbestimmung effektiv durchsetzen.[1059] Gerade in stark vernetzten Umgebungen wäre die Alternative eine Dauerschleife an Einwilligungsanfragen und Einstellungsnotwendigkeiten, die von Nutzern weder gewollt sind noch geleistet werden können.[1060] Die Relevanz von Art. 25 DS-GVO kann daher kaum überschätzt werden und steht zu Recht an vorderster Front der datenschutzrechtlichen Diskussion und Praxis.[1061] Diese Erwägungen werden auch im dritten Teil der Arbeit, bei den technischen Reformansätzen, nochmals vertieft aufgegriffen.[1062]

2. *Rechtfertigung*

Eine erste Linie der Rechtfertigung von *privacy by default* und ähnlichen Instrumenten verweist darauf, dass die durch Tracking verursachten sozialen Kosten größer sind als der soziale Nutzen und daher Tracking, wo schon nicht verboten, so wenigstens erschwert werden muss.[1063] Diese Kosten-Nutzen Rechnung kann jedoch so pauschal nicht aufgehen;[1064] vielmehr müsste hier eine granulare Betrachtung der einzelnen Formen der Datenverarbeitung erfolgen, mit ungewissem Ergebnis, da sich viele Risiken der Datenverarbeitung nur äußerst schwer quantifizieren lassen.[1065] Zudem wurde bereits darauf hingewiesen, dass auch Tracking durchaus positive Effekte für den Einzelnen haben kann.[1066]

Ein zweites Argument lautet, dass *privacy by default* dem im dritten Kapitel der Arbeit beschriebenen,[1067] verhaltensökonomisch bedingten Marktversagen entgegenwirken sollen.[1068] Wenn tatsächlich Nutzer die Risiken der Datenver-

---

[1059] *Roßnagel*, MMR 2005, 71 (74).

[1060] *Roßnagel*, MMR 2005, 71 (72); *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 168 f.

[1061] Siehe etwa *Hansen/Limniotis*, Recommendations on shaping technology according to GDPR provisions. Exploring the notion of data protection by default, ENISA Report, 2018; *Bygrave*, 4 Oslo Law Review 2017, 105; *Islam*, Privacy by Design for Social Networks, PhD Thesis, 2014.

[1062] Siehe unten, § 6 B.I.

[1063] Vgl. *Soghoian*, End the Charade: Regulators Must Protect Users' Privacy by Default, Paper for the *Office of the Privacy Commissioner of Canada*, 2010; *Willis*, 29 Berkeley Technology Law Journal 2014, 61 (88 f.).

[1064] *Willis*, 29 Berkeley Technology Law Journal 2014, 61 (130).

[1065] Siehe unten, Text bei § 4, Fn. 1098.

[1066] Siehe oben, § 3 B.I.

[1067] Siehe oben, § 3 B.II.1.b).

[1068] *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 311 f.

arbeitung im Schnitt unterschätzen, so kann dies durch eine dispositive Regelung zugunsten des Datenschutzes tendenziell ausgeglichen werden: Der *status quo bias*[1069] sorgt dann dafür, dass eine signifikante Anzahl von Nutzern keine Regelung trifft und sich die Unterschätzung der Risiken für sie nicht nachteilig auswirkt.[1070] Dem kann man jedoch entgegenhalten, dass mit diesem Mechanismus einerseits eine autonome Ausübung von Datensouveränität nicht unbedingt gefördert wird[1071] und andererseits keineswegs gesagt ist, dass der *status quo bias* eine etwaige Unterschätzung von Risiken genau ausgleicht und nicht seinerseits eine Verzerrung in die entgegengesetzte Richtung bewirkt.[1072]

Eine bessere Rechtfertigung bietet daher ein Blick auf die ökonomische Struktur von dispositiven Regeln. An *privacy by default* wird in der Literatur bisweilen kritisiert, dass eine derartige Regel den Präferenzen von Nutzern, deren Interesse an Datenschutz gering ausgeprägt ist, widerspricht.[1073] Dies ist richtig, allerdings muss zugleich bedacht werden, dass *tracking by default* in gleicher Weise die Präferenzen von Nutzern mit stark ausgeprägtem Interesse an Datenschutz missachtet. Bei der Wahl zwischen diesen beiden dispositiven Regeln[1074] spricht nicht nur die Verwirklichung des Datenschutzgrundrechts, sondern auch eine weitere Erwägung entscheidend für *privacy by default*: Diese Regel kann letztlich als ein sogenannter *penalty default* angesehen werden.[1075] Darunter versteht man dispositive Regelungen, die nicht versuchen, die Präferenzen der Mehrheit der Betroffenen abzubilden, sondern die Anreize für eine informationell bessergestellte Partei setzen, durch Informationen und Handlungen die Informationsasymmetrie auszugleichen und die andere Partei zu einem Opt-Out zu bewegen.[1076] Auf den Fall der Datenverarbeitung gewendet bedeutet dies: Unternehmen haben gegenüber Nutzern nicht nur einen erheblichen Wissensvorsprung, sondern bestimmen regelmäßig auch das Design des Opt-Out aus der dispositiven Regel. Lautet die Regel *tracking by default*, so haben Unternehmen (infolge rationaler Ignoranz) nur geringe An-

[1069] Dazu *Samuelson/Zeckhauser*, 1 Journal of Risk and Uncertainty 1988, 7; *Hacker*, Verhaltensökonomik und Normativität, 2017, 85 f.; *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 264 ff.; *Baumgartner/Gausling*, ZD 2017, 308 (312); *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (9).

[1070] Vgl. *Kesan/Shah*, 82 Notre Dame Law Review 2006, 583 (602).

[1071] Siehe bereits oben, Text bei § 4, Fn. 317 und ausführlich *Hacker*, Verhaltensökonomik und Normativität, 2017, 221 ff. und 622.

[1072] *Hacker*, Verhaltensökonomik und Normativität, 2017, 605 ff.

[1073] Vgl. *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 9; *Kapsner/Sandfuchs*, 6 Review of Philosophy and Psychology, 2015, 455 (460).

[1074] Für mögliche Zwischenstufen, siehe *Willis*, 29 Berkeley Technology Law Journal 2014, 61 (86 f.).

[1075] *P. Schwartz*, 117 Harvard Law Review 2004, 2055 (2100); *Kesan/Shah*, 82 Notre Dame Law Review 2006, 583 (620 f., 632 f.); *Willis*, 29 Berkeley Technology Law Journal 2014, 61 (89); *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 10.

[1076] Grundlegend *Ayres/Gertner*, 99 Yale Law Journal 1989, 87 (94, 97 ff.); siehe ferner *Korobkin*, 83 Cornell Law Review 1998, 608 (617–618); *Möslein*, Dispositives Recht, 2011, 324 ff.

reize, Informationen zur Datenverarbeitung kognitiv zu optimieren und einfache Möglichkeiten des Opt-Out bereitzustellen: Datenschutz ist gegenwärtig kein wirksamer Wettbewerbsparameter.[1077] Dies zeigt sich zum Beispiel an den teilweise komplexen Schritten, die notwendig sind, um bei großen Online-Firmen einen gegen *tracking* gerichteten Opt-Out durchsetzen zu können.[1078] Bei umgekehrter Regelung, *privacy by default*, haben Anbieter hingegen erhebliche Anreize, Informationen verständlich bereitzustellen und den Opt-Out einfach zu gestalten, um Nutzer zu einem Opt-Out aus der dispositiven Regel, der sich dann als ein Hineinoptieren in die Datenverarbeitung darstellt, zu bewegen.[1079] Insgesamt können daher bei dieser Regelung eine deutlich bessere Informationslage und auch eine erhebliche Vereinfachung der Möglichkeit der Ausübung von Wahlfreiheit seitens der Nutzer erwartet werden. *Privacy by default* ist daher für Nutzer mit niedrigen Datenschutzpräferenzen grundsätzlich günstiger als *tracking by default* für Nutzer mit stark ausgeprägten Datenschutzpräferenzen und sorgt zugleich für eine Verbesserung der Voraussetzungen für autonome und informierte Entscheidungen.

Hinzu kommt schließlich, dass *privacy by design* nicht nur bei einer individualistischen Perspektive, sondern auch mit Blick auf die kollektive Dimension des Datenschutzes überzeugt: Soweit es zu einem tatsächlichen Absinken der veröffentlichten Informationen führt, werden negative Externalitäten der Datenveröffentlichung reduziert.[1080] Die Aufnahme von Art. 25 DS-GVO in den Kanon des Datenschutzrechts ist daher insgesamt folgerichtig.[1081]

4. Verpflichtungsgrad

Inhaltlich sind sowohl der Datenschutz durch Technikgestaltung als auch durch datenschutzrechtliche Voreinstellungen, wie auch die Grundsätze nach Abs. 5 Abs. 1 DS-GVO, als echte Pflichten ausgestaltet, deren Verletzung nach Art. 83 Abs. 4 lit. a DS-GVO sanktionsbewehrt ist, wenngleich in geringerem Umfang als die Verletzung der Grundsätze der Datenverarbeitung nach Art. 5 Abs. 1 i. V. m. Art. 83 Abs. 5 lit. a DS-GVO. Allerdings wird umgekehrt die Er-

[1077] *Warner/Sloan*, 15 Vanderbilt Journal of Entertainment and Technology Law 2012, 49 (60 f., 63 f.); *Autorité de la Concurrence/Bundeskartellamt*, Competition Law and Data, Joint Report (10.5.2016), 24 f.; *Kerber*, GRUR Int. 2016, 639 (642); *Botta/Wiedemann*, The Antitrust Bulletin 2019, 428 (433).

[1078] Siehe nur den Bericht der norwegischen Verbraucherbehörde *Forbrukerrådet*, Deceived by Design, Bericht, 2018; ferner *Conti/Sobiesk*, Proceedings of the 19th International Conference on World Wide Web 2010, 271; *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (4); vgl. auch *Willis*, 29 Berkeley Technology Law Journal 2014, 61 (99 ff.).

[1079] *Willis*, 29 Berkeley Technology Law Journal 2014, 61 (89).

[1080] Siehe zu den negativen Externalitäten oben, § 3 B.II.1.c).

[1081] Vgl. zur (zu bejahenden) Grundrechtskonformität von Art. 25 Abs. 2 DS-GVO auch *Krönke*, Der Staat 55 (2016), 319 (349); sehr kritisch hingegen, wegen einer vermeintlichen subliminalen „Moralsteuerung" der Nutzer, *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 315 f.

füllung der aus Art. 25 DS-GVO resultierenden Pflichten gemäß Art. 83 Abs. 2 lit. d DS-GVO bei der Berechnung einer Geldbuße wegen einer anderweitigen Verletzung der DS-GVO positiv berücksichtigt.

4. Inhaltliche Ausformung

In inhaltlicher Hinsicht besteht eine ersichtlich enge Verbindung mit den Grundsätzen der Datenverarbeitung.

a) Art. 25 Abs. 1 DS-GVO

Nach Art. 25 Abs. 1 DS-GVO muss die Erfüllung der Anforderungen der DS-GVO, und besonders der Grundsatz der Datenminimierung, bereits auf technischer Ebene durch „geeignete technische und organisatorische Maßnahmen" sichergestellt werden. Als einziges Beispiel nennt der Wortlaut die Pseudonymisierung. Daneben werden im 78. Erwägungsgrund noch weitere Verfahren genannt, etwa Transparenz hinsichtlich der Funktion der Verarbeitung und technische Kontrollmöglichkeiten für Nutzer. Anders als in Art. 10 des Entwurfs der ePrivacy-Verordnung[1082] werden Hersteller freilich durch Art. 25 Abs. 1 DS-GVO nicht unmittelbar in die Pflicht genommen, sondern im 78. Erwägungsgrund lediglich ermutigt, Datenschutz auf technischer Ebene beim Produktdesign zu verwirklichen.[1083] Der Hersteller kann jedoch womöglich nach Maßgabe der deliktischen Produzentenhaftung für Produkte haften, die nicht datenschutzrechtskonform nutzbar sind.[1084] Art. 25 Abs. 1 DS-GVO hingegen entfaltet unmittelbare Wirkung nur, soweit der Verantwortliche selbst das Design der Verarbeitung bestimmt. Wird dieses dagegen durch einen vom Verantwortlichen verschiedenen Hersteller implementiert, so trifft den Verantwortlichen immerhin die Pflicht, zwischen unterschiedlichen, funktional im Wesentlichen äquivalenten Produkten so auszuwählen, dass dem Grundsatz des Datenschutzes durch Technikgestaltung möglichst weitgehend Rechnung getragen wird.[1085] Inwiefern eine eigene Pflicht des Verantwortlichen besteht, den Einsatz von Instrumenten des Selbstdatenschutzes *durch Nutzer* zu unterstützen oder zu tolerieren, wird an anderer Stelle genauer untersucht.[1086]

[1082] Dazu oben, § 4 B.I.4.c)bb).

[1083] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 20 f.; *Specht-Riemenschneider*, MMR 2020, 73 (74); siehe aber auch weitergehend *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 26.

[1084] Dazu ausführlich *Specht-Riemenschneider*, MMR 2020, 73 (75 ff., besonders 77).

[1085] *Baumgartner/Gausling*, ZD 2017, 308 (311); vgl. auch *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 19; *Hansen/Limniotis*, Recommendations on shaping technology according to GDPR provisions. Exploring the notion of data protection by default, ENISA Report, 2018, 15; *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 25 DS-GVO Rn. 13.

[1086] Siehe oben, S. 219, sowie unten, § 6 B.I.2.

b) Art. 25 Abs. 2 DS-GVO

Nach Art. 25 Abs. 2 DS-GVO dürfen ferner Voreinstellungen nur solche Verarbeitungen zulassen, die für den jeweiligen Verarbeitungszweck erforderlich sind. Die Voreinstellungen müssen sich damit im Rahmen des Zweckbindungsgrundsatzes, Art. 5 Abs. 1 lit. b DS-GVO, bewegen. Letztlich ist dies ein Unterfall des Datenschutzes durch Technikgestaltung, eben durch Gestaltung der Voreinstellungen.[1087] Dass diese aufgrund verhaltensökonomischer Effekte zentral sind, wurde bereits thematisiert.[1088]

Damit wird entscheidend, welche Zwecke eine Verarbeitung jeweils verfolgt. Problematisch ist, dass den Zweck eigentlich einseitig der Verarbeiter setzt.[1089] Damit wäre denkbar, dass der Verantwortliche einen ihm opportunen, bestimmten Zweck (Schaltung personalisierter Werbung) frei definiert und die Voreinstellungen daran ausrichten kann.[1090] Jedoch muss die betroffene Person eine Einwilligung gerade in Bezug auf einen bestimmten Zweck geben (Art. 6 Abs. 1 lit. a DS-GVO), und auch bei der vertragserforderlichen Datenverarbeitung gem. Art. 6 Abs. 1 lit. b DS-GVO ist die Zustimmung zum Vertrag, und damit implizit den damit verfolgten Zwecken, notwendig. Lediglich bei Art. 6 Abs. 1 lit. f DS-GVO ist daher eine Zustimmung der betroffenen Person zum jeweiligen Zweck entbehrlich. Doch auch für im Rahmen der Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO legitime Verarbeitungen und darauf bezogene Zwecke müssen Voreinstellungen entsprechend gewählt werden können. Denn Art. 25 Abs. 2 DS-GVO verpflichtet gerade nicht – wie im Diskurs zu *privacy by default* häufig gefordert[1091] – zu einem absoluten Minimum an Datenüberlassung durch die Voreinstellungen, sondern orientiert sich, ähnlich wie Art. 5 Abs. 1 lit. c DS-GVO, am Zweck der konkreten Verarbeitung.[1092]

Richtigerweise wird man daher den für Art. 25 Abs. 2 DS-GVO relevanten Zweck mit Blick auf die Rechtmäßigkeit der Verarbeitung bestimmen können: Nur solche Zwecke sind relevant, die sich auf rechtmäßige Datenverarbeitungen beziehen.[1093] Bei Zugrundelegung der Ausführungen zu Art. 6 Abs. 1 lit. b

---

[1087] *Cavoukian*, Privacy by Design – The 7 Foundational Principles, 2009/2011, 2; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 8.

[1088] Siehe oben, Text bei § 4, Fn. 875.

[1089] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 68.

[1090] *Koops/Leenes*, 28 International Review of Law, Computers & Technology 2014, 159 (164 f.); *Roßnagel/Richter/Nebel*, ZD 2013, 103 (106).

[1091] Für dahingehende *best practices Hansen/Limniotis*, Recommendations on shaping technology according to GDPR provisions. Exploring the notion of data protection by default, ENISA Report, 2018, 22.

[1092] *Baumgartner/Gausling*, ZD 2017, 308 (313).

[1093] *Koops/Leenes*, 28 International Review of Law, Computers & Technology 2014, 159 (164 f.); *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 25 DS-GVO Rn. 28.

DS-GVO[1094] bedeutet dies insbesondere, dass die Parteien subjektiv Zwecke frei (im Rahmen der Grenzen der Rechtsordnung) vereinbaren können, die Erfüllung von Nutzerpflichten zur Überlassung von Daten bzw. die Erfüllung einer Bedingung für die Dienstbereitstellung dabei jedoch außen vor bleiben muss. Denn sonst würde Art. 25 Abs. 2 DS-GVO bei datenfinanzierten Diensten im Wesentlichen leerlaufen, was der gesetzlichen Intention zuwiderliefe.[1095]

c) Operationalisierung

Beide Absätze des Art. 25 DS-GVO sind eng mit den in der DS-GVO angelegten und sogleich noch näher zu besprechenden Formen der regulierten Selbstregulierung verknüpft. Einerseits ist eine Präzisierung der Anforderungen aus Abs. 25 DS-GVO in genehmigten Verhaltensregeln möglich, Art. 40 Abs. 2 lit. h DS-GVO. Andererseits kann nach Art. 25 Abs. 3 DS-GVO „[e]in genehmigtes Zertifizierungsverfahren gemäß Artikel 42 […] als Faktor herangezogen werden, um die Erfüllung der [aus Art. 25 Abs. 1 und 2 DS-GVO resultierenden] Anforderungen nachzuweisen."

Solche Spezifizierungen sind auch dringend nötig, um die vagen und einzelfallbezogenen Anforderungen des Art. 25 DS-GVO praxistauglich zu machen.[1096] Dabei muss insbesondere geklärt werden, welche Anstrengungen und Kosten den Verantwortlichen für die Berücksichtigung der datenschutzrechtlichen Anforderungen bei der Technikgestaltung auferlegt werden können. Diese sind, zusammen mit den anderen in Art. 25 Abs. 1 DS-GVO genannten Abwägungskriterien, den datenschutzrechtlichen Risiken gegenüberzustellen.[1097] Ein rein effizienzbasiertes Kalkül, welches den marginalen Nutzengewinn der Nutzer mit den marginalen Kosten der Verantwortlichen vergleicht und letzteren bis zu einem Überwiegen der Kosten Pflichten auferlegt, ist im datenschutzrechtlichen Bereich aufgrund der kaum möglichen Quantifizierung des Nutzengewinns der betroffenen Personen praktisch nicht operationalisierbar.[1098] Daher wird man sich mit qualitativen Aussagen behelfen müssen, die eine Abwägung, ähnlich wie bei Art. 6 Abs. 1 lit. f DS-GVO, nachvoll-

[1094] Dazu oben, § 4 B.II.2.b)bb).

[1095] Diese speist sich gerade aus der Regulierung der Voreinstellungen im Bereich sozialer Netzwerke, siehe *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 43 und 53 sowie Art. 25 Abs. 2 S. 3 DS-GVO, der klar (auch) auf Posts in sozialen Netzwerken ausgerichtet ist, siehe *Baumgartner/Gausling*, ZD 2017, 308 (313); zu *privacy by design* und sozialen Netzwerken ausführlich *Islam*, Privacy by Design for Social Networks, PhD Thesis, 2014.

[1096] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 25.

[1097] Zu den Abwägungskriterien im Einzelnen *Mantz*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 25 DS-GVO Rn. 36 ff.; *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 25 DS-GVO Rn. 19 ff.

[1098] Vgl. zu derartigen Operationalisierungsschwierigkeiten *Hacker*, Verhaltensökonomik und Normativität, 2017, 326 ff. und 922; spezifisch mit Blick auf Datenverarbeitungsprozesse *Ben-Shahar*, 11 Journal of Legal Analysis, 2019, 104 (109, 131 f.).

ziehbar machen[1099] und dabei auch auf die Einsatzfähigkeit und Wirkmächtigkeit der verfügbaren datenschützenden Techniken eingehen.[1100] Diverse Techniken, mit denen *data protection by design* umgesetzt werden kann, sind bereits Gegenstand der Forschung und Anwendung (dazu im Einzelnen unten, § 6 B.II.1.).[1101]

5. *Anwendung auf die drei Leitfälle*

Die potenzielle Sprengkraft von Art. 25 DS-GVO erhellt am klarsten aus seiner Anwendung auf die drei Leitfälle. Hier ist insbesondere zu fragen, ob ein Drittbezug (in allen Leitfällen) bereits durch das Design verhindert und separat vom Betroffenen aktiviert werden muss.[1102]

a) Datenweiterleitung an Dritte

Im Rahmen der Datenweiterleitung, etwa zu Zwecken personalisierter Werbung, stellt sich damit die Frage, ob eine derartige Konnektivität von vornherein Teil einer Anwendung oder eines IoT-Geräts sein darf. Denn das Design und die Voreinstellungen müssen, wie gesehen, zur Datenminimierung beitragen und dem Zweckbindungsgrundsatz genügen.

Dies bedeutet erstens, dass die Daten, beispielsweise innerhalb des Internets der Dinge, gerade nicht standardmäßig zu Werbezwecken genutzt werden dürfen, wenn dies nicht einen klar kommunizierten Zweck des Gerätes ausmacht (und die übrigen Rechtmäßigkeitsvoraussetzungen erfüllt sind). Denn mit der Profilbildung zu Werbezwecken sind, wie ausgeführt, typischerweise erhebliche datenschutzrechtliche Risiken verbunden,[1103] weswegen sie zumeist im Rahmen gegenwärtiger Geschäftsmodelle rechtswidrig ist.[1104] Vielmehr muss die standardmäßige Datenweiterleitung auf funktional notwendige bzw. effiziente Verteilungen zwischen verschiedenen Akteuren beschränkt bleiben.[1105] Dies trifft die Anbieter innerhalb des Internets der Dinge auch nicht unverhältnismäßig stark, da typischerweise die IoT-Produkte ohnehin mit einer monetären Zahlung erworben werden (data on top-Modell), sodass die Monetarisierung von Daten über Werbekanäle keinesfalls die einzige oder Haupteinnahmequelle darstellt. Bei rein datenfinanzierten Diensten kann der Ver-

[1099] Vgl. *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 25.

[1100] Dazu ausführlich *Hansen/Hoepman/Jensen*, Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, ENISA Report, 2015, 12 ff.

[1101] Siehe etwa den Überblick bei *Danezis et al.*, Privacy and Data Protection by Design – from policy to engineering, ENISA Report, 2014, 22 ff.; *Islam*, Privacy by Design for Social Networks, PhD Thesis, 2014.

[1102] Dies bejahend *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 39.

[1103] Dazu oben, Text bei § 4, Fn. 1009.

[1104] Siehe oben, § 4 B.I.6., § 5 D.II.3. und § 5 E.I.5.

[1105] Dazu oben, Text bei § 3, Fn. 172.

antwortliche wiederum die Nutzer vor die Wahl stellen, die Voreinstellungen zugunsten der Werbefinanzierung abzuändern oder monetär zu bezahlen.

Zweitens müssen Daten, soweit dies für die Erfüllung der Verarbeitungsziele möglich ist, in anonymisierter Form ausgewertet werden. Dies ist etwa denkbar, wenn Profile über den Verkehrsfluss zur Optimierung der Routenplanung erstellt werden. Dabei entspricht lediglich eine Vorgehensweise dem Grundsatz des Datenschutzes durch Technikgestaltung, bei welcher nicht auf die Rohdaten der einzelnen Nutzer, sondern lediglich auf die aggregierten Gesamtdaten zugegriffen wird.[1106]

Drittens muss standardmäßig eine Löschung von Daten unmittelbar nach der Nutzung durch das Gerät erfolgen, etwa nach Ausführung eines Auftrags durch ein sprachbasiertes Gerät.[1107] Schließlich sind zumutbare Anstrengungen zu unternehmen, Geräte mit *do not collect switches* auszustatten, welche eine Datenerhebung einfach und sicher unterbrechen,[1108] wie dies etwa Amazons Echo ermöglicht.[1109]

b) Datenerhebung durch Dritte

Im Bereich der Geräte-Identifier wurde bereits diskutiert, dass Abs. 25 Abs. 2 DS-GVO nur dann Genüge getan wird, wenn die Voreinstellungen ein nicht rechtskonformes Tracking standardmäßig verhindern.[1110] Insbesondere *third-party tracking* ist jedoch häufig gegenwärtig rechtswidrig[1111] und darf daher nicht in den Voreinstellungen zugelassen werden. Dies sollte die Kontroverse um Art. 9 Abs. 2, Art. 10 ePrivacy-Verordnung entscheidend beeinflussen.

Die Möglichkeit, Tracking zu verhindern, muss sich darüber hinaus gemäß Art. 25 Abs. 1 DS-GVO in einem datenschutzfreundlichen Design niederschlagen. Davon ist die Realität jedoch noch weit entfernt. Notwendig sind insofern Wahlangebote zur Realisierung von Datenschutzpräferenzen. Demgegenüber bieten jedoch 80 % der populärsten Webseiten in der EU nicht einmal die

---

[1106] *Bolognini/Ziegler*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 93 (96); *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 25.

[1107] Vgl. *Federal Trade Commission*, Internet of Things. Privacy & Security in a Connected World, 2015, 35; *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 25; *Rosner/Kenneally*, Clearly Opaque. Privacy Risks of the Internet of Things, Bericht, 2018, 100.

[1108] *Artikel-29-Datenschutzgruppe*, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, 2014, 26; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 66; *Gray*, Always On: Privacy Implications of Microphone-Enabled Devices, Future of Privacy Forum, 2016, 9; *Becker*, JZ 2017, 171 (178).

[1109] *Gray*, Always On: Privacy Implications of Microphone-Enabled Devices, Future of Privacy Forum, 2016, 9; siehe auch den *privacy mode* für IoT-Geräte, entwickelt bei *Zibuschka/Horsch/Kubach*, Open Identity Summit 2019, 119 (126).

[1110] Siehe oben, § 4 B.I.4.c.bb).

[1111] Siehe oben, § 4 B.I.6., § 5 D.II.3. und § 5 E.I.5.

Möglichkeit des Cookie Opt-Outs (Stand: 2018/19).[1112] Die Möglichkeit der Durchsetzung von Datenschutzpräferenzen, die gegen die Setzung von (nicht-essenziellen) Cookies gerichtet sind, hängt eng mit der technischen Ausgestaltung der Cookie Library bzw. dem Code zur Setzung der Cookies zusammen.[1113] So ist ein Opt-Out für *third-party tracking* technisch teilweise schwer umzusetzen, wenn der Cookie bereits platziert wurde,[1114] aber es ist technisch ohne Weiteres möglich, Präferenzen abzufragen, bevor der Cookie platziert wird.[1115] Daher muss durch den Erstanbieter ein Code ausgewählt werden, der die Setzung von Cookies (und die Verwendung anderer Geräte-Identifier) blockiert, bis die Zustimmung durch die betroffene Person erteilt wird. Dies ist nach der Entscheidung des EuGH in Sachen *Planet49* ohnehin unionsrechtlich zwingend.[1116] Lediglich die nachträgliche Entfernung von Drittanbietercookies kann sich technisch schwierig gestalten, da es hier zum Teil an einer Zugriffsmöglichkeit des Erstanbieters fehlt.[1117] Auch hier müssen daher durch die Industrie letztlich die technischen Voraussetzungen (durch APIs[1118]) geschaffen werden, um den Widerruf einer Einwilligung wirksam zu implementieren. Auch dies ist technisch ohne Weiteres möglich und wird zum Teil, etwa bei Google Analytics, bereits praktiziert.[1119]

Dass ganz grundsätzlich eine Wahlmöglichkeit hinsichtlich der Akzeptanz oder Zurückweisung von Cookies, auch unter Auswahl spezifischer Cookie-Typen, technisch möglich ist, zeigt der Umstand, dass 8,5 % der populärsten

---

[1112] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (1).

[1113] *Degeling et al.*, 26th Annual Network and Distributed System Security Symposium (NDSS '19), 1 (11).

[1114] *Degeling et al.*, 26th Annual Network and Distributed System Security Symposium (NDSS '19), 1 (11).

[1115] *Degeling et al.*, 26th Annual Network and Distributed System Security Symposium (NDSS '19), 1 (1, 11).

[1116] Siehe oben, § 4 B.I.4.a)bb)(1)(b).

[1117] *Degeling et al.*, 26th Annual Network and Distributed System Security Symposium (NDSS '19), 1 (11); der Nutzer kann einige Cookies selbst entfernen (siehe etwa https://support.mozilla.org/en-US/kb/clear-cookies-and-site-data-firefox?redirectlocale=en-US&redirectslug=delete-cookies-remove-info-websites-stored), muss dazu aber neben dem Widerruf der Einwilligung selbst tätig werden; zudem ist die manuelle Entfernung zumeist nicht ausreichend, siehe nur *Soltani et al.*, 2010 AAAI Spring Symposium Series, 158; *Ayenson et al.*, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning, Working Paper, 2011, https://ssrn.com/abstract=1898390; sowie die Nachweise zu *fingerprinting* oben, § 3, Fn. 186.

[1118] API steht für Application Programming Interface und beschreibt eine Schnittstelle, über die Dritte auf eine Softwareanwendung zugreifen können. Im hiesigen Kontext geht es darum, dass der Erstanbieter über eine API die Löschung des Cookies durch den Drittanbieter auslöst, siehe *Degeling et al.*, 26th Annual Network and Distributed System Security Symposium (NDSS '19), 1 (11).

[1119] *Degeling et al.*, 26th Annual Network and Distributed System Security Symposium (NDSS '19), 1 (11).

Webseiten der EU im Jahr 2019 eine solche Auswahl für die Nutzer anboten.[1120] So offeriert etwa die *Washington Post* ein Jahresabonnement, das $ 90 statt $ 60 kostet, bei dem im Gegenzug jedoch auf *third-party tracking* gänzlich verzichtet wird.[1121] Auch *Der Standard* bietet eine Wahl zwischen einem monetären Abo ohne Tracking und einer Variante über eine Einwilligung in die Datenverarbeitung an,[1122] ebenso mittlerweile *Spiegel Online*.[1123]

c) Datenerhebung bei Dritten

Um das Problem der Datenerhebung bei Dritten abzumildern, wird man im Rahmen von Abs. 25 Abs. 1 DS GVO schließlich verlangen müssen, dass die Verantwortlichen im Rahmen des Zumutbaren der Analyse von Daten einen Vorababgleich vorschalten, sodass Daten zum Beispiel nur erhoben werden von der Person, der die Stimme des Eigentümers zugeordnet werden kann. Allerdings gilt dies nur insoweit, als diejenigen, welche die entsprechende Software designen, auch Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO und nicht lediglich Hersteller sind. Hier bricht sich die oben genannte Unterscheidung besonders kritisch Bahn.[1124] In Betracht kommt bei einer Disjunktion von Hersteller und Verantwortlichem dann allerdings, wie erwähnt, eine (durch andere, in Art. 25 Abs. 1 DS-GVO genannte Aspekte moderierte) Auswahlverpflichtung des Verantwortlichen hinsichtlich eines Herstellers, der derartige Funktionalitäten bereithält.

IV. Co-Regulierung

Neben dem klassischen Pflichtenregime der Art. 5–22 DS-GVO hält die Verordnung, anders als noch die DSRL, auch eine Reihe von Mechanismen bereit, die von einem Zusammenspiel aus der Eigeninitiative der Verantwortlichen und den Aufsichtsbehörden leben (1.). Hierunter fallen einerseits die, allerdings verpflichtend ausgestaltete, Datenschutz-Folgenabschätzung nach Art. 35 f. DS-GVO[1125] (2.) und andererseits die Verhaltensregeln und Zertifizierungen nach Art. 40 ff. DS-GVO (3.). Die Terminologie für die Einstufung dieser Mechanismen ist in der Literatur nicht einheitlich. Bisweilen wird von

[1120] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (6): 434 von 5087 Webseiten; siehe auch die Auswertung einer Stichprobe, ebd., 4.

[1121] https://www.washingtonpost.com/gdpr-consent/.

[1122] https://apps.derstandard.at/privacywall/story/2000093545236/cookies-oder-zahlen-ein-fuer-und-wider-zur-datenschutz-entscheidung.

[1123] Spiegel Online, Werbung oder nicht? Sie haben die Wahl, 10.2.2020, https://www.spiegel.de/backstage/spiegel-de-ohne-werbung-oder-nicht-sie-haben-die-wahl-a-81628063-a527-4c84-aa00-5ded37933bb4.

[1124] *Bygrave*, 4 Oslo Law Review 2017, 105 (bei Fn. 48).

[1125] Vgl. *Binns*, 7 International Data Privacy Law 2017, 22 (30), der Art. 35 f. DS-GVO als Form der „Meta-Regulierung" einordnet.

Selbstregulierung gesprochen,[1126] eher trifft es jedoch die Formulierung der regulierten Selbstregulierung[1127] oder, jedenfalls in der internationalen Literatur noch gebräuchlicher, der Co-Regulierung.[1128] Denn sowohl bei der Datenschutz-Folgenabschätzung (Art. 36 DS-GVO) als auch bei der Genehmigung der Verhaltensregeln (Art. 40 Abs. 5 und Abs. 9 DS-GVO) und der Erteilung der Zertifizierung (Art. 42 Abs. 5 DS-GVO) handeln staatliche Stellen durch Wahrnehmung hoheitlicher Aufgaben, allerdings erst nach der (zum Teil) freiwilligen Initiative der Unternehmen oder Verbände. Sie ziehen sich mithin, wie es für die Co-Regulierung typisch ist,[1129] auf eine Gewährleistungsverantwortung zurück, wenngleich lediglich bezogen auf die von der Co-Regulierung erfassten Bereiche.

1. Allgemeine Funktionen und Relevanz der Co-Regulierung

Co-Regulierung soll mehrere wichtige Funktionen erfüllen. Erstens ermöglicht Co-Regulierung eine Flexibilisierung rechtlicher Anforderungen im technisch komplexen Umfeld.[1130] Zweitens wird, was bei komplexen technischen Vorgängen besonders wichtig erscheint, die Kompetenz der betroffenen Industrieakteure aktiv als Ressource genutzt.[1131] Drittens kann sie idealerweise zu

[1126] *Spindler*, ZD 2016, 407.

[1127] *Martini*, NVwZ-Extra 6/2016, 1 (7); dies deutet auch *Spindler*, ZD 2016, 407 (407) an; zur Abgrenzung von regulierter Selbstregulierun und Co-Regulierung *Marsden*, Internet Co-Regulation, 2011, 59.

[1128] Bei der Co-Regulierung kommt es zu einer Verbindung von Eigeninitiativen der regulierten Akteure und Spezifizierungs-, Überwachungs- und/oder Durchsetzungsaufgaben staatlicher Akteure, siehe *Bartle/Vass*, Self-regulation and the regulatory state: A survey of policy and practice, Centre for the Study of Regulated Industries, University of Bath School of Management, Research Report 17, 2005, 33; *Senden*, 9(1) Electronic Journal of Comparative Law 2005, 1 (11 ff.); *Hans-Bredow-Institut*, Study on Co-Regulation Measures in the Media Sector, Study for the European Commission, Directorate Information Society and Media, 2006, 35; *Coglianese/Mendelson*, in: Baldwin et al. (Hrsg.), The Oxford Handbook of Regulation, 2010, 146 (147) (unter der Bezeichnung „meta-regulation"); *Marsden*, Internet Co-Regulation, 2011, 54, 61; *Australian Communications and Media Authority*, Optimal conditions for effective self- and co-regulatory arrangements, Occasional Paper, 2015, 8; zu Co-Regulierung im Bereich der neuen Technologien *Tropina*, in: *Tropina/Callanan* (Hrsg.), Self- and Co-regulation in Cybercrime, Cybersecurity and National Security, 2015, 1 (16 ff.); *Marsden*, Internet Co-Regulation, 2011, 130 ff.

[1129] *Eifert*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts – Band I, 2. Auf. 2012, 1319 Rn. 52.

[1130] Vgl. *Coglianese/Lazer*, in: Donahue/Nye (Hrsg.), Market-Based Governance, Washington, DC 2002, 201 (202); *Hepburn*, Alternatives to Traditional Regulation, *OECD* Report, 2006, 6; *Eifert*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts – Band I, 2. Auf. 2012, 1319 Rn. 59; *Australian Communications and Media Authority*, Optimal conditions for effective self- and co-regulatory arrangements, Occasional Paper, 2015, 10.

[1131] *Coglianese/Lazer*, in: Donahue/Nye (Hrsg.), Market-Based Governance, Washington, DC 2002, 201 (202); *Bartle/Vass*, Self-regulation and the regulatory state: A survey of policy and practice, Centre for the Study of Regulated Industries, University of Bath School of Management, Research Report 17, 2005, 48; *Coglianese/Mendelson*, in: Baldwin et al.

einer Internalisierung der rechtlichen Wertungen durch die Regulierten führen.[1132] Viertens ermöglicht sie, im Gegensatz zur reinen Selbstregulierung, ein im Einzelfall zu justierendes Maß an Aufsichts- und Durchsetzungskompetenzen durch (zumindest theoretisch) allein dem öffentlichen Wohl verpflichtete staatliche Akteure.[1133] Zugleich ist unübersehbar, dass der Erfolg von Co-Regulierung, ebenso wie jener der Selbstregulierung, von dem Wohlwollen und der aktiven, auf die Erfüllung der Ziele der DS-GVO ausgerichteten Partizipation der Unternehmen und Verbände angewiesen ist.[1134] Inwiefern diese notwendige Bedingung erfüllt wird, kann allein die künftige Entwicklung des Regimes der Co-Regulierung erweisen.

2. *Datenschutz-Folgenabschätzung, Art. 35 DS-GVO*

Einen ersten Pfeiler der Co-Regulierung im Kontext der DS-GVO stellt die Datenschutz-Folgenabschätzung nach Art. 35 f. DS-GVO dar. Sie ist ein neues Instrument der DS-GVO, das in der DSRL so noch nicht enthalten war.[1135]

a) Relevanz

Gemeinsam mit Art. 25 Abs. 1 und Art. 32–34[1136] DS-GVO ist die Datenschutz-Folgenabschätzung zentral für den risikobasierten Ansatz der Verordnung:[1137] Unterschiedlich hohe Risiken lösen hier ganz dezidiert unterschiedlich weitreichende Verpflichtungen der Verantwortlichen aus.[1138] Dies wird übergreifend und explizit bereits in Art. 24 Abs. 1 DS-GVO festgehalten. Danach muss der

(Hrsg.), The Oxford Handbook of Regulation, 2010, 146 (164); *Eifert*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts – Band I, 2. Auf. 2012, 1319 Rn. 59.

[1132] *Coglianese/Lazer*, in: Donahue/Nye (Hrsg.), Market-Based Governance, Washington, DC 2002, 201 (202); *Coglianese/Mendelson*, in: Baldwin et al. (Hrsg.), The Oxford Handbook of Regulation, 2010, 146 (164); *Eifert*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts – Band I, 2. Auf. 2012, 1319 Rn. 59.

[1133] Vgl. *Binns*, 7 International Data Privacy Law 2017, 22 (34); *Coglianese/Mendelson*, in: Baldwin et al. (Hrsg.), The Oxford Handbook of Regulation, 2010, 146 (161 f.); *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 42 DS-GVO Rn. 12.

[1134] Vgl. *Bennear*, in: Coglianese/Nash (Hrsg.), Leveraging the Private Sector: Management-Based Strategies for Improving Environmental Performance, 2006, 51 (80).

[1135] Siehe zu *prior checking* nach Art. 20 DSRL und den Bezügen zu Datenschutz-Folgenabschätzungen *Le Grand/Barrau*, in: Wright/De Hert (Hrsg.), Privacy Impact Assessment, 2012, 97.

[1136] Die darin behandelte IT-Sicherheit ist zwar auch für den Bereich der digitalen Wirtschaft enorm wichtig, gerade bei vernetzten Geräten. Diese Fragestellungen können jedoch vorliegend, da sie insbesondere das hier nicht thematische Hacking betreffen, nicht behandelt werden.

[1137] Vgl. zu Risikomanagement und Datenschutz-Folgenabschätzungen bereits früh *Wright/De Hert*, in: Wright/De Hert (Hrsg.), Privacy Impact Assessment, 2012, 3 (10 ff.).

[1138] *Lynskey*, The Foundations of EU Data Protection Law, 2015, 85; *Quelle*, in: Leenes et al. (Hrsg.), Data Protection and Privacy: The Age of Intelligent Machines, 33 (37 f.).

Verantwortliche unter Berücksichtigung von Eintrittswahrscheinlichkeit und Schwere der datenschutzrechtlichen, aber auch anderer Risiken[1139] geeignete technische und organisatorische Maßnahmen einsetzen, um die Verarbeitung gemäß den Anforderungen der DS-GVO zu gewährleisten und nachzuweisen. Dies mindert zwar nicht die Pflichtenstellung aus den Art. 5–22 DS-GVO,[1140] knüpft aber das Niveau der vorsorgenden technischen und organisatorischen Umsetzung dieser Pflichten an das datenschutzrechtliche Risiko.[1141]

Im Rahmen der Datenschutz-Folgenabschätzung wird der Verantwortliche selbst in die Pflicht genommen, bereits im Vorfeld der Verarbeitung die möglichen Risiken und potenzielle Gegenmaßnahmen zu eruieren.[1142] Dem Verantwortlichen wird damit zugemutet, die eigenen Praktiken zu evaluieren und, wo möglich, kritisch zu hinterfragen. Er wird damit jedoch nicht zum Richter in eigener Sache, da eine behördliche und gerichtliche Überprüfung der Verarbeitung auch nach einer Datenschutz-Folgenabschätzung (natürlich) möglich bleibt. Art. 35 DS-GVO ist jedoch, neben Art. 25 und Art. 32 DS-GVO, eines der Instrumente, welches den datenschutzrechtlichen Fokus von einer ex post-Perspektive der Sanktionierung unrechtmäßigen Verhaltens hin zu einer ex ante-Perspektive der Verhinderung datenschutzrechtswidriger Praktiken verschiebt.[1143] Angesichts begrenzter behördlicher und gerichtlicher Ressourcen sowie der aufgezeigten Schwächen des individuellen Kontrollregimes erscheint diese Vorverlagerung der Steuerungswirkung[1144] jedenfalls grundsätzlich als eine überaus sinnvolle Ergänzung des bisherigen Pflichtenkatalogs.

Ob die Datenschutz-Folgenabschätzung in der Praxis zu einer verstärkten Berücksichtigung datenschutzrechtlicher Fragen bei der unternehmerischen

---

[1139] Siehe *Article 29 Data Protection Working Party*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 2017, 6: „the reference to ‚the rights and freedoms' of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion".

[1140] Vgl. *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 24 DS-GVO Rn. 11; *Article 29 Data Protection Working Party*, Statement on the role of a risk-based approach in data protection legal frameworks, WP 218, 3 Rn. 2; siehe aber, für Argumente für eine Rückwirkung von Art. 24 Abs. 1 DS-GVO auf Art. 5–22 DS-GVO, *Quelle*, in: Leenes et al. (Hrsg.), Data Protection and Privacy: The Age of Intelligent Machines, 33 (42 ff.); siehe auch *Gellert*, 5 International Data Privacy Law 2015, 3 (16).

[1141] *Petri*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 24 DS-GVO Rn. 3.

[1142] *Wright/De Hert*, in: Wright/De Hert (Hrsg.), Privacy Impact Assessment, 2012, 3 (5 f.).

[1143] *Hacker*, 55 Common Market Law Review 2018, 1143 (1171); vgl. auch *Article 29 Data Protection Working Party*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 2017, 4, 14.

[1144] Dazu *Eifert*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts – Band I, 2. Auf. 2012, 1319 Rn. 54.

Datenverarbeitung führen wird, ist allerdings noch nicht abzusehen. Jedenfalls plausibel erscheint, dass wenigstens das Bewusstsein für datenschutzrechtliche Risiken dadurch gestärkt wird. Ein Unterlassen der gebotenen Datenschutz-Folgenabschätzung, ein Fehler oder eine Nichtkonsultation der Aufsichtsbehörde entgegen Art. 36 Abs. 1 DS-GVO kann gemäß Art. 83 Abs. 4 lit. a DS-GVO mit einer Geldbuße von bis zu 2 % des Jahresumsatzes geahndet werden.[1145]

b) Norminhalt

Die Pflicht der Durchführung einer Datenschutz-Folgenabschätzung ist nach Art. 35 Abs. 1 S. 1 DS-GVO daran geknüpft, dass „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen" besteht. In Abs. 3 sind drei Beispiele enthalten, bei denen der Verordnungsgeber von dem Bestehen eines hinreichenden Risikos ausgeht: systematische Profilbildung mit automatisierter Entscheidung (Abs. 3 lit. a DS-GVO); umfangreiche Verarbeitung sensitiver Daten (Abs. 3 lit. b DS-GVO); und die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (Abs. 3 lit. c DS-GVO). Um darüber hinaus abzuschätzen, ob ein hinreichendes Risiko vorliegt, hat die Artikel-29-Datenschutzgruppe eine Liste aus neun Kriterien veröffentlicht, die in einer Gesamtschau zur Anwendung gebracht werden müssen.[1146] Sind mindestens zwei davon erfüllt, so muss nach Ansicht der Datenschutzgruppe typischerweise eine Datenschutz-Folgenabschätzung vorgenommen werden.[1147]

Diese Abschätzung weist eine enge Verbindung zu der Abwägung nach Art. 25 Abs. 1 DS-GVO auf.[1148] Dabei muss der Verantwortliche gemäß Abs. 35 Abs. 7 DS-GVO eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und Zwecke anfertigen, die Notwendigkeit und Verhältnismäßigkeit der Verarbeitungen hinsichtlich des Zwecks überprüfen, die datenschutzrechtlichen Risiken ermitteln und mögliche Abhilfemaßnahmen diskutieren.[1149] Letztlich müssen hier die für und wider die Rechtmäßigkeit der Verarbeitung sprechenden Gesichtspunkte durch den Verantwortlichen erfasst und risikospezifisch in die Abwägung eingestellt werden. Gerade bei kleine-

[1145] *Article 29 Data Protection Working Party*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 2017, 4.

[1146] *Article 29 Data Protection Working Party*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 2017, 9–11; dazu unten sogleich genauer bei der Anwendung auf die drei Leitfälle.

[1147] *Article 29 Data Protection Working Party*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 2017, 11.

[1148] *Bygrave*, 4 Oslo Law Review 2017, 105; *Baumgartner/Gausling*, ZD 2017, 308 (309).

[1149] Abhilfemaßnahmen müssen nicht notwendig implementiert werden, siehe *Quelle*, in: Leenes et al. (Hrsg.), Data Protection and Privacy: The Age of Intelligent Machines, 33 (50).

ren Verarbeitern darf jedoch die institutionelle Kompetenz für eine derartige, häufig komplexe, juristisch fokussierte Abwägung bezweifelt werden. Insofern werden Sanktionen für Fehler bei der Einschätzung nur bei evident sachwidrigen Erwägungen verhängt werden können.

Ermittelt der Verantwortliche im Rahmen der Abschätzung ein hohes Risiko, ergreift jedoch keine Maßnahmen zu dessen Eindämmung, so muss er nach Art. 36 Abs. 1 DS-GVO die Aufsichtsbehörde konsultieren. Diese kann sodann Vorschläge unterbreiten und im Rahmen ihrer allgemeinen Befugnisse Maßnahmen ergreifen (Art. 36 Abs. 2 DS-GVO).

c) Anwendung auf die drei Leitfälle

Mit Blick auf die drei hier verhandelten Leitfälle ist insbesondere zu fragen, ob typischerweise ein hinreichendes datenschutzrechtliches Risiko erreicht wird, um die Notwendigkeit einer Datenschutz-Folgenabschätzung auszulösen. Dies dürfte regelmäßig zu bejahen sein. Damit steigt immerhin inkrementell die Wahrscheinlichkeit, dass datenschutzrechtskonforme Praktiken bereits bei der Entwicklung der jeweiligen Anwendung ausgearbeitet werden.

aa) Datenweiterleitung an Dritte

Die Weiterleitung von Daten an Dritte erhöht das Risiko einer Exposition, eines Hacks, aber auch, infolge der Zusammenführung von Daten, der Bildung von Profilen, die wiederum *chilling*-Effekte und Diskriminierung zur Folge haben können. Dies gilt auch für die Datenweiterleitung zum Zwecke personalisierter Werbung, da typischerweise gerade nicht garantiert werden kann, dass die übermittelten Daten wirklich nur zu Zwecken der Werbeexposition verwendet werden. Werbenetzwerke sammeln und aggregieren erhebliche Mengen von Daten, sodass nicht ausgeschlossen ist, dass diese dereinst auch für andere Zwecke (z. B. Kreditvergabe, Versicherung) genutzt werden. Damit sind zumindest drei der von der Artikel-29-Datenschutzgruppe hervorgehobenen Risikofaktoren regelmäßig verwirklicht: Verwendung von Daten über Präferenzen, Interessen oder Lokalisierung (Faktor 1); systematische Beobachtung (Faktor 3); und innovative Nutzung oder Anwendung neuer technischer Lösungen (Faktor 8). Zudem muss berücksichtigt werden, dass gerade die Werbenetzwerke häufig Daten in großem Umfang verarbeiten (Faktor 5) und Daten aus verschiedenen Quellen zusammenführen (Faktor 6). Werden sensitive oder hochpersönliche Daten genutzt, ist ein weiteres Kriterium (Faktor 4) erfüllt und eine Datenschutz-Folgenabschätzung zweifellos durchzuführen. Diese Erwägungen gelten für die Datenweiterleitung im Rahmen des Internets der Dinge, da auch hier dieselben Faktoren einschlägig sind.[1150]

[1150] Vgl. *Rosner/Kenneally*, Clearly Opaque. Privacy Risks of the Internet of Things, Bericht, 2018, 103; *Bolognini/Ziegler*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 93 (96 f.).

bb) Datenerhebung durch Dritte

Im Wesentlichen identische Erwägungen sprechen dafür, dass Verantwortliche beim *third-party tracking* ebenfalls regelmäßig eine Datenschutz-Folgenabschätzung durchführen müssen. Hierbei ist zu beachten, dass die Verantwortung für die initiale Erhebung der Daten typischerweise zwischen dem Anbieter des Tracking-Instruments und dem Anbieter des konkret genutzten Produkts gemäß Abs. 26 DS-GVO geteilt ist,[1151] diese sich also hinsichtlich einer Datenschutz-Folgenabschätzung und möglicher Abhilfemaßnahmen untereinander verständigen müssen.[1152]

cc) Datenerhebung bei Dritten

Die Möglichkeit einer beabsichtigten oder unbeabsichtigten Datenerhebung bei Dritten geht mit zusätzlichen Risiken einher, da für diese Dritten häufig keine wirksamen Möglichkeiten individueller Kontrolle der Datenerhebung bestehen. Daher dürfte auch in diesen Fällen grundsätzlich eine Datenschutz-Folgenabschätzung notwendig sein.[1153]

3. Verhaltensregeln und Zertifizierungsverfahren

Die Verhaltensregeln und Zertifizierungsverfahren der DS-GVO tragen gegenüber der Datenschutz-Folgenabschätzung noch stärker selbstregulatorische Züge, da keine rechtliche Verpflichtung zu ihrer Durchführung besteht. Anreize werden vielmehr indirekt durch Art. 24 Abs. 3 DS-GVO geschaffen, wonach die Einhaltung von genehmigten Verhaltensregeln oder Zertifizierungsverfahren als ein Gesichtspunkt herangezogen werden kann, um den in Art. 24 Abs. 1 S. 2 DS-GVO geforderten Nachweis hinsichtlich der Erfüllung der Pflichten des Verantwortlichen zu erbringen. Zudem wird die Einhaltung von genehmigten Verhaltensregeln oder Zertifizierungsverfahren im Rahmen der Bemessung der Geldbuße nach Art. 83 Abs. 2 lit. j DS-GVO berücksichtigt. Dieser Fall kann etwa eintreten, wenn eine andere als die genehmigende Aufsichtsbehörde einen Rechtsverstoß feststellt, obgleich das Verhalten einer genehmigten Verhaltensregel entspricht.[1154]

[1151] Dazu oben, §§ 5 C.I.2.c).

[1152] *Article 29 Data Protection Working Party*, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, 2017, 7 f.

[1153] Siehe für ein konkretes Beispiel im Rahmen einer *Smart City Ziegler/Menon/Annichino*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 149 (159 ff.).

[1154] Vgl. *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 40 DS-GVO Rn. 48.

a) Genehmigte Verhaltensregel, Art. 40 f. DS-GVO

Die potenziell weiter reichenden Rechtswirkungen zeitigt die genehmigte Verhaltensregel nach Art. 40 f. DS-GVO.[1155] Ausgearbeitet werden derartige Verhaltensregeln nach Art. 40 Abs. 2 DS-GVO durch Verbände oder anderweitige Vertretungsorganisationen von Verantwortlichen. Ein Beispiel stellen die genehmigten Verhaltensregeln der Wirtschaftsauskunfteien hinsichtlich Löschfristen dar.[1156] Thematisch können die Regeln auf eine Reihe von Punkten bezogen sein, die in Art. 40 Abs. 2 DS-GVO enthalten sind und etwa die Grundsätze der Fairness und Transparenz der Datenverarbeitung, die berechtigten Interessen der Verantwortlichen in bestimmten Zusammenhängen oder auch Maßnahmen zu Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen umfassen.

Die Verhaltensregeln werden sodann der zuständigen Aufsichtsbehörde vorgelegt und von dieser, sofern sie mit den Vorgaben der DS-GVO in Einklang stehen, nach Art. 40 Abs. 5 DS-GVO genehmigt. Damit ist jedenfalls diese Aufsichtsbehörde nach dem Grundsatz der Selbstbindung der Verwaltung an die in den Verhaltensregeln niedergelegte Einschätzungen gebunden.[1157]

Sofern sich die Verhaltensregeln auf Verarbeitungstätigkeiten in mehreren Mitgliedstaaten beziehen, nimmt zudem der nach Abs. 68 DS-GVO eingerichtete Europäische Datenschutzausschuss dazu Stellung, Art. 40 Abs. 7 DS-GVO. Bestätigt die Stellungnahme die DS-GVO-Konformität, so werden die Verhaltensregeln schließlich noch der Kommission vorgelegt. Diese kann wiederum gem. Art. 40 Abs. 9 DS-GVO – und hierin besteht die besondere Relevanz des Verfahrens – im Wege von Durchführungsrechtsakten nach Art. 291 Abs. 2 AEUV[1158] beschließen, dass die Verhaltensregeln EU-weite Gültigkeit besitzen und damit als Konkretisierung unbestimmter Rechtsbegriffe oder Vorgaben der DS-GVO präzisierend wirken. Dieser Kommissionsakt bindet nach wohl herrschender Meinung gemäß Abs. 288 Abs. 2 oder 4 AEUV (je nach Rechtsnatur[1159]) die Aufsichtsbehörden und Gerichte[1160] der Mitgliedstaaten dahingehend, dass diese Verhaltensweisen, welche den genehmigten

[1155] Dazu ausführlich *Bergt*, CR 2016, 670.

[1156] Siehe https://www.schufa.de/de/ueber-uns/daten-scoring/verhaltensregeln-loeschfristen/verhaltensregeln-loeschfristen.jsp; dazu *Reifert*, ZD 2019, 305 (306 ff.).

[1157] *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 40 DS-GVO Rn. 41; *Bergt*, CR 2016, 670 (676); *Reifert*, ZD 2019, 305 (307).

[1158] Es findet gem. Art. 40 Abs. 9 S. 2 DS-GVO das Prüfverfahren nach Art. 93 Abs. 2 DS-GVO, Art. 5 der Verordnung (EU) Nr. 182/2011 Anwendung; dazu *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 291 Rn. 15; *Reifert*, ZD 2019, 305 (309).

[1159] *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 291 Rn. 11.

[1160] Zwar entfaltet die Selbstbindung der Verwaltung keine Bindungswirkung für Gerichte; dies ist jedoch anders bei manchen Durchführungsrechtsakten, zu denen Verwaltungsbehörden explizit ermächtigt wurden, so etwa die Kommission bei Akten gem. Art. 291 Abs. 2 AEUV, siehe vgl. *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 291 Rn. 38; *Reifert*, ZD 2019, 305 (309); aA *Spindler*, ZD 2016, 407 (411) (keine Bindung der Gerichte).

Verhaltensregeln entsprechen, als im Einklang mit der DS-GVO befindlich bewerten müssen.[1161] Umstritten ist ferner allerdings, ob aus der Gültigkeitserklärung folgt, dass die insofern genehmigten Verhaltensweisen verbindlich wären und positiv befolgt werden müssten.[1162] Dies wird in jenen (wohl seltenen) Fällen relevant, in denen die genehmigten Verhaltensweisen über das von der DS-GVO eigentlich geforderte Verhalten (infolge eines Rechtsirrtums der Verfahrensbeteiligten) hinausgehen. Zwar kommt Durchführungsverordnungen und Durchführungsbeschlüssen nach Art. 288 Abs. 2 und 4 AEUV grundsätzlich Verbindlichkeit zu;[1163] die Unzulässigkeit der Abänderung des Basisrechtsakts folgt allerdings aus Art. 290 AEUV ex negativo.[1164] Ferner spricht Art. 40 Abs. 9 S. 1 DS-GVO nur von allgemeiner Gültigkeit, gerade nicht von Verbindlichkeit. Dass es sich dabei um ein Redaktionsversehen handelt, ist nicht anzunehmen; daher ist die Vorgabe der DS-GVO als Basisrechtsakt eindeutig gegen eine allgemeine Verbindlichkeit gerichtet.[1165]

Die genehmigten Verhaltensweisen erweisen sich damit als ein Modell der co-regulativen Normentwicklung, das zu einer Anpassung der allgemeinen Bestimmungen der DS-GVO auf bestimmte Verarbeitungssituationen führen und damit zu größerer Rechtssicherheit beitragen soll.[1166] Damit stellt es eine weitere, differenzierte Stufe des datenschutzrechtlichen Ordnungsrahmens dar. Aufgrund der inhaltlichen Offenheit der genehmigungsfähigen Verhaltensweisen lässt sich ihre Wirkung auf die Beantwortung der hier in Rede stehenden Leitfragen jedoch zum jetzigen Zeitpunkt noch nicht absehen. Sie haben einerseits das Potenzial, durch größere Komplexität die Benutzerfreundlichkeit zu verringern; andererseits können klare Vorgaben für spezifische Konstellationen für die Ausübung von Privatautonomie durchaus förderlich sein, wenn diesbezügliche Probleme, etwa Informationsasymmetrien, erkannt und wirkungsvoll ausgeräumt werden.

[1161] *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 40 DS-GVO Rn. 51 mwN; *Bergt*, CR 2016, 670 (676 f.); aA *Spindler*, ZD 2016, 407 (411) (Entscheidungsbefugnis der Kommission, ob Bindungswirkung oder nur Vermutungswirkung intendiert ist).

[1162] So *Martini*, NVwZ-Extra 6/2016, 1 (11); *Härting*, Datenschutz-Grundverordnung, 2016, Rz. 788; dagegen *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 40 DS-GVO Rn. 51; *Bergt*, CR 2016, 670 (676).

[1163] Art. 288 Abs. 5 AEUV ex negativo; siehe auch *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 288 Rn. 86 zum Beschluss.

[1164] *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 291 Rn. 11; *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 291 Rn. 58.

[1165] Ebenso *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 40 DS-GVO Rn. 51; *Bergt*, CR 2016, 670 (676).

[1166] *von Grafenstein*, in: González Fuster et al. (Hrsg.), Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics, 2020, (im Erscheinen).

b) Genehmigtes Zertifizierungsverfahren, Art. 42 f. DS-GVO

Das Ziel der Zertifizierungsverfahren nach Art. 42 f. DS-GVO besteht vor allem darin, Nutzern vor Augen führen, welche Verantwortlichen die Vorgaben der DS-GVO bei regelmäßigen Überprüfungen einhalten.[1167] Dadurch soll der Marktmechanismus für die Verbesserung des Datenschutzes genutzt werden.[1168] Die Zertifizierung wird gemäß Art. 42 Abs. 7 DS-GVO für höchstens drei Jahre erteilt. Sie berührt jedoch gemäß Abs. 42 Abs. 4 DS-GVO in keiner Weise die Verantwortlichkeit des Verantwortlichen (führt also insbesondere nicht zu einem Haftungsausschluss[1169]). Insofern dient sie für der DS-GVO unterworfene Unternehmen alleine der Reputationsbildung, auch wenn sie intern durchaus Compliance-Maßnahme wirken kann.[1170]

Die Zertifizierung kann insofern Übersichtlichkeit fördern und Nutzern Möglichkeiten zur Kontrolle bieten, als solche Verantwortliche schnell ausfindig gemacht werden können, bei denen die Wahrscheinlichkeit, dass die Verarbeitung datenschutzkonform geschieht, besonders hoch ist. Damit werden Suchkosten gesenkt und Reputationseffekte gestärkt. Die Effektivität dieser Auswirkungen hängt jedoch entscheidend davon ab, dass die Gütezeichen vereinheitlicht werden[1171] und die Zertifizierung korrekt durchgeführt wird.[1172] Zuständig hierfür sind nach nationalem Recht akkreditierte, unabhängige Zertifizierungsstellen, Art. 43 DS-GVO. Auch hier bleibt letztlich abzuwarten, inwiefern die Zertifizierung ihrer Hinweisfunktion gerecht werden und die Ausübung von Wahlfreiheit positiv beeinflussen kann. Das Regime der Co-Regulierung ist mithin insgesamt in der Theorie viel versprechend; in der Praxis jedoch steht seine Bewährungsprobe noch aus.

D. Ergebnisse von § 4

1. Die Analyse der datenschutzrechtlichen Vorschriften offenbart bereits zahlreiche Wechselwirkungen zwischen unionalem Datenschutzrecht und allgemeinem Privatrecht. Nicht nur hat die Widerruflichkeit der Einwilligung erhebliche Auswirkungen auf vertragsrechtliche Sekundäransprüche; an vier hier untersuchten Stellen ragen umgekehrt auch privatrechtliche Wertungen unmittelbar in die DS-GVO hinein. Sie wirken sich aus bei der Konkretisierung

[1167] Siehe den 100. Erwägungsgrund der DS-GVO; ferner *Scuderio/Ziegler*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 129 (130).

[1168] *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 42 DS-GVO Rn. 4.

[1169] *Spindler*, ZD 2016, 407 (412).

[1170] Zu letzterem *Bock*, in: Wright/De Hert (Hrsg.), Enforcing Privacy. Regulatory, Legal and Technological Approaches, 2016, 335 (354).

[1171] Kritisch zum Bestand daher *Jung*, ZD 2018, 208 (210 f.).

[1172] Detaillierte Vorschläge bei *Bock*, in: Wright/De Hert (Hrsg.), Enforcing Privacy. Regulatory, Legal and Technological Approaches, 2016, 335 (341 ff.).

des datenschutzrechtlichen Grundsatzes der Datenverarbeitung nach Treu und Glauben (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO); bei den allgemeinen Wirksamkeitsvoraussetzungen der Einwilligung (dazu im Einzelnen unten, § 5 B.II.); bei der Wirksamkeit des Vertrags als notwendige Voraussetzung der vertragserforderlichen Datenverarbeitung (Art. 6 Abs. 1 lit. b DS-GVO) sowie schließlich auch bei der Interessenabwägungsklausel (Fortwirkung privatautonomer Gestaltung, Art. 6 Abs. 1 lit. f DS-GVO).

2. Die Normen der DS-GVO prägen den rechtlichen Rahmen der digitalen Wirtschaft entscheidend. Sie können als Folge der doppelten Zuspitzung der hier verfolgten Fragestellung danach unterteilt werden, ob sie ihrem Schwerpunkt nach eher ermöglichenden oder regulatorischen Charakter haben. Unter erstere Kategorie fällt insbesondere der Erlaubnistatbestand von Art. 6 Abs. 1 lit. a DS-GVO im Verbund mit den Wirksamkeitsvoraussetzungen der Einwilligung in Art. 4 Nr. 11 DS-GVO sowie das Recht auf Datenübertragung nach Art. 20 DS-GVO. Der Erlaubnistatbestand in Art. 6 Abs. 1 lit. b DS-GVO hingegen ist primär rein permissiv ausgerichtet und fördert nur mittelbar, über die auch hier anwendbaren Informationspflichten der Art. 12 ff. DS-GVO, aktiv Privatautonomie und informierte Entscheidungen; der Ermöglichungscharakter ist insoweit vorhanden, aber reduziert.

3. Die Analyse der Ermöglichungsstrukturen offenbart jedoch erhebliche Defizite im rechtlichen wie auch tatsächlichen Bereich. Das Recht auf Datenübertragung lebt von der Existenz funktional äquivalenter Alternativen am Markt, die es selbst nicht garantieren kann und die unter den Rahmenbedingungen der in vielen Bereichen von Netzwerkeffekten geprägten digitalen Wirtschaft tendenziell unwahrscheinlich erscheinen.

4. Über die beiden Erlaubnistatbestände (Art. 6 Abs. 1 lit. a und b DS-GVO) hingegen können zwar, in der Theorie, die Verarbeitung personenbezogener Daten durch die Einwilligung unmittelbar und durch Vertragskonstruktionen, für welche die Daten erforderlich sind, mittelbar privatautonom gesteuert werden. Allerdings versagt dieses Regime weitgehend aufgrund einer doppelten Dysfunktionalität, die man als Dilemma individueller Kontrolle im Datenschutzrecht bezeichnen könnte.

5. Rationalen Parteien mit niedrigen Datenschutzpräferenzen ist es verwehrt, rechtssicher hinsichtlich ihrer Daten zu kontrahieren und diese etwa als Erweiterung ihrer Budgetrestriktionen einzusetzen. Dies liegt insbesondere an den aufgezeigten Interpretationsmöglichkeiten hinsichtlich des Kopplungsverbots nach Art. 7 Abs. 4 DS-GVO und des Erforderlichkeitsmaßstabs nach Art. 6 Abs. 1 lit. b DS-GVO. *De lege lata* müssen diese nach hier vertretener Auffassung vielmehr so ausgelegt werden, dass eine weit reichende Datenüberlassung als Gegenleistung nur dann möglich ist, wenn diese zur Erfüllung von wirksam vereinbarten Pflichten des Verantwortlichen erforderlich ist (subjektiver Erfor-

derlichkeitsmaßstab unter Ausblendung der Nutzerpflichten). Im Rahmen der gegenwärtig gepflogenen Geschäftsmodelle wird dies selten der Fall sein.

6. Besonders rationale Parteien mit niedrigen Datenschutzpräferenzen stellen jedoch nur eine Minderheit der Nutzergruppe dar. Hinsichtlich aller anderer scheitert das individuelle Kontrollregime an rationaler Ignoranz, verhaltensökonomischen Effekten und negativen Externalitäten. Hier fehlt es regelmäßig schon an den empirisch-ökonomischen Voraussetzungen für die wirksame Inanspruchnahme (quasi-)rechtsgeschäftlicher Gestaltungsmacht auf Seiten der Nutzer. Ferner lassen sich hohe Datenschutzpräferenzen gegenwärtig nur schwer am Markt durchsetzen.

7. Heterogenität der Regulierungsadressaten wird also nur unzureichend normativ erfasst. Angesichts dieser Defizite des individuellen Kontrollregimes rücken insbesondere die regulatorischen Strukturen des Datenschutzrechts in den Vordergrund. Hier sind vor allem die Interessenabwägungsklausel von Art. 6 Abs. 1 lit. f DS-GVO, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen nach Art. 25 DS-GVO sowie co-regulative Mechanismen wie Datenschutz-Folgenabschätzungen nach Art. 35 f. DS-GVO oder Verhaltensregeln und Zertifizierungen nach Art. 40 ff. DS-GVO zu nennen.

8. Die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO ist gekennzeichnet durch ein hohes Maß von Flexibilität, das zugleich durch genehmigte Verhaltensregeln, Fallgruppenbildung und Leitlinien des Europäischen Datenschutzausschusses für bestimmte Verarbeitungssituationen präzisiert werden kann und muss. Eine gewisse Rechtsunsicherheit ist durch die Einwirkung des Datenschutzgrundrechts auf Kontexte des Marktaustauschs vorgezeichnet und letztlich im Interesse sachgerechter Entscheidungen hinzunehmen. Das Risiko von Fehleinschätzungen der Verantwortlichen muss dann jedoch bei *hard cases*, sofern ernsthafte Abwägungsprozesse nachgewiesen werden können, sanktionsmildernd berücksichtigt werden.

9. Art. 6 Abs. 1 lit. f DS-GVO kommt eine gesteigerte ökonomische und rechtliche Relevanz in zweifacher Hinsicht zu. Erstens suggerieren die verschärften Anforderungen an die Einwilligung und die hier vertretene Auslegung der vertragserforderlichen Datenverarbeitung, dass diese Erlaubnistatbestände in vielen der hier betrachteten Fälle digitaler Austauschprozesse letztlich nicht greifen werden. Damit rückt die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO ins Zentrum des rechtlichen Interesses. Zweitens lässt sich darüber in ökonomischer Hinsicht *de facto* eine Regulierung von Datenpreisen ausüben, die in dem Maße sachlich zwingend wird, in dem die in § 4 aufgezeigten Fälle von Marktversagen nicht anderweitig korrigiert werden.

10. Eine zentrale Vorschrift, um den Defiziten des individuellen Kontrollregimes entgegenzutreten, stellt der Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß Abs. 25 DS-GVO dar. Zwar

können keinesfalls alle Anforderungen der DS-GVO auf technischem Wege automatisch erfüllt werden. Doch leistet die Norm, trotz all ihrer Beschränkungen, einen zentralen Beitrag dazu, Rechtsverstöße im datenschutzrechtlichen Bereich nicht mehr nur ex post zu sanktionieren, sondern ex ante zu verhindern. Diese Stoßrichtung weist auch die Datenschutz-Folgenabschätzung auf. Zugleich wirkt sie negativen Externalitäten entgegen. Diverse technische Anwendungen für die Umsetzung dieser Regeln stehen bereit. Wenn sie konsequent genutzt werden, kann *data protection by design and default* an die Seite, und bisweilen an die Stelle, des individuellen Kontrollregimes treten. Wirkliche Wahlfreiheit wird dadurch jedoch nur gewährleistet, wenn zugleich praktikable Methoden der Auswahl der technischen Spezifizierungen und Voreinstellungen angeboten werden. Dies zeigt einmal mehr, dass weitere rechtliche Mechanismen notwendig sind, um die Voraussetzungen für eine wirksame Inanspruchnahme von Privatautonomie im digital geprägten Umfeld zu schaffen (siehe § 6).

11. Hinsichtlich der drei Leitfälle lässt sich übergreifend feststellen, dass auf Grundlage der bisher vorherrschenden Geschäftsmodelle Datenweiterleitung zu Zwecken personalisierter Werbung oder zu nicht funktional erforderlicher Verarbeitung im Internet der Dinge (Leitfall 1), *third-party tracking* (Leitfall 2) sowie Datenerhebung bei Dritten in stark vernetzten Umgebungen (Leitfall 3) kaum in datenschutzkonformer Weise durchgeführt werden kann. Dies liegt insbesondere an den strengen Anforderungen an die Unmissverständlichkeit und die Informiertheit der Einwilligung sowie an der hier vertretenen Auffassung zum subjektiven Erforderlichkeitsmaßstab beim Kopplungsverbot und bei Art. 6 Abs. 1 lit. b DS-GVO. Hinzu kommt ein grundsätzliches Überwiegen des Datenschutzgrundrechts in diesen Konstellationen im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO. Ausnahmen können bei der technisch unabwendbaren Erfassung von Daten Dritter im Rahmen des Internets der Dinge bestehen, wenn zugleich die Eingriffsintensität minimierende Maßnahmen getroffen werden.

12. Damit sind datenbasierten Geschäftsmodellen, aber auch der Entwicklung des Internets der Dinge enge datenschutzrechtliche Grenzen gesetzt. Diese können auf zwei Arten überwunden werden. Einerseits können Verantwortliche eine datenschonende Alternative anbieten, damit das Kopplungsverbot ausschalten und den Weg für eine wirksame Einwilligung freimachen. Andererseits können sie eigene Pflichten zur Personalisierung von Produkten und zur Schaltung von personalisierter Werbung in die Nutzungsbedingungen aufnehmen. Insbesondere kann damit der Versuch unternommen werden, eine vertragliche Einbeziehung Dritter (auf Anbieter- und Nutzerseite) zu bewerkstelligen und damit die Legitimierungswirkung von Art. 6 Abs. 1 lit. b DS-GVO zu nutzen. Diese zweite Variante zeigt, dass eine Ergänzung des Datenschutzrechts durch die regulatorischen Strukturen des allgemeinen Zivilrechts notwendig ist, um zu bestimmen, inwiefern derartige vertragliche Vereinbarungen wirksam sind. Dem widmet sich das folgende Kapitel.

§ 5 Vernetzte Datenerhebung und -analyse im allgemeinen Privatrecht

Die datenschutzrechtliche Analyse hat ergeben, dass die Rechtmäßigkeit der Datenverarbeitung in zentralen Bereichen der digitalen Wirtschaft im Rahmen sowohl der Geschäftsmodelle mit Daten als Gegenleistung als auch des Internets der Dinge überaus zweifelhaft ist. Hinsichtlich der Einwilligung besteht erhebliche Rechtsunsicherheit und nach hier vertretener Auffassung eine nur sehr eingeschränkte Möglichkeit, in den drei betrachteten Leitfällen die Legalität der Datenverarbeitung zu garantieren. Ein ähnliches Ergebnis zeigt sich hinsichtlich der Datenverarbeitung auf Grundlage der Interessenabwägungsklausel. Anbieter können das rettende Ufer der datenschutzrechtlichen Rechtmäßigkeit daher vor allem auf vertraglichen Wegen gewinnen, indem Verpflichtungen der Verantwortlichen aufgenommen werden, für deren Erfüllung die gewünschten Formen der Datenverarbeitung notwendig sind (weite Leistungspflichten).

Aus diesem Befund ergibt sich für die zivilrechtliche Analyse eine doppelte Zielsetzung. Erstens muss angesichts der Unsicherheit des die Einwilligung betreffenden datenschutzrechtlichen Regimes der DS-GVO untersucht werden, inwiefern die regulatorischen Strukturen des allgemeinen Privatrechts[1] (z. B. §§ 134, 138, 305 ff. BGB) eigenständige, womöglich gar über die DS-GVO hinausgehende Grenzen für die Einwilligung bereithalten. Dies wäre insbesondere relevant, wenn der EuGH zu einer permissiveren Interpretation des Kopplungsverbots und anderer Schranken der Privatautonomie im Datenschutzrecht kommen sollte. Allerdings ist nicht ausgeschlossen, dass auch die allgemeine Rechtsgeschäftslehre des BGB, welche die wirksame Wahrnehmung von Privatautonomie verbürgen soll, eigene Möglichkeiten (z. B. Stellvertretung), aber auch Grenzen der datenschutzrechtlichen Einwilligung beinhaltet.

Zweitens rückt die Frage in das Zentrum des Interesses, inwiefern vertragliche Pflichten wirksam vereinbart werden können, die datenschutzrechtliche Legitimationswirkung nach Art. 6 Abs. 1 lit. b DS-GVO entfalten.[2] Hier sind ebenfalls einerseits die Ermöglichungsstrukturen des allgemeinen Zivil-

[1] Siehe zum Begriff des allgemeinen Privatrechts nur *Säcker*, in: MüKo, BGB, 8. Aufl. 2019, Einleitung Rn. 1.

[2] Siehe etwa die Strategie von Facebook, einen Großteil der Datenverarbeitung nun nicht mehr über die Einwilligung, sondern über Art. 6 Abs. 1 lit. b (sowie f) DS-GVO zu rechtfertigen; dazu zu Recht kritisch *Buchner*, WRP 2019, 1243 (1247).

rechts zu untersuchen, vor allem hinsichtlich der Möglichkeit der Einbeziehung Dritter in einen Vertrag. Andererseits halten auch die Ordnungsstrukturen des Zivilrechts Grenzen der privatautonomen Vertragsgestaltung bereit, die sich unmittelbar auf Art. 6 Abs. 1 lit. b DS-GVO auswirken.

Bei alledem muss jedoch jeweils ein besonderes Augenmerk auf die Wechselwirkung zwischen den jeweiligen Rechtsgebieten gelegt werden. Der Rechtsrahmen des Zivilrechts kann sich nur entfalten, wenn seine Anwendbarkeit nicht durch das unionale Datenschutzrechtregime präkludiert ist. In einem ersten Schritt muss daher untersucht werden, wie weit der Anwendungsvorrang des Unionsrechts insoweit reicht und inwiefern das unionale Datenschutzrecht mit unional harmonisierten Bereichen des nationalen Zivilrechts interagiert (A.). Nur so kann ein integriertes Marktordnungsrecht für digitale Austauschprozesse im Wechselspiel von Datenschutzrecht und allgemeinem Zivilrecht entstehen.

Der Fokus der eigentlichen zivilrechtlichen Untersuchung wird sodann im Schuldrecht liegen und dort das Vertragsrecht sowie das Deliktsrecht als die primären Orte der Strukturierung von Privatautonomie und des Schutzes von Rechtsgütern beleuchten. Dabei sind die Differenzen zum Datenschutzrecht schon im Ausgangspunkt unübersehbar. Im Datenschutzrecht gilt das Verbotsprinzip: Es ist nur erlaubt, was spezifisch erlaubt ist.[3] Im allgemeinen Zivilrecht hingegen herrscht der entgegengesetzte Grundsatz: Es ist erlaubt, was nicht spezifisch verboten ist.[4] Zunächst werden daher Ermöglichungsstrukturen des allgemeinen Zivilrechts für die Einwilligung und vertragliche Vernetzungskontexte dargestellt (B.), mit einem besonderen Fokus auf den Rückgriff auf die Rechtsgeschäftslehre des BGB hinsichtlich der Einwilligung (B.I.) und auf die Einbindung Dritter in datenschutzrechtsrelevante vertragliche Konstruktionen (B.II.). Sodann wechselt der Schwerpunkt des Kapitels zu regulatorischen zivilrechtlichen Strukturen, die auf ihren Eigenwert gegenüber und ihre Vereinbarkeit mit dem Datenschutzrecht hin untersucht werden (C.). Die Anwendbarkeit des deutschen Schuldrechts wird hier, trotz der häufig durch internationale Anknüpfungspunkte geprägten Sachverhaltskonstellationen, zu Analysezwecken unterstellt.

A. Zum Verhältnis von unionalem Datenschutzrecht und mitgliedstaatlichem Privatrecht

Das Rechtsgebiet im Schnittbereich von Datenschutzrecht und Privatrecht stellt in zweifacher Hinsicht eine Querschnittsmaterie dar. Erstens erstreckte es sich über verschiedene, durch das äußere System der Rechtsordnung[5] de-

[3] Siehe bereits oben, Text bei § 4, Fn. 417.
[4] Vgl. *Emmerich*, in: MüKo, BGB, 8. Aufl. 2019, § 311 Rn. 1; *Sattler*, JZ 2017, 1036 (1038).
[5] Zum Begriff des äußeren Systems *Bydlinski*, System und Prinzipien des Privatrechts,

finierte Rechtsgebiete und umspannt dabei neben dem Datenschutzrecht und dem im Rahmen dieser Untersuchung im Zentrum stehenden bürgerlichen Recht auch vor allem das Antidiskriminierungsrecht, das Lauterkeitsrecht und das Kartellrecht. Zweitens – und dies ist für die vorliegende Arbeit entscheidend – liegen die Rechtsmaterien zum Teil auf unterschiedlichen Ebenen des europäischen Mehrebenensystems. Während das Datenschutzrecht, wie gesehen, größtenteils durch unionale Verordnungen geprägt ist, werden die genuin privatrechtlichen Rechtsgebiete, und zumal das BGB, einerseits durch unionsrechtlich harmonisierte Bereiche (etwa das AGB-Recht und jetzt die Umsetzung der DIDD-Richtlinie[6]) und andererseits durch lediglich dem nationalen Recht überantwortete Gebiete konstituiert.

Für das Verhältnis dieser heterogenen Normstrukturen untereinander sind beide Typen von Querschnitten (durch Rechtsgebiete und Normebenen) gleichermaßen relevant. In methodischer Hinsicht muss jedoch logisch primär danach differenziert werden, auf welchen Ebenen die jeweiligen Rechtsbereiche liegen. Geht es um das Verhältnis genuin nationalen Rechts zum unionalen Datenschutzrecht, so muss jeweils gefragt werden, inwiefern letzterem Anwendungsvorrang zukommt (I.). Bei unionsrechtlich harmonisierten Materien des nationalen Rechts bestimmt sich das Verhältnis zum unionalen Datenschutzrecht hingegen nicht nach dem Anwendungsvorrang, sondern nach eigens zu entwickelnden Kriterien für eine Integration unterschiedlicher Sachbereiche des Unionsprivatrechts (II.).

I. Anwendungsvorrang des Unionsrechts

Der unionsrechtliche Anwendungsvorrang ist bereits vielfach in seinen Voraussetzungen und Wirkungen im Schrifttum erläutert worden,[7] weshalb sich die Darstellung hier auf die für das Verhältnis des Datenschutzrechts zu seinen privatrechtlichen Nachbarrechtsgebieten maßgeblichen Aspekte beschränken kann.

Anwendungsvorrang kann das Unionsrecht nur dann beanspruchen, wenn erstens der betreffenden Regelung unmittelbare Anwendbarkeit[8] zugesprochen wird.[9] Nach der ständigen Rechtsprechung des EuGH muss die spezifi-

1996, 10 ff.; *Canaris*, Systemdenken und Systembegriff in der Jurisprudenz, 1983, 19; ferner *Hilbert*, Systemdenken in Verwaltungsrecht und Verwaltungsrechtswissenschaft, 2015, 55.

[6] Siehe bereits die Nachweise oben, in § 1, Fn. 42.

[7] Siehe nur *Kirchhof*, NVwZ 2014, 1537; *Jarass/Beljin*, NVwZ 2004, 1; *Beljin*, EuR 2002, 351; *Niedobitek*, VerwArch 2001, 58; monographisch *Komendera*, Normenkonflikte zwischen EWG- und BRD-Recht, 1974; *Huthmacher*, Der Vorrang des Gemeinschaftsrechts bei indirekten Kollisionen, 1985; *Kulms*, Der Effektivitätsgrundsatz, 2013; *Mangold*, Gemeinschaftsrecht und deutsches Recht, 2011, vor allem §§ 5, 15.

[8] Synonyme Begriffe sind unmittelbare Wirkung und direkte Wirkung; siehe zur Begrifflichkeit *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 174 f.

[9] *Jarass/Beljin*, NVwZ 2004, 1 (3); *Beljin*, EuR 2002, 351 (353 f.).

sche unionsrechtliche Regelung dafür zumindest inhaltlich unbedingt und hinreichend genau formuliert sein.[10] Dies gilt nicht nur für das Primärrecht[11] und Verordnungen,[12] sondern grundsätzlich auch für Richtlinienbestimmungen,[13] bei denen jedoch zusätzlich die Umsetzungsfrist erfolglos abgelaufen sein muss.[14] Die DS-GVO und die ePrivacy-Richtlinie sind in den hier interessierenden Normbereichen daher unmittelbar anwendbar. Eine Ausnahme bilden die ePrivacy-Richtlinie und die DSRL im Horizontalverhältnis, da Richtlinien insoweit nach ständiger Rechtsprechung keine unmittelbare Anwendung finden (keine Ersetzungswirkung/*substitutionary effect*[15]).[16] Lediglich im Einzelfall kommt eine Ausschlusswirkung[17] der Richtlinie gegenüber nationalem Recht (*exclusionary effect*[18]) auch im Horizontalverhältnis in Betracht.[19] Dies

[10] EuGH, Urt. v. 19.1.1982 – Rs. 8/81 (*Becker*); Urt. v. 10.4.1984 – Rs. 14/83 (*von Colson und Kamann*); Urt. v. 30.5.1991 – verb. Rs. 19/90 und 20/90 (*Karella u. a.*) – Rn. 17.

[11] EuGH, Urt. v. 16.6.1966 – Rs. 57/65 (*Lütticke*), NJW 1966, 1630 (1630 f.); *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 175.

[12] *Geismann*, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl. 2015, AEUV, Art. 288 Rn. 12; *Schroeder*, in: Streinz, EUV/AEUV, 3. Aufl. 2018, AEUV, Art. 288 Rn. 45.

[13] *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 251.

[14] EuGH, Urt. v. 5.4.1979 – Rs. 148/78 (*Ratti*); *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 288 Rn. 142 f.

[15] Zum Begriff *Dougan*, 44 Common Market Law Review 2007, 931 (933); *Craig/de Búrca*, EU Law, 2015, 277; *Beljin*, EuR 2002, 351 (353); siehe auch *Streinz*, in: Streinz, EUV/AEUV, 3. Aufl. 2018, EUV, Art. 4 Rn. 40 („Durchgriff des Unionsrechts").

[16] St. Rspr., siehe nur EuGH, Urt. v. 26.2.1986 – Rs. 152/84 (*Marshall*) – Rn. 48; Urt. v. 5.10.2004 – verb. Rs. C-397/01 bis C-403/01 (*Pfeiffer*) – Rn. 108 f.; Urt. v. 7.8.2018 – Rs. C-122/17 (*Smith*) – Rn. 42 f.; Urt. v. 6.11.2018 – verb. Rs. C-569/16 und C-570/16 (*Bauer und Willmeroth*) – Rn. 76; *Canaris*, in: Festschrift Bydlinski, 2002, 47 (55); *Herresthal*, Rechtsfortbildung im europarechtlichen Bezugsrahmen, 2006, 83 f.; *Schroeder*, in: Streinz, EUV/AEUV, 3. Aufl. 2018, AEUV, Art. 288 Rn. 101; *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 288 Rn. 159; weitergehend (unmittelbare Adressierung Privater bei hinreichend bestimmtem Verbot durch Richtlinie) *Wank*, NZA 2004, 246 (252); *Kainer*, GPR 2016, 262 (268 ff.) (Ersetzungswirkung im Zusammenspiel mit einer Primärrechtsnorm).

[17] Begriff bei GA *Saggio*, Schlussanträge v. 16.12.1999 – verb. Rs. C-240/98 bis C-244/98 (*Océano*) – Rn. 37; siehe auch *Streinz*, in: Streinz, EUV/AEUV, 3. Aufl. 2018, EUV, Art. 4 Rn. 39 („Sperrwirkung"); *Canaris*, in: Festschrift Bydlinski, 2002, 47 (54) („derogatorische Wirkung).

[18] *Dougan*, 44 Common Market Law Review 2007, 931 (933); *Craig/de Búrca*, EU Law, 2015, 277.

[19] Der Ausnahmecharakter folgt aus der Rechtsprechung des EuGH, siehe ausdrücklich Urt. v. 7.8.2018 – Rs. C-122/17 (*Smith*) – Rn. 44 f.; Urt. v. 6.11.2018 – verb. Rs. C-569/16 und C-570/16 (*Bauer und Willmeroth*) – Rn. 92; Urt. v. 11.9.2018 – Rs. C-68/17 (*IR*) – Rn. 67–70; Urt. v. 17.4.2018 – Rs. C-414/16 (*Egenberger*) – Rn. 75–82; Urt. v. 5.10.2004 – verb. Rs. C-397/01 bis C-403/01 (*Pfeiffer*) – Rn. 108 f.; siehe auch *Steindorff*, EG-Vertrag und Privatrecht, 1996, 444 f.; *Weatherill*, 16 Yearbook of European Law 1996, 129 (173 Fn. 180); differenzierend (keine Aberkennung eines richtlinienwidrigen, national gewährten Rechts, an dem der Berechtigte ein eigenes Interesse geltend machen kann) *Gundel*, EuZW 2001, 143 (147 f.); eine Ausschlusswirkung ablehnend *Suhr*, Richtlinienkonforme Auslegung im Privatrecht und nationale Auslegungsmethodik, 2011, 268; weitergehend aber (grundsätzlich

betrifft jedoch, wie gesehen,[20] nur noch Altfälle aus der Zeit vor dem Geltungsbeginn der DS-GVO.

Die zweite Voraussetzung des Anwendungsvorrangs liegt nun darin, dass auch eine Kollision zwischen nationalem und unionalem Recht vorliegen muss.[21] Dies ist nicht der Fall, wenn das Unionsrecht selbst, wie die DS-GVO an vielen Stellen,[22] eine explizite Öffnungsklausel zugunsten einer mitgliedsstaatlichen Regelung enthält.[23] Verhältnismäßig klar liegen die Dinge auch, wenn die unionsrechtliche Regelung bestimmte mitgliedsstaatliche Rechtsbereiche explizit für unangetastet erklärt. Dies ist beispielsweise bei Art. 3 Abs. 10 der DIDD-Richtlinie[24] und bei Art. 3 Abs. 6 der Warenkauf-Richtlinie[25] der Fall, nur selten jedoch in der DS-GVO.[26]

Ist das Unionsrecht unmittelbar anwendbar und liegt ein Kollisionsfall vor, so greift der Anwendungsvorrang: entgegenstehendes nationales Recht („unvereinbare Maßnahmen" in den Worten des EuGH in der Rechtssache *Costa/E.N.E.L.*[27]) wird zwar nicht ungültig, darf aber, soweit die Kollision reicht, nicht angewendet werden.[28] Entscheidend ist mithin, ob überhaupt eine Kolli-

---

Ausschlusswirkung auch im Rechtsstreit zwischen Privaten) GA *Saggio*, Schlussanträge v. 16.12.1999 – verb. Rs. C-240/98 bis C-244/98 (*Océano*) – Rn. 37; *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 288 Rn. 163; *Beljin*, EuR 2002, 351 (365 f.); wohl auch *Craig/de Búrca*, EU Law, 2015, 217. In Ansehung von Art. 288 Abs. 3 AEUV ist letztere Position europarechtsdogmatisch vorzugswürdig, was hier aber nicht weiter verfolgt werden muss.

[20] Siehe oben, § 4 B.I.4.b).

[21] *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 1 Rn. 21; *Jarass/Beljin*, NVwZ 2004, 1 (3); allgemein zum Begriff der Kollision zwischen Teilrechtsordnungen, mit weitem Verständnis, *Prütting*, Rechtsgebietsübergreifende Normenkollisionen, 2020, 14 f.

[22] Siehe unten, § 5, Fn. 249.

[23] Siehe nur EuGH, Urt. v. 16.6.1987 – Rs. 53/86 (*Lubertie Romkes*); *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 1 Rn. 73; *Huthmacher*, Der Vorrang des Gemeinschaftsrechts bei indirekten Kollisionen, 1985, 174 f.

[24] Dieser lautet: „Diese Richtlinie lässt die Freiheit der Mitgliedstaaten zur Regelung von Aspekten des allgemeinen Vertragsrechts, wie der Bestimmungen über das Zustandekommen, die Wirksamkeit, die Nichtigkeit oder die Wirkungen eines Vertrags einschließlich der Folgen der Vertragsbeendigung, soweit diese Aspekte nicht in dieser Richtlinie geregelt werden, oder zur Regelung des Rechts auf Schadensersatz unberührt."

[25] Art. 3 Abs. 6 der Warenkauf-Richtlinie lautet: „Diese Richtlinie berührt nicht die Freiheit der Mitgliedstaaten zur Regelung von Aspekten des allgemeinen Vertragsrechts, wie der Bestimmungen über das Zustandekommen, die Wirksamkeit, die Nichtigkeit oder die Wirkungen eines Vertrags einschließlich der Folgen der Vertragsbeendigung, soweit diese Aspekte nicht in dieser Richtlinie geregelt werden, oder zur Regelung des Rechts auf Schadensersatz."

[26] Siehe Art. 2 Abs. 4 und Art. 8 Abs. 3 DS-GVO; zu Letzterem unten, § 4 B.I.3.b)cc).

[27] EuGH, Urt. v. 15.7.1964 – Rs. 6/64 (*Costa/E.N.E.L.*), Slg. 1964, 1259 (1271).

[28] *Craig/de Búrca*, EU Law, 2015, 266; *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 177.

sion vorliegt. Hier müssen zwei Typen von Kollisionen unterschieden werden: direkte und indirekte Kollisionen.[29]

1. Direkte Kollision

Bei der direkten Kollision regeln nationales und unionales Recht denselben Sachverhalt, statuieren jedoch (partiell) unvereinbare Rechtsfolgen.[30] Liegt eine direkte Kollision vor, so präkludiert das Unionsrecht abweichendes nationales Recht im Wege des Anwendungsvorrangs.[31] Die Rechtsfolgen der direkten Kollision lassen daher an Klarheit kaum zu wünschen übrig. Mit erheblichen rechtlichen Unwägbarkeiten behaftet ist vielmehr die Feststellung, ob eine direkte Kollision überhaupt vorliegt. Dies setzt zweierlei voraus.

a) Tatbestandliche Erfassung auf beiden Ebenen

Erstens muss der Sachverhalt, inklusive aller relevanten Elemente, auf beiden Ebenen überhaupt tatbestandlich erfasst sein. Dies muss letztlich durch Auslegung der jeweiligen Rechtsakte geklärt werden. Der EuGH rekurriert für die Feststellung des Anwendungsbereichs einer unionsrechtlichen Bestimmung auf die klassischen Auslegungsmethoden, insbesondere Wortlaut, Systematik und Zielsetzung der Norm. So bemühte er in den Rechtssachen *Abels* und *Karella* systematische[32] und teleologische Kriterien für die Feststellung des unionsrechtlichen Regelungsumfangs.[33] In der Rechtssache *Rabobank*, in der es um die Möglichkeit des Rückgriffs auf nationales Vertretungsrecht im Rahmen des europäischen Gesellschaftsrechts ging, zog er hierfür „Wortlaut und Regelungsgehalt", also Sinn und Zweck, der unionsrechtlichen Vorschrift heran.[34] Teleologische Kriterien waren auch in der jüngst entschiedenen Rechtssache *Schyns* maßgeblich für die Frage, ob die Verbraucherkreditrichtlinie[35] eine Aussage zu verantwortungsbewusster Kreditvergabe enthält.[36]

---

[29] *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 1 Rn. 22.

[30] *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 1 Rn. 75; *Jarass/Beljin*, NVwZ 2004, 1 (3); *Niedobitek*, VerwArch 2001, 58 (73 f.); *Kulms*, Der Effektivitätsgrundsatz, 2013, 31.

[31] Statt vieler *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 1 Rn. 75, 79; *Jarass/Beljin*, NVwZ 2004, 1 (4).

[32] EuGH, Urt. v. 7.2.1985 – Rs. 135/83 (*Abels*) – Rn. 16 f.

[33] EuGH, Urt. v. 7.2.1985 – Rs. 135/83 (*Abels*) – Rn. 18–23; Urt. v. 30.5.1991 – verb. Rs. 19/90 und 20/90 (*Karella u. a.*) – Rn. 25 f.

[34] EuGH, Urt. v. 16.12.1997 – Rs. C-104/96 (*Rabobank*) – Rn. 22.

[35] Richtlinie 2008/48/EG des Europäischen Parlaments und des Rates vom 23. April 2008 über Verbraucherkreditverträge, ABl. 2008 L 133/66.

[36] EuGH, Urt. v. 6.6.2019 – Rs. C-58/18 (*Schyns*) – Rn. 42–45; der EuGH rekurrierte hierbei jedoch nicht nur auf die Erwägungsgründe der Verbraucherkreditrichtlinie (44. und 26. EG), sondern – methodisch unhaltbar – auch auf den erst sechs Jahre später und damit nach der Finanzkrise erlassenen dritten Erwägungsgrund und Art. 18 Abs. 5 lit. a der Wohnimmobilienkreditrichtlinie.

b) Abschließende Regelung auf Unionsebene: Risikospezifizität zum Ersten

Zweitens muss die unionsrechtliche Regelung abschließend sein;[37] sie darf also zum Beispiel nicht lediglich Mindestvorgaben enthalten.[38] Eine direkte Kollision liegt mithin vor, wenn der Sachverhalt nicht allein durch nationales Recht erfasst wird, sondern die Auslegung des Unionsrechts zudem ergibt, dass der Gemeinschaftsgesetzgeber einen normativen Rahmen aufgestellt hat, innerhalb dessen er aller Eventualitäten, inklusive des infrage stehenden Umstands, „Herr zu werden"[39] können glaubt.[40] Insbesondere muss dabei untersucht werden, inwiefern bei unionsrechtlich nicht explizit geregelten Fragestellungen (zum Beispiel weiteren zivilrechtlichen Wirksamkeitsvoraussetzungen der Einwilligung) die unionsrechtliche Regelung eine implizite negative Regelungsanordnung hinsichtlich des fraglichen Sachverhalts enthält[41] oder aber die Regelung der betrefflichen Fragestellung der nationalen Rechtsordnung anheimstellt.[42] Dies kann jeweils nur durch Auslegung ermittelt werden.[43] Dass das Ergebnis eines derartigen Auslegungsvorgangs erhebliche Rechtsunsicherheit birgt, muss nicht eigens betont werden.[44]

---

[37] EuGH, Urt. v. 22.6.1993 – Rs. C-11/92 (*The Queen v Secretary of State for Health*) – Rn. 12; EuGH, Urt. v. 5.4.1979 – Rs. 148/78 (*Ratti*) – Rn. 26 f.; siehe auch *Furrer*, Die Sperrwirkung des sekundären Gemeinschaftsrechts auf die nationalen Rechtsordnungen, 1994, 113 f.; vgl. ferner BVerfG GRUR 2020, 88 Rn. 79 – Recht auf Vergessen II.

[38] Siehe etwa EuGH, Urt. v. 22.6.1993 – Rs. C-11/92 (*The Queen v Secretary of State for Health*) – Rn. 22, wo eine Kollision vom EuGH letztlich verneint wird, weil die betreffenden Bestimmungen (zur Tabaketikettierung) lediglich Mindestvorgaben enthielten.

[39] Formulierung in EuGH, Urt. v. 23.1.1975 – Rs. 31/74 (*Galli*) – Rn. 9/11.

[40] Ausführlich *Furrer*, Die Sperrwirkung des sekundären Gemeinschaftsrechts auf die nationalen Rechtsordnungen, 1994, 101–103 und 105 ff., besonders 125; *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 46; so nunmehr auch BVerfG GRUR 2020, 88 Rn. 79 – Recht auf Vergessen II.

[41] *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 69; siehe auch *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, 401 f.; vgl. für das nationale Recht *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, 1995, 91; *Canaris*, Die Feststellung von Lücken im Gesetz, 1983, 44–47; *Bydlinski*, Juristische Methodenlehre und Rechtsbegriff, 1991, 475; *Basedow*, ZEuP 2014, 402 (402 f.); *Jarass/Beljin*, NVwZ 2004, 1 (3).

[42] Dies kann entweder dergestalt erfolgen, dass eine ausfüllungsbedürftige Regelungslücke im unionalen Rechtsakt vorliegt, die jedoch durch nationales Recht geschlossen werden soll (*Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 69; *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 606; *Bleckmann*, ZGR 1992, 364 [367]), oder durch schlichte Nichtregelung, die nicht einmal die Voraussetzungen einer Regelungslücke erfüllt, siehe siehe etwa EuGH, Urt. v. 19.9.2000 – Rs. C-454/98 (*Schmeink & Cofreth und Strobel*) – Rn. 48 f.; Urt. v. 6.2.2003 – Rs. C-245/00 (*Sena*) – Rn. 34; Urt. v. 6.11.2003 – verb. Rs. C-78/02 bis C-80/02 (*Karageorgou u. a.*) – Rn. 49; Urt. v. 18.6.2009 – Rs. C-566/07 (*Stadeco*) – Rn. 35 (zum Teil vom EuGH als Lücke bezeichnet); zum Begriff der Regelungslücke *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, 1995, 193; ferner *Canaris*, Die Feststellung von Lücken im Gesetz, 1983, 60 f., 137.

[43] Siehe EuGH, Urt. v. 29.7.2019 – Rs. C-469/17 (*Funke Medien*) – Rn. 40.

[44] So auch BVerfG GRUR 2020, 88 Rn. 77 – Recht auf Vergessen II.

Nach hier vertretener Auffassung wird man jeweils danach fragen müssen, ob das spezifische Risiko, dessen sich die nationale Regelung annimmt, durch die unionale Regelung bereits unmittelbar adressiert wurde.[45] Dies kann entweder der Fall sein, wenn eine unionale Regelung, unter Berücksichtigung der unionalen Gesamtrechtsordnung,[46] ihrem Sinn und Zweck nach das in Rede stehende Risiko abdeckt (positive Regelung) oder wenn die Auslegung mit hinreichender Deutlichkeit ergibt, dass das relevante Risiko im konkreten Fall gerade keine Rolle spielen soll (negative Regelung). Letztlich muss dies in jedem Einzelfall separat geklärt werden.

Dass gerade die Adressierung von *Risiken* den relevanten Abgrenzungspunkt darstellt, erhellt im Datenprivatrecht nicht zuletzt daraus, dass die DS-GVO, wie gesehen,[47] ein risikobasiertes Regulierungsinstrument darstellt, das unterschiedliche Rechtsfolgen an das Vorhandensein unterschiedlicher Risiken knüpft. Zum Beispiel bestehen für besonders sensitive Daten nach Art. 9 DS-GVO spezielle Schutzvorkehrungen, ebenso nach Art. 8 DS-GVO für Minderjährige. Diese Dimension war auch bei der Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO prominent zu berücksichtigen.[48] Ferner müssen für die Datenverarbeitung Verantwortliche gem. Art. 24 Abs. 1 DS-GVO technisch-organisatorische Compliance-Maßnahmen ergreifen und nachweisen, die sich an der Eintrittswahrscheinlichkeit und der Schwere der Risiken für die von der Verarbeitung Betroffenen orientieren. Auch für die Reichweite der nach Art. 25 Abs. 1 DS-GVO notwendigen Maßnahmen der Technikgestaltung (*privacy by design/default*) und die nach Art. 32 Abs. 1 DS-GVO erforderlichen Sicherheitsmaßnahmen sind diese Risiken maßgeblich.[49] Schließlich lösen hohe Risiken die Notwendigkeit einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO aus. Die unterschiedlichen, durch Datenverarbeitungsvorgänge berührten Risiken sind für die datenschutzrechtliche Regulierung zentral; sie müssen insofern auch den Maßstab abgeben für die Frage, ob neben dem Datenschutzrecht andere rechtliche Materien diese Vorgänge abweichend regeln können.

2. Indirekte Kollision

Die indirekte Kollision ist für das Datenprivatrecht ebenso relevant wie die direkte Kollision, aber zugleich in ihrer rechtlichen Behandlung etwas komple-

[45] Vgl. *Schantz*, in: BeckOK DatenschutzR, 28. Ed. 1.2.2019, Art. 1 DS-GVO Rn. 9; *Zerdick*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 1 Rn. 13; *Europäische Kommission*, Aufbau einer Europäischen Datenwirtschaft, COM(2017) 9 final, 6: „Beschränkungen [des freien Verkehrs personenbezogener Daten in der Union] aus anderen Gründen als dem Schutz personenbezogener Daten (beispielsweise das Steuerrecht oder Rechnungslegungsvorschriften) fallen dagegen nicht unter diese Verordnung."

[46] Siehe *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, 401; *Bleckmann*, ZGR 1992, 364 (367 f.).

[47] Siehe oben, Text bei § 1, Fn. 82 f.

[48] Siehe oben, § 6 E.I.2.c)bb); ferner *Buchner*, DuD 2016, 155 (157).

[49] Siehe insbesondere auch Art. 32 Abs. 2 DS-GVO.

xer als diese. Bei einer indirekten Kollision wird die Wirksamkeit des Unionsrechts beeinträchtigt durch die nationale Regelung eines unionsrechtlich gerade nicht geregelten Aspekts des durch das Unionsrecht erfassten Sachverhalts oder durch die nationale Regelung eines gänzlich anderen Sachverhalts, insbesondere auch durch Rechtsfolgen, die sich aus anderen Rechtsgebieten ergeben.[50] Darunter fallen nicht nur verfahrensrechtliche,[51] sondern auch materiellrechtliche Regelungen.[52] Durch den Rekurs auf die „Beeinträchtigung der Wirksamkeit des Unionsrechts" ist der Anwendungsbereich der indirekten Kollision ebenso weit wie unbestimmt.

Nach herrschender Meinung wird der Anwendungsvorrang auch bei indirekter Kollision ausgelöst.[53] Er reicht jedoch auch nach dem Verständnis des EuGH nur soweit, wie der unionsrechtliche Effektivitäts- oder Äquivalenzgrundsatz verletzt sind.[54] Bekanntermaßen verlangt ersterer, dass mitgliedstaatliches Recht die Wirksamkeit des Unionsrechts nicht praktisch unmöglich machen[55] oder übermäßig erschweren darf.[56] Das Äquivalenzgebot fordert demgegenüber, dass unionsrechtlich determinierte Sachverhalte gegenüber rein national geregelten nicht nachteilig behandelt werden.[57]

Sofern keine Benachteiligung grenzüberschreitender Fälle erfolgt, ist zwar das Äquivalenzprinzip gewahrt. Deutlich komplexere Abwägungsfragen stellen sich jedoch bei der Bestimmung der Reichweite des Effektivitätsgebots.[58] Damit dieses einschlägig ist, muss zunächst festgestellt werden, dass die Wirksamkeit des Unionsrechtsakts überhaupt eingeschränkt wird. Bereits darin liegt eine wertende Betrachtung. In Betracht kommt insbesondere, dass die Durchsetzung des Unionsrechtsakts erschwert[59] oder auch seine Harmonisie-

[50] *Jarass/Beljin*, NVwZ 2004, 1 (4); *Huthmacher*, Der Vorrang des Gemeinschaftsrechts bei indirekten Kollisionen, 1985, 135. In der Literatur finden sich gewisse definitorische Unterschiede, die hier aber dahinstehen können, siehe etwa *Kulms*, Der Effektivitätsgrundsatz, 2013, 31: Regelung einer anderen Rechtsfrage.

[51] *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 1 Rn. 22.

[52] *Jarass/Beljin*, NVwZ 2014, 1 (4).

[53] *Jarass/Beljin*, NVwZ 2014, 1 (4); *Beljin*, EuR 2002, 351 (357); *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 1 Rn. 22; wohl auch *Schroeder*, in: Streinz, EUV/AEUV, 3. Aufl. 2018, AEUV, Art. 288 Rn. 44.

[54] EuGH, Urt. v. 21.9.1983 – verb. Rs. 205 bis 215/82 (*Deutsche Milchkontor*) – Rn. 22 f.; *Niedobitek*, VerwArch 2001, 58 (75); *Jarass/Beljin*, NVwZ 2004, 1 (4); *Beljin*, EuR 2002, 351 (357).

[55] Grundlegend EuGH, Urt. v. 16.12.1976 – Rs. 33/76 (*Rewe*) – Rn. 5; Urt. v. 16.12.1976 – Rs. 45/76 (*Comet*) – Rn. 11/18.

[56] St. Rspr. seit EuGH, Urt. v. 9.11.1983 – Rs. 199/82 (*San Giorgio*) – Rn. 14; siehe aus jüngerer Zeit etwa Urt. v. 4.12.2003 – Rs. C-63/01 (*Evans*) – Rn. 45; Urt. v. 29.10.2009 – Rs. C-63/08 (*Virginie Pontin*) – Rn. 43; monographisch *Kulms*, Der Effektivitätsgrundsatz, 2013.

[57] Grundlegend EuGH, Urt. v. 16.12.1976 – Rs. 33/76 (*Rewe*) – Rn. 5; Urt. v. 16.12.1976 – Rs. 45/76 (*Comet*) – Rn. 11/18; monographisch *König*, Der Äquivalenz- und Effektivitätsgrundsatz in der Rechtsprechung des EuGH, 2011.

[58] *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 42 f.

[59] Siehe nur *Heinze*, Schadensersatz im Unionsprivatrecht, 2017, 20 ff.

rungswirkung gefährdet wird.[60] Hierfür ist jeweils eine Analyse im konkreten Einzelfall erforderlich.[61] Allerdings können dafür einige analytische Leitlinien aufgestellt werden.

a) Allgemeine Grenzen des Effektivitätsgrundsatzes

Der Effektivitätsgrundsatz ist nicht ohne Grenzen. Zwar wird der verfassungsrechtliche Vorbehalt der Kernbereichsgarantie der grundgesetzlichen Grundrechte (Art. 23 Abs. 1 GG), als Grenze der europäischen Integration,[62] in den hier interessierenden Fallkonstellationen des Datenprivatrechts kaum einmal zum Tragen kommen. Auch aus unionsrechtlicher Perspektive sind dem *principe d'effectivité* jedoch Schranken gezogen. Grundsätzlich kann eine nationale Regelung zwar keine abweichende Rechtsfolge auslösen, wenn der Regelungserfolg des Unionsrechts weitgehend vereitelt, und nicht nur behindert, wird.[63] Beschränkte Wirksamkeitseinbußen sind jedoch hinzunehmen, wenn sie die Durchsetzung des Unionsrechts nicht „übermäßig erschweren".[64] Gewisse nationale Unterschiede sind dabei aufgrund des Teilcharakters der Unionsrechtsordnung unvermeidlich und grundsätzlich im Falle indirekter Kollisionen auch hinzunehmen.[65]

b) Methodische Ausfüllung des Effektivitätsgrundsatzes

Nationale Regelungen müssen sich dennoch prinzipiell am Effektivitätsgrundsatz messen lassen. Aus primärrechtlicher Warte ist für dessen Reichweite die Zielsetzung der jeweiligen nationalen Maßnahme entscheidend.[66] Nur auf dieser Grundlage kann letztlich ein sachgerechter Ausgleich zwischen den Regelungsansprüchen des Unionsrechts und jenen der mitgliedsstaatlichen Vorschriften erreicht werden.[67]

---

[60] Siehe genauer sogleich, Text bei § 5, Fn. 68.

[61] Siehe zur Berücksichtigung des Einzelfalls durch den EuGH bei der Anwendung des Effektivitätsgrundsatzes etwa EuGH, Urt. v. 27.2.2003 – Rs. C-327/00 (*Santex*) – Rn. 56 f.; diesem Maßstab zustimmend *Kulms*, Der Effektivitätsgrundsatz, 2013, 149; *Niedobitek*, VerwArch 2001, 58 (75 f.); *Kment*, EuR 2006, 201 (203).

[62] Siehe dazu etwa *S. Dietz*, AöR 142 (2017), 78; *Thiele*, EuR 2017, 367; *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 30–32.

[63] *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 1 Rn. 76.

[64] EuGH, Urt. v. 4.12.2003 – Rs. C-63/01 (*Evans*) – Rn. 45; *Heinze*, Schadensersatz im Unionsprivatrecht, 2017, 64.

[65] EuGH, Urt. v. 21.9.1983 – verb. Rs. 205 bis 215/82 (*Deutsche Milchkontor*) – Rn. 21; *Niedobitek*, VerwArch 2001, 58 (74 f.).

[66] Siehe auch, für die Berücksichtigung der Zielsetzung einer nationalen Regelung bei der Reichweite des Effektivitätsgrundsatzes, *Schroeder*, AöR 129 (2004), 3 (20); *Heinze*, Schadensersatz im Unionsprivatrecht, 2017, 65; *Furrer*, Die Sperrwirkung des sekundären Gemeinschaftsrechts auf die nationalen Rechtsordnungen, 1994, 114 ff.

[67] *Samara-Krispis/Steindorff*, 29 Common Market Law Review 1992, 615 (621) („recon-

Die Zentralität der *Zielsetzung* nationaler Bestimmungen erhellt schon aus der vom EuGH vertretenen Begründung des Anwendungsvorrangs. Sein Geltungsgrund findet sich in dem autonomen Charakter des Unionsrechts und der Gefahr für dessen einheitliche Anwendung bei Hinnahme einseitiger, vom Unionsrecht abweichender Gesetzgebung durch die Mitgliedstaaten.[68] Zugleich verwies der EuGH bereits in der grundlegenden Rechtssache *Costa/E.N.E.L.* auf die Ziele des EWG-, heute: EU-Vertrags, als maßgeblichen normativen Anker für die Begründung des Anwendungsvorrangs:[69] Nach Art. 4 Abs. 3 UAbs. 3 EUV[70] unterlassen die Mitgliedstaaten alle Maßnahmen, welche die Ziele des Vertrags gefährden könnten.[71] Die Verwirklichung dieser Ziele ist auch Stoßrichtung des Effektivitätsgrundsatzes,[72] der normativ denn auch im Durchsetzungsgebot des Art. 4 Abs. 3 EUV gründet.[73]

aa) Zweistufige Prüfung

Die Abgrenzung zwischen unionsrechtlich noch tolerierten und nicht mehr tolerierbaren nationalen Regelungen im Bereich des Datenprivatrechts muss daher nach funktionalen Kriterien erfolgen, welche die Wirksamkeit des Unionsrechts und seine Zielsetzungen in den Blick nehmen.[74] Bei einer solchen Perspektive wird man nach jeweils durch die einzelne Regelung spezifisch adressierten Risiken für funktionierende Austauschverhältnisse zu unterscheiden haben. Dabei muss nach hier vertretener Auffassung in einer zweistufigen Prüfung geklärt werden, ob die Wirksamkeitseinbuße durch die nationale Norm aus unionsrechtlicher Perspektive hinnehmbar ist, weil sie ein spezifisches Risiko adressiert, das auf unionaler Ebene nicht berücksichtigt wurde (erste Stufe), und ob die Regelung auch mit den Zielen des Unionsrechtsakts kompatibel ist (zweite Stufe).

---

ciliation"); dem folgend *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 653.

[68] EuGH – Rs. 6/64 (*Costa/E.N.E.L.*), Slg. 1964, 1259 (1270); *Schroeder*, AöR 129 (2004), 3 (16); *Niedobitek*, VerwArch 2001, 58 (60); *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 38.

[69] EuGH – Rs. 6/64 (*Costa/E.N.E.L.*), Slg. 1964, 1259 (1270).

[70] Ex-Art. 5 Abs. 2 EWG, auf den der EuGH in der Rs. *Costa/E.N.E.L.* rekurriert, siehe § 5, Fn. 69; siehe auch *Streinz*, in: Streinz, EUV/AEUV, 3. Aufl. 2018, EUV, Art. 4 Rn. 70; *Kulms*, Der Effektivitätsgrundsatz, 2013, 31.

[71] Siehe auch *Huthmacher*, Der Vorrang des Gemeinschaftsrechts bei indirekten Kollisionen, 1985, 159.

[72] EuGH, Urt. v. 13.2.1969 – Rs. 14/68 (*Walt Wilhelm*) – Rn. 4; *Schroeder*, AöR 129 (2004), 3 (19).

[73] Siehe nur *Heinze*, Schadensersatz im Unionsprivatrecht, 2017, 62, sowie die Nachweise in § 5, Fn. 70.

[74] Vgl. auch *Huthmacher*, Der Vorrang des Gemeinschaftsrechts bei indirekten Kollisionen, 1985, 153–160 zum unionsrechtlichen Funktionssicherungsprinzip als Grundlage des Anwendungsvorrangs bei indirekten Kollisionen.

(1) Risikospezifizität zum Zweiten

Um eine Verletzung des Effektivitätsgrundsatzes zu vermeiden, muss sich die nationale Regelung mithin zunächst eines anderen spezifischen Risikos als die unionsrechtliche annehmen (Risikospezifizität).[75] Sofern dasselbe Risiko auf unionaler wie auch nationaler Ebene relevant ist, ist eine abweichende Bewertung auf nationaler Ebene durch den Anwendungsvorrang gesperrt. Insofern gelten die gleichen Erwägungen wie im Rahmen der direkten Kollision.[76]

(2) Zielkompatibilität

Zweitens muss jedoch das national adressierte Risiko sachlich hinreichend gewichtig erscheinen, um die Tragweite des Unionsrechts zu beschränken und die abweichende Rechtsfolge zu rechtfertigen.[77] Andernfalls stünde es im Belieben der Mitgliedstaaten, sachferne, aber vom Unionsrecht nicht berücksichtigte Gesichtspunkte einzuführen und so dessen Wirksamkeit zu konterkarieren. Sachliche Rechtfertigung der Zielsetzung bedeutet dabei nach dem hier vertretenen Ansatz insbesondere: Die Ziele einer nationalen Vorschrift müssen, um mit dem Effektivitätsgrundsatz vereinbar zu sein, gerade auch als Ziele des Unionsrechts rekonstruierbar sein (Zielkompatibilität).[78] Nur so kann die Einheitlichkeit des Unionsrechts wenigstens auf einer abstrakten Ebene gewahrt bleiben.

Dass damit eine gewisse Beschränkung der zu berücksichtigenden Zielsetzungen und Risiken auf die unionsrechtlich relevanten einhergeht,[79] ist methodisch als Folge des Anwendungsvorrangs des Unionsrechts letztlich hinzunehmen. Dies ist in gewissem Rahmen unvermeidlich, wenn eine nationale Rechtsordnung sich zu Gunsten einer supranationalen ihrer Rechtsetzungshoheit in bestimmten Rechtsbereichen begibt.

Das Kriterium der unionsrechtlichen Rekonstruierbarkeit der Zielsetzung der nationalen Norm zeigt sich auch deutlich in der gerade bereits angesprochenen Rechtssache *Schyns*. Dort stellte der EuGH explizit fest, dass eine (indirekte) Kollision zwischen einer nationalen Regelung und der Verbraucherkreditrichtlinie deshalb nicht vorlag, weil das Ziel der nationalen Regelung die Zielsetzung der relevanten Norm der Verbraucherkreditrichtlinie (jeweils die Praktizierung verantwortungsbewusster Kreditvergabe) gerade unterstützte.[80]

---

[75] Siehe oben, § 5, Fn. 45.

[76] Siehe oben, § 5 A.I.1.b).

[77] *Nettesheim*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 1 Rn. 76.

[78] Vgl. *Kulms*, Der Effektivitätsgrundsatz, 2013, 151: Parallelwertung im Unionsrecht; kritischer ebd., 210; ferner *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 41 (ähnliche Vorschrift im Gemeinschaftsrecht).

[79] Siehe *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 655 („Präponderanz des gemeinschaftsrechtlich geschützten Interesses").

[80] EuGH, Urt. v. 6.6.2019 – Rs. C-58/18 (*Schyns*) – Rn. 45.

bb) Folgerung: Sachgerechte Ergänzung des Unionsrechts durch nationales Recht

Nationales Recht übt, wenn die beiden genannten Kriterien der Risikospezifizität und Zielkompatibilität vorliegen, eine Ergänzungsfunktion gegenüber dem Unionsrecht aus:[81] Es beansprucht nicht die Durchsetzung idiosynkratischer Regelungsziele, sondern fügt sich in die unionsrechtliche Zwecksetzung, trotz potenziell abweichender Beurteilung des Einzelfalls, grundsätzlich ein. Ob andere Mitgliedstaaten ähnliche Regelungen vorhalten, wird zwar vom EuGH teilweise als relevant angesehen,[82] kann jedoch richtigerweise als gänzlich kontingentes Faktum kein Bewertungskriterium sein. Maßgeblich ist mithin die Passfähigkeit des Ziels der nationalen Regelung für die Zwecke des Unionsrechts.

Im Bereich der Schaffung eines rechtlichen Rahmens für die digitale Wirtschaft ist daher der Anwendungsvorrang in Fällen der indirekten Kollision als ein funktionaler Mechanismus zum Aufbau eines digitalen Binnenmarkts unter besonderer Berücksichtigung des Datenschutzgrundrechts zu rekonstruieren, in dem verschiedene Typen von Risiken, die sich aus digitalen Austauschprozessen ergeben, sachadäquat und durch einander ergänzende Normbereiche adressiert werden.

cc) Methodisches Ergebnis

Grundsätzlich kann bei einer Minderung der Wirksamkeit des Unionsrechts eine Verletzung des Effektivitätsgebots, zumal im Datenprivatrecht, nur unter den beiden genannten Voraussetzungen verneint werden: Adressierung eigenständiger, spezifischer Risiken durch die nationale Norm (Risikospezifizität); und sachliche Vereinbarkeit der nationalen Regelung mit den Zielen des Unionsrechts (Zielkompatibilität). Denn dann ist der durch die nationale Regelung entschiedene Sachverhalt, trotz Überschneidungen mit dem unionsrechtlich geregelten, hinreichend different, um eine eigenständige Beantwortung der durch die differierenden Risiken hervorgerufenen Rechtsfragen zu ermöglichen, ja zu fordern. Nur so kann ein abgestimmtes System der Marktordnung entwickelt werden, das jeweils spezifische (Markt-)Risiken konkret adressiert, ohne zugleich die Integrationsfunktion des Unionsrechts für den Binnenmarkt zu beschädigen. Dies entspricht einem Privatrecht, das in seiner regulatorischen Funktion spezifische, ökonomisch oder sonst normativ relevante Risiken sachgerecht zuweist.

[81] *Huthmacher*, Der Vorrang des Gemeinschaftsrechts bei indirekten Kollisionen, 1985, 183.

[82] Siehe die Nachweise bei *Kulms*, Der Effektivitätsgrundsatz, 2013, 153.

c) Operationalisierung für das Datenprivatrecht

Wenn eine zentrale Voraussetzung für die Kompatibilität nationaler Regelungen mit dem Anwendungsvorrang des Unionsrechts im Falle indirekter Kollision die Rekonstruierbarkeit der nationalen Zielsetzung als solche des Unionsrechts ist, ruft dies unmittelbar die Frage nach den wesentlichen Zielen des unionalen Datenschutzrechts auf.

aa) Ziele des unionalen Datenschutzrechts

Art. 1 Abs. 1 DS-GVO benennt diese Ziele markant: einerseits die Ausgestaltung des Datenschutzgrundrechts („Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten") und andererseits der freie Verkehr personenbezogener Daten zwischen den Mitgliedstaaten.[83]

Beide Ziele bedingen einander, stehen jedoch zugleich in einem Spannungsverhältnis.[84] Zunächst ist anzuerkennen, dass gerade die Vereinheitlichung des Datenschutzniveaus zwischen den Mitgliedstaaten dazu dient, den grenzüberschreitenden Verkehr personenbezogener Daten zu erleichtern. Insofern leistet die grundsätzliche Vollharmonisierung der DS-GVO einen unbestreitbaren Beitrag zum Funktionieren des Binnenmarkts.[85] Nur so ist die Formulierung in Art. 1 Abs. 3 DS-GVO zu verstehen, wonach der „freie Verkehr personenbezogener Daten in der Union […] aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden" darf. Den Mitgliedstaaten ist mithin das Argument abgeschnitten, gerade wegen unterschiedlicher Datenschutzrechtsniveaus den Datenverkehr weiter zu beschränken, als es die DS-GVO ohnehin tut.[86] Voraussetzung hierfür ist jedoch lediglich die Existenz eines Regimes der weitgehenden Harmonisierung des Datenschutzniveaus, unabhängig davon, wie die Schutzhöhe konkret ausgeprägt ist.[87]

Gerade diese Frage der Schutzhöhe impliziert jedoch ein Spannungsverhältnis zwischen den beiden Hauptzielen der DS-GVO. Einerseits sprechen der sechste und zehnte Erwägungsgrund von einem hohen Schutzniveau; anderer-

[83] Siehe auch den 1.–3. und 9. Erwägungsgrund der DS-GVO; hinzu tritt die Ausgestaltung des Grundrechts auf Achtung der Privatsphäre, Art. 7 GRCh: EuGH, Urt. v. 6.10.2015 – Rs. C-362/14 (*Schrems*) – Rn. 42; Urt. v. 13.5.2014 – Rs. C-131/12 (*Google Spain*) – Rn. 69; siehe auch *Zerdick*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 1 Rn. 7; *Schantz*, in: BeckOK DatenschutzR, 26. Ed. 1.2.2017, Art. 1 DS-GVO Rn. 6.

[84] *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 1 DS-GVO Rn. 20; *Franzen*, in: Franzen/Gallner/Oetker, Kommentar zum europäischen Arbeitsrecht, 2. Aufl. 2018, Art. 1 DS-GVO Rn. 2.

[85] *Zerdick*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 1 Rn. 2 und unten, § 5 A.I.2.c)bb)(1).

[86] Siehe den 9., 10. und 13. Erwägungsgrund der DS-GVO; ferner *Plath*, in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Artikel 1 DSGVO Rn. 6.

[87] *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 319; vgl. auch *Klement*, JZ 2017, 161 (163).

seits wird der Binnenmarkt, auf den das Ziel der Gewährleistung eines freien Datenverkehrs ausgerichtet ist, nach Art. 26 Abs. 2 AEUV gerade durch die vier Grundfreiheiten konstituiert. Es ist unübersehbar, dass ein höheres Datenschutzniveau zugleich die unternehmerische Ausübung dieser Grundfreiheiten, sofern die unternehmerische Tätigkeit gerade auf grenzüberschreitende Datenverarbeitung gerichtet ist, erschwert. Gleiches gilt für die in Art. 16 GRCh verankerte unternehmerische Freiheit. Diese wird nicht nur im vierten Erwägungsgrund der DS-GVO erwähnt, sondern ihre Ausgestaltung auch prominent von der Kommission im Entwurf zur DS-GVO als ein zentrales Ziel derselben herausgestellt.[88] Während mithin die Vereinheitlichung des Schutzniveaus zugleich den Interessen der Verarbeiter dient, tritt die Spannung zwischen der Binnenmarktzielsetzung einerseits und der Ausgestaltung des Datenschutzgrundrechts andererseits bei der Feinjustierung der Höhe des Schutzniveaus offen zutage.

Diese Janusköpfigkeit der DS-GVO ist primärrechtlich bedingt, schon durch die Rechtsgrundlage für die Verordnung. Beide Ziele werden in Art. 16 Abs. 2 AEUV genannt. Dies ist eine klare Fortentwicklung gegenüber der DSRL: Deren Rechtsgrundlage in Art. 100a EGV, nunmehr Art. 114 AEUV, erwähnte das Datenschutzgrundrecht gerade nicht, sondern nur die Harmonisierung des Binnenmarkts.[89] Dies führte dazu, dass Generalanwalt *Tizzano* klar aussprach, dass die Ausgestaltung des Datenschutzes keine von Binnenmarkterwägungen unabhängige Zielsetzung der DSRL sein könne.[90] Diese durch die Rechtsgrundlage bedingten Grenzen sind durch Art. 16 Abs. 2 AEUV nunmehr beseitigt.

Angesichts dieser primärrechtlichen Ausgangslage stehen die beiden Hauptziele der DS-GVO daher gleichrangig nebeneinander.[91] Zumal für das Da-

---

[88] *Europäische Kommission*, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig, 2 („dass die digitale Wirtschaft im Binnenmarkt weiter Fuß fasst").

[89] *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 333, ff.; *Klement*, JZ 2017, 161 (164).

[90] GA *Tizzano*, Schlussanträge v. 14.11.2002 – verb. Rs. C-465/00, C-138/01 und C-139/01 (*Österreichischer Rundfunk u. a.*) – Rn. 53 f.; GA *Tizzano*, Schlussanträge v. 19.9.2002 – Rs. C-101/01 (*Lindqvist*) – Rn. 42; zustimmend *Lynskey*, The Foundations of EU Data Protection Law, 2015, 60; für eine Pluralität der Zwecke, unter Berücksichtigung der Interessen der Datenverarbeiter und des Binnenmarktbezugs, auch *Klement*, JZ 2017, 161 (162 f.).

[91] Die Einschätzung, dass die Gewährleistung des freien Verkehrs personenbezogener Daten „Hauptziel" der DSRL ist, findet sich zwar in den älteren Urteilen EuGH, Urt. v. 20.5.2003 – verb. Rs. C-465/00, C-138/01 und C-139/01 (*Österreichischer Rundfunk u. a.*) – Rn. 70; Urt. v. 9.3.2010 – Rs. C-518/07 (*Kommission/Deutschland*) – Rn. 20. Dies erklärt sich jedoch wohl primär aus der erwähnten Heranziehung der Rechtsgrundlage in Art. 100a EGV Abs. 1 aF (später Art. 95 Abs. 1 EGV, nunmehr Art. 114 Abs. 1 AEUV) für den Erlass der DSRL (siehe *Lynskey*, The Foundations of EU Data Protection Law, 2015, 60 f.). Eine eigenständige Kompetenz der Union zur Harmonisierung des Datenschutzrechts wurde

tenschutzprivatrecht, dessen Regelung kompetenziell nur auf Art. 16 Abs. 2 UAbs. 1 S. 1 Var. 3 AEUV gestützt werden kann („und über den freien Datenverkehr"),[92] bleibt die Binnenmarktfinalität daher zwingend.[93] Die doppelte Zielsetzung kommt in dem Doppeltitel der DS-GVO (Verordnung einerseits „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten", andererseits „zum freien Datenverkehr") auch programmatisch zum Ausdruck[94] und wurde vom EuGH bereits bei der Auslegung der Datenschutz-Richtlinie mehrfach betont.[95] Die beiden Zielsetzungen müssen daher im Wege der Auslegung in jedem Einzelfall in einen schonenden Ausgleich gebracht werden.[96] Der vierte Erwägungsgrund der DS-GVO ruft ferner in Erinnerung, dass auch das Datenschutzgrundrecht kein uneingeschränkt gewährtes Recht ist, sondern mit anderen primärrechtlich geschützten Rechten und Rechtsgütern, unter anderem der unternehmerischen Freiheit, abgewogen werden muss. Dies macht jedoch zugleich die Frage der Passfähigkeit nationaler Zielsetzungen für die Ziele des unionalen Datenschutzrechts komplexer.

bb) Unionsrechtskompatible nationale Zielsetzungen

Nationale Regelungen müssen sich in diese Zielsetzungen des unionalen Datenschutzrechts zumindest einfügen. Dabei kommen Zielsetzungen in Be-

erst durch den Vertrag von Lissabon in Art. 16 Abs. 2 AEUV eingefügt. Die, im Übrigen in anderen Urteilen abgemilderte (siehe § 5, Fn. 95), Wertung des EuGH zur DSRL kann daher auf die DS-GVO wegen der geänderten Rechtsgrundlage sowie infolge der markanten Auswechslung der Reihenfolge der Benennung der beiden Ziele im 3. Erwägungsgrund der DS-GVO gegenüber dem 3. Erwägungsgrund der DSRL nicht übertragen werden. Für Gleichrangigkeit auch *Buchner*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 1 DS-GVO Rn. 1; *Pötters*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 1 DS-GVO Rn. 5; *Lynskey*, The Foundations of EU Data Protection Law, 2015, 62 f.; *Klement*, JZ 2017, 161 (164); wohl auch *Plath*, in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Artikel 1 DSGVO Rn. 6; *Schneider*, DV 44 (2011), 499 (505); tendenziell für einen Vorrang des Datenschutzgrundrechts *Schantz*, in: BeckOK DatenschutzR, 26. Ed. 1.2.2017, Art. 1 DS-GVO Rn. 3; deutlicher Hornung/Spiecker gen. Döhmann, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 1 DS-GVO Rn. 28 ff.; *Clifford/Graef/Valcke* 20 German Law Journal 2019, 679 (709); wohl auch *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 317 ff., 333.

[92] *Klement*, JZ 2017, 161 (164); *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 335 f.

[93] *Klement*, JZ 2017, 161 (164); vgl. auch *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 336.

[94] Siehe auch Art. 1 DS-GVO und deren 10. Erwägungsgrund; ferner *Buchner*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 1 DS-GVO Rn. 19; *Schantz*, in: BeckOK DatenschutzR, 26. Ed. 1.2.2017, Art. 1 DS-GVO Rn. 2; *Kamann/Miller*, NZKart 2016, 405 (407 f.); *Svantesson*, 34 Computer Law and Security Review 2018, 25 (29); zur DSRL *Roßnagel*, MMR 2004, 95 (100); *v. Lewinski/Herrmann*, ZD 2016, 467 (470).

[95] EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 96; Urt. v. 24.11.2011 – verb. Rs. C-468/10 und C-469/10 (*ASNEF*) – Rn. 29, 34.

[96] Anders jedoch versteht etwa *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 317 f. das Verhältnis der Zielsetzungen, die auf unterschiedlichen Ebenen lägen und daher nicht in einen Ausgleich gebracht werden müssten oder könnten.

tracht, welche den Binnenmarkt (1) oder das Datenschutzgrundrecht stärken sollen (2) oder aber darüberhinausgehende, weitere Ziele verfolgen (3).

(1) Binnenmarktkompatibilität

Die Verankerung auch im Komplex der binnenmarktrelevanten Vorschriften macht die DS-GVO, und das unionale Datenschutzrecht im Allgemeinen, zu einem gewichtigen Teil des unionalen Wirtschaftsrechts und ist insbesondere bei der hier interessierenden Frage der Konkurrenz mit nationalen Regelungen zu beachten.

Im Rahmen des unionalen Wirtschaftsrechts stellen, wie der EuGH prägnant feststellte, die Schaffung eines Binnenmarkts und einer Wirtschafts- und Währungsunion die zentralen Ziele dar.[97] Unter diesen ist das nunmehr in Art. 3 Abs. 3 EUV verankerte, seit jeher für das europäische Projekt zentrale[98] Binnenmarktziel für digitale Austauschprozesse in der Tat besonders maßgeblich. Dies betont auch die Kommission unermüdlich in ihrer digitalen Binnenmarktstrategie.[99] Die Binnenmarktkompetenzvorschrift des Art. 114 Abs. 1 AEUV ist denn auch Rechtsgrundlage für Gesetzgebungsvorhaben betreffend die digitale Wirtschaft, so etwa die DIDD-Richtlinie[100] und die Richtlinie über den Online-Warenhandel.[101] Der Binnenmarkt wird zwar gem. Art. 26 Abs. 2 AEUV primär durch die vier Grundfreiheiten verwirklicht; jedoch gewinnt das Datenschutzrecht auch hier, wie gesehen, zunehmend an Bedeutung, da einheitliche rechtliche Rahmenbedingungen angesichts der Ubiquität des Datenbezugs modernen Wirtschaftens die Ausübung der Grundfreiheiten, gerade durch Unternehmen, erheblich erleichtern.[102] Dies war gerade Grund für die Ersetzung der Datenschutz-*Richtlinie* durch die Datenschutz-Grund*verordnung*.[103] Die marktintegrative Funktion des harmonisierten Datenschutzrechts

[97] EuGH, Gutachten 1/91 v. 14.12.1991, EWR I, EU:C:1991:490, Rn. 18; Urt. v. 20.3.2003 – Rs. C-3/00 (*Dänemark/Kommission*) – Rn. 56; siehe auch *Kirchhof*, NVwZ 2014, 1537 (1540).

[98] *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 20–25 („Hauptaufgabe der Gemeinschaft", ebd., 22); *Furrer*, Die Sperrwirkung des sekundären Gemeinschaftsrechts auf die nationalen Rechtsordnungen, 1994, 74 („zentrales […] Ordnungsprinzip").

[99] *Europäische Kommission*, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 final.

[100] *Europäische Kommission*, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM(2015) 634 final, 5.

[101] *Europäische Kommission*, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte des Online-Warenhandels und anderer Formen des Fernabsatzes von Waren, COM(2015) 635 final, 6.

[102] *Pötters*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 1 DS-GVO Rn. 16 f.

[103] Siehe den 13. Erwägungsgrund S. 1 der DS-GVO; *Europäische Kommission*, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig, 2.

hatte der EuGH bereits in den ersten beiden Entscheidungen zur DSRL – *Österreichischer Rundfunk* und *Lindqvist*[104] – gestärkt, indem er davon absah, die Anwendbarkeit der Richtlinie von einer konkreten Betroffenheit einer Grundfreiheit im Einzelfall, und damit von einem grenzüberschreitenden Element, abhängig zu machen.[105]

Dies hat Auswirkungen auf die Anwendbarkeit nationaler Regelungen neben der DS-GVO. Erwächst der Anwendungsvorrang im Bereich der digitalen Wirtschaft insbesondere aus dem Verbot, durch mitgliedsstaatliche Maßnahmen die Verwirklichung des Binnenmarktes zu unterminieren, so erscheint es zulässig, bei einer auf das Funktionieren des Binnenmarktes ausgerichteten, marktspezifischen Perspektive jedenfalls tendenziell solche nationale Normen nicht dem Anwendungsvorrang im Falle indirekter Kollision zu unterwerfen, deren Zielsetzung gerade in der Einhegung von spezifischen, durch das unionale Datenschutzrecht nicht adressierten Risiken für den europäischen Binnenmarkt besteht.[106] Ob eine solche Zielsetzung vorliegt, muss jeweils im Einzelfall durch Auslegung geklärt werden. Auch hier verbleibt signifikante und irreduzible Rechtsunsicherheit.

(2) Datenschutzkompatibilität

Das zweite große Ziel des sekundärrechtlichen unionalen Datenschutzrechts ist nach Art. 1 Abs. 1 und Abs. 2 DS-GVO, wenig überraschend, die Ausgestaltung des primärrechtlich verankerten Datenschutzgrundrechts.[107] Diese grundrechtliche Prägung ist gerade Signum des Datenschutzprivatrechts. Insofern sind nationale Regelungen, die mit unionsrechtlichen indirekt kollidieren, auch dann mit einer legitimen Zielsetzung ausgestattet, wenn sie das Datenschutzrecht stärken sollen. Allerdings sind die unionsrechtlichen Vorgaben hier, sofern nicht eine der zahlreichen Öffnungsklauseln der DS-GVO greift, nicht selten abschließend, sodass in diesen Fällen eine direkte Kollision regelmäßig wahrscheinlicher ist. Daher zieht eine Abweichung von unionsrechtlichen Vorgaben im Bereich der Ausgestaltung des Datenschutzgrundrechts regelmäßig die Unanwendbarkeit der nationalen Vorschrift nach sich.[108]

---

[104] EuGH, Urt. v. 20.5.2003 – verb. Rs. C-465/00, C-138/01 und C-139/01 (*Österreichischer Rundfunk u. a.*) – Rn. 42; EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 41 f. Zu beiden Rechtssachen ausführlich oben, § 4 A.II.2.b)aa)(1).

[105] *Lynskey*, The Foundations of EU Data Protection Law, 2015, 54.

[106] Ähnlicher Vorschlag, allerdings ohne die Binnenmarktbeschränkung, bei *Samara-Krispis/Steindorff*, 29 Common Market Law Review 1992, 615 (621 f.): nationale Regelungen können dann aufrechterhalten werden, wenn sie bei einheitlicher Betrachtung *lex specialis* gegenüber der europäischen Regelung wären, also wiederum spezifische, zusätzliche Elemente einführen.

[107] *Pötters*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 1 DS-GVO Rn. 21–23.

[108] Ähnlich im Ergebnis *Schantz*, in: BeckOK DatenschutzR, 27. Ed. 1.2.2019, Art. 1 DS-GVO Rn. 9.

Ein Bereich, in dem unionsrechtliche Regelungen nicht notwendig abschließend sind, ist jedoch derjenige, den man als sekundäres Datenschutzrecht bezeichnen könnte. Damit sind Vorschriften angesprochen, die zwar nicht spezifisch das Datenschutzgrundrecht ausgestalten, jedoch in bestimmten digitalen Austauschprozessen die Gewährleistung effektiven Datenschutzes befördern. Dies können zum Beispiel Normen des allgemeinen Teils des BGB sein, die ganz grundsätzlich die Dispositionsfreiheit schützen (z. B. § 119 BGB), jedoch im Zusammenspiel mit den Voraussetzungen einer wirksamen Einwilligung gerade auch zu einer notwendigen Voraussetzung des selbstbestimmten Umgangs mit personenbezogenen Daten werden. Eine derartige Zielsetzung erscheint mit Blick auf das unionale Datenschutzrecht durchaus legitim, auch wenn im Einzelfall geprüft werden muss, ob eine nationale Regelung die Harmonisierungswirkung des Unionsrechtsakts übermäßig behindert.[109]

(3) Sonstige Zielsetzungen

Zuletzt ist zu bemerken, dass mit diesen Ausführungen nicht ausgeschlossen werden soll, dass auch andere Erwägungen, jenseits von Binnenmarktkompatibilität und der Stärkung des Datenschutzgrundrechts, eine nationale Abweichung rechtfertigen können, da sich auch das unionale Datenschutzrecht nicht in diesen beiden Zielen vollkommen erschöpft.[110] Grundlage der Zulässigkeit einer nationalen Norm ist im Fall einer indirekten Kollision jedoch richtigerweise, abgesehen von der eng begrenzten Kernbereichs- und Identitätskontrolle nach Art. 23 Abs. 1 GG,[111] nicht ein im nationalen Recht wurzelnder Vorbehalt gegenüber dem Unionsrecht.[112] Vielmehr muss die Schranke immer aus dem Unionsrecht selbst entwickelt und mit seinen Zielen im Einzelfall vereinbar sein.[113] Angesichts der Vielzahl von Öffnungsklauseln in der DS-GVO (diesbezüglich allem in Art. 85 ff. DS-GVO) wird man zudem auch hier häufig davon ausgehen können, dass die Berücksichtigung sonstiger Zielsetzungen in der DS-GVO abschließend (partiell durch Delegation an die Mitgliedstaaten) geregelt ist.

Für den Bereich der journalistischen Tätigkeit etwa besteht eine Öffnungsklausel in Art. 85 DS-GVO, welche die Abwägung von Belangen der Informations- und Meinungsfreiheit mit dem Datenschutzgrundrecht zur Aufgabe der

---

[109] Dazu im Einzelnen unten, § 5 B.II.

[110] Vgl. nur den 4. Erwägungsgrund der DS-GVO; ferner, zu Informations- und Meinungsfreiheit, *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 257 f., 359 ff.; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 60 f., 80 ff.; sowie sogleich im Text.

[111] Dazu oben, Text bei § 5, Fn. 62.

[112] So aber *Komendera*, Normenkonflikte zwischen EWG- und BRD-Recht, 1974, 174–182.

[113] Siehe ausführlich *Huthmacher*, Der Vorrang des Gemeinschaftsrechts bei indirekten Kollisionen, 1985, 167 ff., auch zur Kritik der auf einem nationalen Vorbehalt aufruhenden Position von *Komendera*; ferner *Kulms*, Der Effektivitätsgrundsatz, 2013, 151 f.

Mitgliedstaaten erklärt. Der EuGH hat im Urteil *Satamedia*, beruhend auf der Vorgängervorschrift in Art. 9 DSRL, denn auch eine Veröffentlichung von personenbezogenen Daten zu journalistischen Zwecken überaus weitgehend für zulässig erachtet.[114]

d) Ergebnis zur indirekten Kollision

Insgesamt zeigt sich damit, dass auf unionsrechtlicher Ebene zwei große Zielsetzungen das Datenschutzrecht umspannen: die Stärkung des digitalen Binnenmarkts einerseits und die Gewährleistung des Datenschutzgrundrechts andererseits. Nationale Vorschriften, deren Zielsetzungen sich im Rahmen dieser teleologischen Struktur bewegen, können daher zumindest grundsätzlich auch bei indirekten Kollisionen anwendbar bleiben. Letztlich ist dies jeweils eine Frage der Reichweite des unionsrechtlichen Effektivitätsgrundsatzes im Einzelfall.

3. Zusammenfassung zum Anwendungsvorrang

Zusammenfassend lässt sich damit sagen: Der unionsrechtliche Anwendungsvorrang greift, wenn in einem Kollisionsfall die unionsrechtliche Norm unmittelbar anwendbar ist. Die unmittelbare Anwendbarkeit des Unionsrechts steht typischerweise allenfalls bei Richtlinienbestimmungen, die zwischen Privaten Anwendung finden sollen, infrage. Im Datenprivatrecht betrifft dies besonders Altfälle aus der Zeit vor Geltungsbeginn der DS-GVO. Steht die unmittelbare Anwendbarkeit fest, so ist der unionsrechtliche Anwendungsvorrang vor nationalem Recht bei direkten Kollisionen unproblematisch zu implementieren, wenn also für denselben Tatbestand unterschiedliche, sich ausschließende Rechtsfolgen statuiert werden. Die nationale Regelung kann, soweit die Kollision reicht, nicht angewendet werden. Ob jedoch das Unionsrecht eine Fragestellung abschließend regelt und somit eine direkte Kollision überhaupt vorliegt, ist nach hier vertretener Auffassung nach dem Kriterium der Risikospezifizität zu beurteilen.

Dieses kommt auch bei der indirekten Kollision zum Tragen. Eine solche liegt vor, wenn nationale Regelungen, zumeist aus anderen Rechtsbereichen, dem Äquivalenz- oder Effektivitätsgrundsatz zuwiderlaufen. Insbesondere die Bestimmung der Grenzen des Effektivitätsgrundsatzes ist hier diffizil. Sie sind für jede fragliche nationale Regelung separat und im Einzelfall zu ziehen. Grundsätzlich gilt jedoch, dass nationale Regelungen hingenommen werden müssen, wenn sie die praktische Wirksamkeit des Unionsrechts lediglich mäßig beeinträchtigen. Dies ist vor allem dann der Fall, wenn die nationale Regelung ein spezifisches, unional nicht abgedecktes Risiko adressiert und zu-

[114] EuGH, Urt. v. 16.12.2008 – Rs. C-73/07 (*Satakunnan Markkinapörssi und Satamedia*) – Rn. 62; zustimmend *Härting*, CR 2009, 229 (232 f.); kritisch *Lynskey*, The Foundations of EU Data Protection Law, 2015, 55 f.

gleich die Zielsetzung der nationalen Regelung auch als unionsrechtliche Zielsetzung rekonstruiert werden kann. Im Rahmen des Datenprivatrechts laufen daher solche nationalen Regelungen tendenziell nicht dem Effektivitätsgrundsatz zuwider, die Risiken adressieren, die auch für den europäischen Binnenmarkt relevant sind.

II. Sachintegration ebenengleichen Rechts

Der Anwendungsvorrang greift hingegen nicht, wenn zwei Rechtsnormen auf derselben Regelungsebene liegen (bzw. die nationale Norm lediglich eine unionsrechtliche Richtlinie umsetzt) und beide Normen innerhalb dieser Ebene denselben Rang innehaben.[115] Dennoch können (natürlich) auch in all diesen außerhalb des Anwendungsvorrangs gelegenen Konstellationen Kollisionslagen und Koordinationsbedürfnisse auftreten. Dies kann auch dann der Fall sein, wenn zwar unterschiedliche, einander aber nicht ausschließende Rechtsfolgen an denselben Tatbestand geknüpft sind (kumulative oder alternative Konkurrenz[116]). In jedem Fall müssen Wege gefunden werden, ein ebeneninternes Konkurrenzverhältnis aufzulösen.[117] Man denke insoweit nur an das umstrittene Verhältnis zwischen dem harmonisierten Bereich der unionsrechtlichen AGB-Kontrolle und der DS-GVO[118] oder auch zwischen der DS-GVO und der DIDD-Richtlinie.[119]

In diesen Fällen besteht mithin ein unabweisliches Bedürfnis nach einer *Sachintegration* der beteiligten Normen und letztlich auch der Rechtsgebiete: Ihre Wertungen müssen aufeinander abgestimmt werden, um nicht nur Kollisionsfälle zu lösen, sondern die Kohärenz der Rechtsordnung im Datenprivatrecht sicherzustellen.[120] Erschwert wird die Auflösung dieser Spannungslagen

---

[115] Zur Anwendung der *lex superior* im Verhältnis von unionalem Primärrecht und Sekundärrecht, siehe *Bengoetxea*, The legal reasoning of the European Court of Justice, 1993, 247; *Höpfner*, Die systemkonforme Auslegung, 2008, 228 f.

[116] Dazu *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, 1995, 88 Fn. 28; für das europäische Recht *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 545.

[117] Dieselben Fragen stellen sich im Falle einer Situierung der Normen auf unterschiedlichen Regelungsebenen, bei der jedoch der Anwendungsvorrang wegen nicht übermäßiger Erschwerung der Durchsetzung des Unionsrechts nicht greift.

[118] Dazu noch ausführlich unten, § 5 C.II.1.

[119] Mittlerweile zumindest entschärft durch den klar ausgesprochenen Vorrang in Art. 3 Abs. 8 DIDD-Richtlinie und die Erläuterungen in den Erwägungsgründen 37–40 der DIDD-Richtlinie; zum angesprochenen Verhältnis *Sein/Spindler*, 15 European Review of Contract Law 2019, 257 (264 f.); *Sein/Spindler*, 15 European Review of Contract Law 2019, 365 (371 f., 381 f.); *Morais Carvalho*, EuCML 2019, 194 (197); *Metzger*, JZ 2019, 577 (579, 581, 583); *Bach*, NJW 2019, 1705 (1711); *Spindler/Sein*, MMR 2019, 415 (418); *Spindler/Sein*, MMR 2019, 488 (489, 491 f.); *Schulze*, ZEuP 2019, 695 (719); siehe auch zuvor schon *Metzger et al.*, 9 JIPITEC 2018, 90 Rn. 18 f., 23 f., 50 ff.; *Grundmann/Hacker*, 13 European Review of Contract Law 2017, 255 (290 f.).

[120] Zum Kohärenzbegriff als Ideal jeglichen Rechtssystems siehe *MacCormick*, Legal

dadurch, dass der Wert der tradierten Kollisionsnormen[121] der *lex specialis*[122] und der *lex posterior*[123] im rechtsbereichsübergreifenden Bereich stark eingeschränkt ist.[124]

Gerade bei rechtsbereichsübergreifenden Normenkollisionen muss daher die Lösung, wenn die Regelungen auf derselben normenhierarchischen Ebene liegen oder der Anwendungsvorrang aus anderen Gründen nicht greift, in Wertungskriterien gesucht werden, welche die spezifischen, durch die jeweiligen Normen adressierten Risiken berücksichtigen und diese zu einem integrierten Regelungsgeflecht verbinden.[125] So stellte schon *Engisch* in seiner grundlegenden Schrift zur „Einheit der Rechtsordnung" fest: Wenn die tradierten Kollisionsnormen versagen, „muß der Jurist die Bedeutung der widersprechenden Normen gegeneinander abwägen und der einen den Vorzug vor der anderen geben".[126]

Mit Blick auf das Datenschutzrechtprivatrecht und das hier in Rede stehende Verhältnis von DS-GVO und allgemeinem Privatrecht stellt sich diese Frage mit besonderer Dringlichkeit für Normen oder Normgebiete, die jeweils unionsrechtlich (und nicht rein national) determiniert sind. In normativer Hinsicht leitet das in Art. 7 AEUV positivrechtlich verankerte Kohärenzprinzip zusätzlich dazu an, einen Ausgleich zwischen unterschiedlichen unionalen Rechtsbereichen zu suchen.[127] Der EuGH betont denn auch, dass die Auslegung des Unionsrechts gerade rechtsaktsübergreifend dessen innere Kohärenz gewähr-

Reasoning and Legal Theory, 1994, 152–194; zu Kohärenz im Technologierecht spezifisch *Guihot* 11, Law, Innovation and Technology 2019, 311.

[121] *Engisch*, Die Einheit der Rechtsordnung, 1935, 47; *Conway*, The Limits of Legal Reasoning and the European Court of Justice, 2012, 148, 153 ff.; *Prütting*, RW 9 (2018), 289 (299); *Prütting*, Rechtsgebietsübergreifende Normenkollisionen, 2020, 109 ff.

[122] Zur *lex specialis* im nationalen Recht repräsentativ *Bydlinski*, Juristische Methodenlehre und Rechtsbegriff, 1991, 465 ff.; im Unionsrecht EuGH, Urt. v. 13.12.2001 – Rs. C-481/99 (*Heininger*) – Rn. 37; *Bengoetxea*, The legal reasoning of the European Court of Justice, 1993, 246; siehe auch *Conway*, The Limits of Legal Reasoning and the European Court of Justice, 2012, 153.

[123] Dazu etwa *Bydlinski*, Juristische Methodenlehre und Rechtsbegriff, 1991, 572 (materielle Derogation).

[124] Ähnlich, wenngleich nicht auf den rechtsbereichsübergreifenden Fall beschränkt, *Engisch*, Die Einheit der Rechtsordnung, 1935, 47, 49; ferner *Prütting*, Rechtsgebietsübergreifende Normenkollisionen, 2020, 109 ff., besonders 114 f., 129; zur Unergiebigkeit der *lex specialis* auch *Conway*, The Limits of Legal Reasoning and the European Court of Justice, 2012, 153; vgl. auch *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, 1995, 89; *R. Dietz*, Anspruchskonkurrenz bei Vertragsverletzung und Delikt, 1934, 42, 55 f., besonders auch 60–66: Subsidiarität infolge erschöpfender Regelung; zur Unergiebigkeit der *lex superior Bydlinski*, Juristische Methodenlehre und Rechtsbegriff, 1991, 572 f.

[125] Vgl. *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, 1995, 232.

[126] *Engisch*, Die Einheit der Rechtsordnung, 1935, 50.

[127] Das unionsrechtliche Kohärenzprinzip impliziert etwa, dass Zielkonflikte zwischen einzelnen Politiken – Sachbereichen – des Unionsrechts harmonisch aufgelöst werden müssen, siehe *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 7 Rn. 3 und 9; ferner *Schorkopf*, in: Grabitz/Hilf/Nettesheim, Das Recht der Europäischen Union, 65. EL August 2018, AEUV, Art. 7 Rn. 16 f.; zum rechtstheoretischen Kohärenzbegriff *Bertea*, 11 European Law Journal 2005, 154 (156–160).

leisten muss.[128] Zugleich hält er jedoch fest, dass auch das Kohärenzprinzip nicht die Systematik und Zielsetzungen des jeweiligen Rechtsbereichs zu überspielen vermag.[129]

Daher kann in einem ersten Schritt danach gefragt werden, inwieweit eine rechtsbereichsübergreifende Auslegung von einzelnen Bestimmungen des Unionsrechts stattfinden kann (1.). Hierzu gibt es in der Tat bereits erste Anhaltspunkte in der Rechtsprechung des EuGH. In einem zweiten Schritt ist bei durch Auslegung nicht auszuräumenden Konkurrenzen von Rechtsfolgebestimmungen dann zu eruieren, ob ein Wertungsvorrang einer Regelung auszumachen ist oder ob nach dem Kumulationsprinzip beide zur Anwendung kommen (2.).

1. Rechtsbereichsübergreifende Auslegung

Im Rahmen der systematischen Auslegung hat der EuGH bereits an einigen Stellen eine *rechtsaktübergreifende* Auslegung des Unionsrechts vorgenommen.[130] Wie jedoch die Generalanwältin *Trstenjak* konzise feststellte, besteht darüber hinaus das Bedürfnis, die verschiedenen Rechtsbereiche des Verbraucherrechts „in gesamtsystematische[r] Betrachtung" so auszulegen, dass die verschiedenen Rechtsakte einander sinnvoll ergänzen.[131] In den Rechtssachen *Pereničová und Perenič*[132] sowie *Bankia*[133] hatte der EuGH nun Gelegenheit, für zwei im Datenprivatrecht zentrale Richtlinien die Reichweite einer *rechtsbereichsübergreifenden* Auslegung zu klären.[134]

Zu dieser Auslegungsfigur gab es zuvor lediglich vereinzelte Ansatzpunkte:[135] Im Fall *Oy Liikenne* etwa bemühte sich der EuGH sicherzustellen, dass die Anwendung der alten Betriebsübergangsrichtlinie 77/187/EWG[136] nicht

---

[128] EuGH, Urt. v. 18.12.2008 – Rs. C-306/07 (*Andersen*) – Rn. 44; Urt. v. 5.12.2013 – Rs. C-508/12 (*Vapenik*) – Rn. 25; Urt. v. 2.5.2019 – Rs. C-694/17 (*Pillar Securitisation*) – Rn. 34.

[129] EuGH, Urt. v. 2.5.2019 – Rs. C-694/17 (*Pillar Securitisation*) – Rn. 35; Urt. v. 16.1.2014 – Rs. C-45/13 (*Kainz*) – Rn. 20.

[130] EuGH, Urt. v. 25.10.2005 – Rs. C-350/03 (*Schulte*) – Rn. 76; Urt. v. 13.12.2001 – Rs. C-481/99 (*Heininger*) – Rn. 37–39; Urt. v. 5.7.2012 – Rs. C-49/11 (*Content Services*) – Rn. 44; Urt. v. 18.12.2008 – Rs. C-306/07 (*Andersen*) – Rn. 40–44; EuGH, Urt. v. 2.5.2019 – Rs. C-694/17 (*Pillar Securitisation*) – Rn. 33–46; *Riesenhuber*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 199 (209 Rn. 24); *Rebhahn*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 395 (406 Rn. 30).

[131] GA *Trstenjak*, Schlussanträge v. 29.11.2011 – Rs. C-453/10 (*Pereničová und Perenič*) – Rn. 88.

[132] EuGH, Urt. v. 15.3.2012 – Rs. C-453/10 (*Pereničová und Perenič*).

[133] EuGH, Urt. v. 19.9.2018 – Rs. C-109/17 (*Bankia*).

[134] Dies gilt unter der Prämisse, für die viel spricht, dass man das Lauterkeitsrecht einerseits und das Schuldvertragsrecht andererseits als zwei unterschiedliche Rechtsbereiche und nicht lediglich Teil eines einheitlichen Verbraucherrechts ansieht.

[135] Siehe *Rebhahn*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 395 (406 Rn. 31).

[136] Richtlinie 77/187/EWG des Rates vom 14. Februar 1977 zur Angleichung der Rechts-

die Ziele des Vergaberechts infrage stellte.[137] Bereits diese Entscheidung zeigt, dass eine rechtsgebietsübergreifende Koordination nur als wertungsorientierte, an der Teleologie der jeweiligen Rechtsgebiete ausgerichtete geleistet werden kann – ein Umstand, den der EuGH nunmehr in der Rechtssache *Pillar Securitisation* nochmals betont.[138]

a) Die Fälle *Pereničová und Perenič* sowie *Bankia*

Doch zunächst zu den beiden eingangs genannten Rechtssachen: Im Fall *Pereničová und Perenič*[139] stand erstmals das Verhältnis der UGP-Richtlinie zur Klauselrichtlinie in Rede. Konkret erhob sich die Frage, inwiefern die Qualifikation einer Geschäftspraxis als unlauter Folgen zeitigt für die Bewertung der Missbräuchlichkeit einer Klausel, die just diese Geschäftspraxis zum Inhalt hat oder auf ihr beruht.[140] Der Sachverhalt betraf die irreführende Angabe des effektiven Jahreszinssatzes in einer Vertragsklausel. Dieselbe methodische Frage zum Verhältnis von UGP-Richtlinie und Klauselrichtlinie wurde nochmals und umfassender im Fall *Bankia* gewürdigt, in dem es um die Herabsetzung des Schätzwerts einer Immobilie durch eine Vertragsklausel ging.[141] Der EuGH erinnerte zunächst daran, dass nach Art. 3 Abs. 2 UGP-Richtlinie das Vertragsrecht von der Richtlinie unberührt bleibt und somit die zivilrechtlichen Folgen einer unlauteren Geschäftspraxis nicht in der UGP-Richtlinie selbst geregelt sind.[142] Wenn demnach das Unionsrecht nicht die Unwirksamkeit einer Klausel einfordert, die eine unlautere Geschäftspraxis beinhaltet oder auf ihr basiert,[143] so stellt die Nichtberücksichtigung der Unlauterkeit im Vollstreckungsverfahren auch die Wirksamkeit der UGP-Richtlinie nicht infrage.[144] Insofern wich der EuGH von seiner Rechtsprechung zur Klauselrichtlinie ab, nach der die Unangemessenheit der Klausel im Vollstreckungsverfahren gerade von Amts wegen geprüft werden muss.[145]

---

vorschriften der Mitgliedstaaten über die Wahrung von Ansprüchen der Arbeitnehmer beim Übergang von Unternehmen, Betrieben oder Betriebsteilen, ABl. 1997 L 61/26.

[137] EuGH, Urt. v. 25.1.2001 – Rs. C-172/99 (*Oy Liikenne*) – Rn. 22–25.

[138] EuGH, Urt. v. 2.5.2019 – Rs. C-694/17 (*Pillar Securitisation*) – Rn. 36; siehe auch schon Urt. v. 16.1.2014 – Rs. C-45/13 (*Kainz*) – Rn. 20.

[139] EuGH, Urt. v. 15.3.2012 – Rs. C-453/10 (*Pereničová und Perenič*).

[140] Zur Frage der Eröffnung des Anwendungsbereichs der §§ 305 ff. BGB hinsichtlich einer Geschäfts*praxis* siehe *Micklitz*, in: van Boom/Garde/Orkun (Hrsg.), The European Unfair Commercial Practices Directive, 2014, 173 (185).

[141] EuGH, Urt. v. 19.9.2018 – Rs. C-109/17 (*Bankia*).

[142] EuGH, Urt. v. 19.9.2018 – Rs. C-109/17 (*Bankia*), Rn. 41–43; siehe auch EuGH, Urt. v. 15.3.2012 – Rs. C-453/10 (*Pereničová und Perenič*) – Rn. 43.

[143] EuGH, Urt. v. 19.9.2018 – Rs. C-109/17 (*Bankia*) – Rn. 33.

[144] EuGH, Urt. v. 19.9.2018 – Rs. C-109/17 (*Bankia*) – Rn. 34.

[145] EuGH, Urt. v. 14.6.2012 – Rs. C-618/10 (*Banco Español de Crédito*) – Rn. 42; Urt. v. 14.3.2013 – Rs. C-415/11 (*Aziz*) – Rn. 64.

Genau dieses Erfordernis kann nun aber zu einer indirekten Relevanz der Unlauterkeit der Geschäftspraxis für das Vollstreckungsverfahren führen, wenn die Unlauterkeit die Missbräuchlichkeit einer auf der Unlauterkeit basierenden Vertragsklausel im Sinne der Klauselrichtlinie nahelegt. Zu diesem Verbindungselement zwischen den beiden Rechtsgebieten bezog der EuGH in den genannten Urteilen Stellung. Er judizierte in *Bankia*: „Zwar ist […] die Feststellung des unlauteren Charakters einer Geschäftspraxis nicht automatisch und für sich allein dazu geeignet, den missbräuchlichen Charakter einer Vertragsklausel zu begründen, jedoch stellt sie einen Anhaltspunkt unter mehreren dar, auf den das zuständige Gericht seine Beurteilung des missbräuchlichen Charakters der Klauseln eines Vertrags stützen kann, wobei diese Beurteilung gemäß Art. 4 Abs. 1 der Richtlinie 93/13 unter Berücksichtigung aller Umstände des konkreten Falls vorzunehmen ist".[146]

Daher impliziert die Qualifikation einer Geschäftspraxis als unlauter zwar nicht unmittelbar die Missbräuchlichkeit einer auf dieser Geschäftspraxis beruhenden Vertragsklausel, dieser Umstand muss jedoch bei der Bewertung der Missbräuchlichkeit einer Klausel als ein Element der Abwägung berücksichtigt werden.

b) Die Ausstrahlungswirkung im Unionsrecht

In *Pereničová und Perenič* sowie *Bankia* erfolgt mithin eine Anbindung des Begriffs der Missbräuchlichkeit an jenen der Unlauterkeit, ohne dass es (trotz der morphologischen Identität der jeweiligen englischen Begriffe: *unfair*) zu einer semantischen Gleichsetzung beider käme. Dass es überhaupt zu einer Ausstrahlung des Begriffs eines Rechtsgebiets auf ein anderes kommt, überrascht nicht, da der EuGH auch sonst betont, dass „jede Vorschrift des [Unions]rechts in ihrem Zusammenhang zu sehen und im Lichte des gesamten [Unions]rechts, seiner Ziele und seines Entwicklungsstands zur Zeit der Anwendung der betreffenden Vorschrift auszulegen ist."[147] Bereits früh urteilte der EuGH zudem zur Auslegung des EWG-Vertrags, dass „auf das System und auf die materiellen Vorschriften des Vertrages zurückgegriffen werden",[148] mithin in systematischer Perspektive das gesamte (in diesem Fall Primär-)Recht in den Blick genommen werden muss.

---

[146] EuGH, Urt. v. 19.9.2018 – Rs. C-109/17 (*Bankia*) – Rn. 49; siehe zuvor bereits EuGH, Urt. v. 15.3.2012 – Rs. C-453/10 (*Pereničová und Perenič*) – Rn. 43 f.

[147] EuGH, Urt. v. 6.10.1982 – Rs. 283/81 (*C.I.L.F.I.T*) – Rn. 20; weiteres Beispiel für eine umfassende Auslegung in EuGH, Urt. v. 4.12.1997 – Rs. C-97/96 (*Daihatsu*) – Rn. 18 f.; rechtsaktsübergreifend (die Haustürwiderrufsrichtlinie und Teilzeitnutzungsrechterichtlinie betreffend) EuGH, Urt. v. 22.4.1999 – Rs. C-423/97 (*Travel Vac*) – Rn. 20–23; siehe auch *Riesenhuber*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 199 (209 Rn. 25); *Conway*, The Limits of Legal Reasoning and the European Court of Justice, 2012, 24 f., 147 f.; siehe auch *Bengoetxea*, The legal reasoning of the European Court of Justice, 1993, 240–251.

[148] EuGH, Urt. v. 31.3.1971 – Rs. 22/70 (*Kommission/Rat*) – Rn. 15/19.

Während rechtsgebietsimmanent jedoch morphologisch identische Begriffe vom EuGH tendenziell auch semantisch identisch ausgelegt werden,[149] überzeugt auch die vom EuGH vorgenommene beschränkte, nicht vollständig den Begriff des anderen Rechtsgebiets determinierende Einflussnahme über Rechtsgebietsgrenzen hinweg:[150] Sie erlaubt es, die jeweiligen Spezifika des entsprechenden Rechtsgebiets zu berücksichtigen, zugleich aber die maßgeblichen Wertungsgesichtspunkte des anderen Rechtsgebiets mit in die Abwägung einzuführen. Die rechtsbereichsübergreifende Auslegung stellt daher einen Spezialfall der systematischen Auslegung dar,[151] die jedoch durch eigenständige teleologische Erwägungen des auszulegenden Normenbereichs ergänzt werden kann.[152] Eine derartige Koordination von Vorschriften im Wege einer nicht deterministischen Ausstrahlung befördert daher einen sachgerechten Ausgleich zwischen den Wertungskriterien verschiedener Sachbereiche.

Jedenfalls für die englischen Textfassungen legte in den Fällen *Pereničová und Perenič* sowie *Bankia* bereits die begriffliche Ebene, auf der jeweils der Begriff der „unfairness" (*unfair commercial practice*; *unfair contract term*) Verwendung findet, eine rechtsbereichsübergreifende Auslegungspraxis nahe. Auch der 15. Erwägungsgrund der Klauselrichtlinie deutet in diese Richtung, nach dem für die Beurteilung der Missbräuchlichkeit unter anderem zu berücksichtigen ist, „ob auf den Verbraucher in irgendeiner Weise eingewirkt wurde." Dies umfasst gerade auch unlautere Einwirkungen.[153] Der EuGH weist jedoch zu Recht darauf hin, dass für die Feststellung der Missbräuchlichkeit nach Art. 4 Abs. 1 der Klauselrichtlinie alle Umstände des konkreten Falles relevant sind;[154] damit kann sich diese nicht in dem Verweis auf die Unlauterkeit der Klausel erschöpfen, da nicht sichergestellt ist, dass im Rahmen dieser Prüfung bereits alle für die Klauselrichtlinie maßgeblichen Aspekte berücksichtigt wurden.[155] Es kommt daher zu Recht nicht zu einem automatischen Durchgriff des Lauterkeitsrechts auf das AGB-Recht.[156] In ähnlicher Weise hält der EuGH auch für den Verbraucherbegriff fest, dass rechtsgebietsfremde Definitionen berücksichtigt werden müssen, aber nicht determinierend wirken.[157] Diese indizierende, aber nicht determinierende Ausstrahlung wird auch

---

[149] EuGH, Urt. v. 5.7.2012 – Rs. C-49/11 (*Content Services*) – Rn. 44; Urt. v. 2.5.2019 – Rs. C-694/17 (*Pillar Securitisation*) – Rn. 27.

[150] Zustimmend auch *Keirsbilck*, 50 Common Market Law Review 2013, 247 (258).

[151] *Riesenhuber*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 199 (208 Rn. 22).

[152] Siehe nochmals EuGH, Urt. v. 2.5.2019 – Rs. C-694/17 (*Pillar Securitisation*) – Rn. 36 f.

[153] Wie hier *Keirsbilck*, 50 Common Market Law Review 2013, 247 (258 Fn. 47).

[154] EuGH, Urt. v. 15.3.2012 – Rs. C-453/10 (*Pereničová und Perenič*) – Rn. 44.

[155] *Alexander*, WRP 2012, 515 (519); *Stempel*, Treu und Glauben im Unionsprivatrecht, 2016, 108.

[156] *Nassall*, LMK 2012, 333461; in diese Richtung aber *Micklitz/Reich*, EuZW 2012, 126 (127).

[157] EuGH, Urt. v. 2.5.2019 – Rs. C-694/17 (*Pillar Securitisation*) – Rn. 34; Urt. v.

für das Verhältnis zwischen datenschutzrechtlichem Fairnessgebot und AGB-Recht entscheidend sein.[158]

2. Konkurrierende Rechtsfolgebestimmungen

Wenn im Wege der Auslegung nicht verhindert werden kann, dass zwei Rechtsbereiche auf europäischer Ebene Normen mit abweichenden Rechtsfolgen hinsichtlich eines (partiell) identischen Sachverhalts beinhalten, erhebt sich die Frage, ob einer der Rechtsbereiche einen Wertungsvorrang beanspruchen oder ob, sofern sich die Rechtsfolgen nicht gänzlich ausschließen, das Kumulationsprinzip obwalten kann. Beispielsweise ist zu klären, ob eine Einwilligung, die alle Voraussetzungen der DS-GVO erfüllt, dennoch unangemessen im Sinne der Klauselrichtlinie und daher unwirksam sein kann.[159]

a) Kein grundsätzlicher Vorrang des Datenschutzrechts

Schon im Ansatz verfehlt ist es, mit einer bisweilen in der Literatur anzutreffenden Position[160] einen grundsätzlichen, hierarchischen Vorrang des Datenschutzgrundrechts gegenüber anderen Rechtspositionen anzunehmen. Wollte man dies auf die sekundärrechtliche Ebene übertragen, so würde daraus ein Generalvorrang der DS-GVO gegenüber Wertungen anderer Rechtsbereiche folgen.[161]

Dies kann jedoch nicht überzeugen. Ausgangspunkt der Diskussion ist die Feststellung des EuGH in der Rechtssache *Google Spain*, wonach die Grundrechte aus Art. 7 und 8 GRCh „grundsätzlich nicht nur gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers, sondern auch gegenüber dem Interesse der breiten Öffentlichkeit daran, die Information bei einer anhand des Namens der betroffenen Person durchgeführten Suche zu finden, überwiegen".[162] Die Passage muss jedoch im Kontext des gesamten Urteils betrachtet werden. So verweist der EuGH zur Begründung seiner Vorrangerwägung auf eine andere Stelle desselben Urteils, in der festgestellt wird, dass die spezifische Veröffentlichung von Informationen im Internet, die durch eine Suchmaschine verknüpft werden können, eine besondere Schwere des Eingriffs in die genannten Grundrechte aus Art. 7 und 8 GRCh indiziert.[163] Nur diese besondere Schwere lässt daher die anderen genannten Interessen und

25.1.2018 – Rs. C-498/16 (*Schrems II*) – Rn. 28; Urt. v. 5.12.2013 – Rs. C-508/12 (*Vapenik*) – Rn. 25.

[158] Siehe unten, § 5 C.II.1.g)bb).

[159] Dazu ausführlich unten, § 5 C.II.1.

[160] *Brkan*, 23 Maastricht Journal of European and Comparative Law 2016, 812 (825) (als deskriptives Faktum); dies ebenfalls erwägend *Svantesson*, 34 Computer Law and Security Review 2018, 25 (31).

[161] So aber wohl *Svantesson*, 34 Computer Law and Security Review 2018, 25 (31).

[162] EuGH, Urt. v. 13.5.2014 – Rs. C-131/12 (*Google Spain*) – Rn. 97.

[163] Urt. v. 13.5.2014 – Rs. C-131/12 (*Google Spain*) – Rn. 80 f.

Grundrechte zurücktreten, nicht etwa eine dem Unionsrecht immanente überproportionale Gewichtung von Privatsphäre und Datenschutz. Daher stellt sich der vom EuGH scheinbar proklamierte Vorrang des Rechts auf Achtung des Privatlebens und des Datenschutzgrundrechts nicht als ein allgemeiner dar, sondern lediglich als ein durch die spezifische Konstellation des Sachverhalts und der im Urteil vorgenommenen Abwägung motivierter und gerechtfertigter.

b) Grundrechtlich geprägte Normenkoordination

Dies verweist auf einen allgemeinen Aspekt: Praktisch alle Art. 7 und 8 GRCh entgegenstehenden „Interessen" sind zugleich als Grundrechte primärrechtlich verankert. Es überrascht, dass der EuGH dies in der Entscheidung *Google Spain* nicht ausdrücklich formuliert, auch die entsprechenden Chartagrundrechte nicht zitiert. Dabei ist unstreitig, dass das Recht auf Informationsfreiheit in Art. 11 GRCh und die unternehmerische Betätigung in Art. 15 f. GRCh verbürgt sind. Auch andere, für das Datenprivatrecht relevante Rechtspositionen sind primärrechtlich radiziert: das Diskriminierungsverbot in Art. 21, der Verbraucherschutz immerhin als Grundsatz in Art. 38 GRCh.[164]

Zwischen grundsätzlich gleichrangigen Unionsgrundrechten muss im Kollisionsfall ein schonender Ausgleich im Einzelfall gefunden werden;[165] Grundsätze können nach Art. 52 Abs. 5 GRCh immerhin bei der Auslegung der sie näher konkretisierenden Bestimmungen berücksichtigt werden.[166] Auch aus primärrechtlicher Warte wäre es daher nachgerade abwegig, einen generellen Vorrang des Datenschutzgrundrechts vor anderen Grundrechten anzunehmen.[167] Vielmehr kann ein solcher Vorrang immer nur auf Grundlage einer spezifischen Abwägung für bestimmte Einzelfälle entwickelt werden.[168] Anhaltspunkte hierfür können sich entweder explizit im Gesetz, besonders in Akten des Sekundärrechts für auf dieser Ebene verortete Koordinationsbedürfnisse, oder aber implizit in den dahinterstehenden Wertungen finden.

---

[164] Zum Charakter von Art. 38 als Grundsatz, nicht Individualgrundrecht, siehe nur *Rudolf*, in: Meyer, Charta der Grundrechte der Europäischen Union, Art. 38 Rn. 4 f.; *Jarass*, in: Jarass, Charta der Grundrechte der EU, 3. Aufl. 2016, Art. 38 Rn. 3.

[165] Siehe nur EuGH, Urt. v. 7.3.2014 – Rs. C-314/12 (*UPC Telekabel*) – Rn. 63; ebenso Urt. v. 31.1.2013 – Rs. C-12/11 (*McDonagh*) – Rn. 62; Urt. v. 22.1.2013 – Rs. C-283/11 (*Sky Österreich*) – Rn. 58, 60; Urt. v. 6.9.2012 – Rs. C-544/10 (*Deutsches Weintor*) – Rn. 47; Urt. v. 29.1.2008 – Rs. C-275/06 (*Promusicae*) – Rn. 65 f.; BVerfG GRUR 2020, 88 Rn. 96 – Recht auf Vergessen II; *Borowsky*, in: Meyer, Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, Art. 52 Rn. 14–16; *Schwerdtfeger*, in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Aufl. 2019, Art. 52 Rn. 36; siehe auch bereits § 5, Fn. 91.

[166] Siehe etwa GA *Wahl*, Schlussanträge v. 12.12.2013 – Rs. C-470/12 (*Pohotovosť*) – Rn. 66.

[167] Siehe auch BVerfG GRUR 2020, 88 Rn. 120–122 – Recht auf Vergessen II.

[168] Ähnlich im Ergebnis auch, als normatives Desiderat, *Brkan*, 23 Maastricht Journal of European and Comparative Law 2016, 812 (827).

aa) Explizite Regelung eines Wertungsvorrangs

Jedenfalls im Grundsatz stellt sich das Verhältnis im Konfliktfall klar dar, wenn ein Wertungsvorrang eines Rechtsgebiets explizit geregelt ist. So bestimmt etwa Art. 2 Abs. 4 DS-GVO, dass die Regelungen der E-Commerce-Richtlinie (ECRL) unberührt bleiben und daher im Zweifel vorgehen. In ähnlicher Weise ordnet Art. 3 Abs. 7 der DIDD-Richtlinie an: „Kollidiert eine Bestimmung dieser Richtlinie mit einer Bestimmung eines anderen Unionsrechtsakts, der einen bestimmten Sektor oder Gegenstand regelt, so hat die Bestimmung dieses anderen Unionsrechtsakts Vorrang vor dieser Richtlinie." Den Vorrang des unionalen Datenschutzrechts etabliert insoweit Art. 3 Abs. 8 UAbs. 2 der DIDD-Richtlinie nochmals ausdrücklich.

bb) Impliziter Wertungsvorrang: Risikospezifizität zum Dritten

In den meisten hier interessierenden Fällen fehlen jedoch explizite Vorrangregelungen. Man wird aber, wie beim Anwendungsvorrang,[169] sagen können, dass einer Norm oder einem Rechtsgebiet nur dann ein impliziter Wertungsvorrang zukommt, wenn ein spezifisches Risiko gerade *ausschließlich* dieser Norm oder diesem Rechtsgebiet zugeordnet ist.[170] Diese Frage ist letztlich nicht zu beantworten ohne Rekurs auf den Sinn und Zweck einer Regelung im Gefüge des jeweiligen Teilrechtsgebiets,[171] was sowohl das Bundesverfassungsgericht[172] als auch der EuGH betonen.[173] Unterschiedliche Zielsetzungen können demnach abweichende Rechtsfolgen rechtfertigen. Dies impliziert wie bei allen die Teleologie betreffenden interpretatorischen Fragen ein besonderes Maß an Vagheit, aber auch Flexibilität.

(1) Abschließende Adressierung eines Risikos im Datenschutzrecht

In den hier interessierenden Konstellationen ist daher insbesondere von Belang, inwiefern ein Risiko im Rahmen des Datenschutzrechts so spezifisch geregelt ist, dass die Regelung als ausschließlich anzusehen ist, mithin keine andere Beurteilung durch andere unionsrechtliche oder Unionsrecht umsetzende nationale Vorschriften mehr möglich ist. Letztlich kommt dies wiederum nur dann in Betracht, wenn die Auslegung der datenschutzrechtlichen Vorschrift ergibt, dass diese alle Eventualitäten berücksichtigen und ihrer gerade systemimma-

[169] Siehe oben, § 5 A.I.1.b) und § 5 A.I.2.b)aa)(1).

[170] Grundlegend *R. Dietz*, Anspruchskonkurrenz bei Vertragsverletzung und Delikt, 1934, 60–66: Subsidiarität infolge erschöpfender Regelung; ferner *Larenz/Canaris*, Methodenlehre der Rechtswissenschaft, 1995, 89, 91.; für das Verhältnis von Datenschutzrecht und Verbraucherrecht *Svantesson*, 34 Computer Law and Security Review 2018, 25 (32).

[171] Zum Begriff des Teilrechtsgebiets ausführlich *Prütting*, Rechtsgebietsübergreifende Normenkollisionen, 2020, 15 ff.

[172] Vgl. insoweit BVerfG GRUR 2020, 88 Rn. 79 – Recht auf Vergessen II, allerdings zum Verhältnis von nationalem und unionalem Recht.

[173] Siehe EuGH, Urt. v. 2.5.2019 – Rs. C-694/17 (*Pillar Securitisation*) – Rn. 36 f.

nent „Herr werden“[174] wollte. Hier bestehen manifeste Parallelen zur Feststellung des abschließenden Charakters einer unionsrechtlichen Bestimmung im Rahmen der Voraussetzungen einer direkten Kollision beim Anwendungsvorrang.[175]

(2) Adressierung eines zusätzlichen Risikos in anderen Rechtsbereichen

Eine gegenüber dem Datenschutzrecht abweichende Wertung durch Regelungen anderer unionaler Rechtsgebiete ist hingegen möglich, wenn sich dort eigene Bewertungsmaßstäbe finden, die Risiken abdecken, die im Datenschutzrecht überhaupt nicht oder jedenfalls nicht spezifisch adressiert werden, so dass von einer abschließenden Regelung durch das Datenschutzrecht nicht ausgegangen werden kann. Die Nutzung einer anderen *Begrifflichkeit* (z. B. Missbräuchlichkeit statt Treu und Glauben oder Transparenz statt Informiertheit) reicht jedoch für sich genommen nicht aus, um eine Abweichungsmöglichkeit von den Wertungen des Datenschutzrechts zu begründen (so wie umgekehrt eine begriffliche nicht notwendig zu einer sachlichen Identität führt[176]). Vielmehr müssen besondere *sachliche* Umstände hinzutreten, die im Datenschutzrecht nicht oder nicht abschließend berücksichtigt werden. In jedem Falle müssen die Wertungen des Datenschutzrechts jedoch, schon um das unionsrechtliche Kohärenzprinzip zu wahren,[177] zumindest berücksichtigt werden. So können sich die jeweiligen Rechtsgebiete gegenseitig ergänzen, was letztlich auch dem Geist der EuGH-Entscheidung in den Rechtssachen *Pereničová und Perenič* sowie *Bankia* entspricht.

III. Zusammenfassung zum Verhältnis von Datenschutzrecht und Privatrecht

Der Anwendungsvorrang beruht auf dem Gedanken, die einheitliche Wirkung des Unionsrechts und die Verwirklichung seiner Ziele unter den Bedingungen des grundsätzlichen Fortbestehens nationaler Rechtsordnungen zu sichern. Koordinationsnotwendigkeiten außerhalb des Anwendungsvorrangs können im Wege der Sachintegration rechtsgebietsübergreifend durch eine wertungsorientierte Normenkoordination bewältigt werden, bei der insbesondere die Kohärenz der auf einer Ebene befindlichen Regelungen als systematische Stimmigkeit und teleologischer Ausgleich gewährleistet werden muss.

Trotz der unterschiedlichen dogmatischen Begründungen und Funktionsweisen von Anwendungsvorrang einerseits und Sachintegration andererseits lassen sich übergreifende Kriterien erkennen. So ist jeweils entscheidend, ob

[174] Formulierung in EuGH, Urt. v. 23.1.1975 – Rs. 31/74 (*Galli*) – Rn. 9/11.
[175] Siehe oben, Text bei § 5, Fn. 39.
[176] Siehe oben, Text bei § 5, Fn. 150.
[177] Dazu bereits oben, Text bei § 5, Fn. 120.

auf unionsrechtlicher Ebene (Anwendungsvorrang) oder im Rahmen eines speziellen Rechtsgebiets (Sachintegration) ein bestimmtes Risiko eine abschließende Regelung dergestalt erfahren hat, dass alle Eventualitäten berücksichtigt werden sollten. Dies ist letztlich eine Frage der Auslegung. Adressiert demgegenüber eine Regelung auf nationaler Ebene (Anwendungsvorrang) oder in einem anderen Rechtsgebiet (Sachintegration) zusätzliche Risiken oder Umstände in spezifischer Weise, so hat diese Regelung grundsätzlich Bestand. Im Rahmen des Anwendungsvorrangs müssen die Regelungsziele jedoch zusätzlich auch als unionsrechtliche rekonstruierbar sein (zweistufige Prüfung), was typischerweise die Binnenmarktkompatibilität der Zielsetzung erfordert.

Dabei lässt sich folgendes Prüfprogramm identifizieren, um zu klären, ob eine Regelung des Datenprivatrechts neben dem unionsrechtlichen Datenschutzrecht bestehen kann. Im Falle einer rein national determinierten Norm muss zunächst ein Anwendungsvorrang des Unionsrechts infolge direkter Kollision ausgeschlossen werden. Dafür muss nicht nur geklärt sein, dass der national geregelte Fall nicht zugleich abweichend positiv im Unionsrecht geregelt ist; es darf zudem keine negative Regelungsanordnung im Unionsrecht bestehen. Ferner muss ein Anwendungsvorrang des Unionsrechts infolge indirekter Kollision untersucht werden. Hier sind der Äquivalenz- und insbesondere der Effektivitätsgrundsatz des Unionsrechts von Belang; letzterer kann mithilfe der zweistufigen Prüfung (Risikospezifizität und Zielkompatibilität) operationalisiert werden. Bei Normen mit normenhierarchischer Provenienz auf derselben Regelungsebene hingegen ist nicht der Anwendungsvorrang, sondern die Sachintegration zu beachten. Auch dort sind jedoch insbesondere die Natur und Spezifizität der adressierten Risiken entscheidend. Letztlich können sich diese Kriterien jedoch immer nur im Einzelfall bewähren; genau dies leisten die folgenden Teile dieser Untersuchung.

B. Ermöglichende Strukturen im allgemeinen Privatrecht

Das allgemeine Privatrecht hält mit der Rechtsgeschäftslehre (§§ 104 ff. BGB) und dem Vertragsrecht (besonders §§ 145 ff., 311 ff. BGB) zentral vom Grundsatz der Ermöglichung privatautonomer Rechtsbeziehungen geprägte Normgruppen bereit,[178] die auch im Kontext der digitalen Austauschprozesse erhebliche Relevanz besitzen. Insofern ist zunächst noch einmal klarzustellen, dass

[178] Siehe nur *Larenz*, Schuldrecht AT I, 14. Aufl. 1987, § 4, 41; *Medicus/Petersen*, BGB AT, 11. Aufl. 2016, Rn. 174 ff.; *Wolf/Neuner*, BGB AT, 11. Aufl. 2016, § 28 Rn. 1; *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, 1971, 412 ff.; *Flume*, AT II, 4. Aufl. 1992, 7 f.; *Emmerich*, in: MüKo, BGB, 8. Aufl. 2019, § 311 Rn. 1 f.; *Di Fabio*, in: Maunz/Dürig, GG, 86. EL Januar 2019, Art. 2 Rn. 101; vgl. auch *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 61 f.; *Sattler*, JZ 2017, 1036 (1038).

sowohl die Einwilligung als auch die Überlassung personenbezogener Daten nach deutschem Schuldrecht als Gegenleistung vereinbart werden können (I.). Wie der Verfasser an anderer Stelle genauer ausgearbeitet hat,[179] kann die Verknüpfung von Leistung und Gegenleistung dabei konditionaler oder aber, sofern dies explizit vereinbart wird oder die Interessen der Parteien dies bei Auslegung nach §§ 133, 157 BGB gebieten, synallagmatischer Natur sein.

Die autonomiefreundlichen Tatbestände des BGB lassen allerdings nicht nur einseitige Willenserklärungen und bilaterale Vertragsverbindungen zu, sondern ermöglichen auf verschiedene Arten auch die Einbindung weiterer Vertragsparteien und Dritter. Jedoch sind Rechtsgeschäftslehre und Vertragsrecht seit jeher nicht ausschließlich vom Grundsatz der Privatautonomie durchdrungen, sondern auch von Verkehrsschutzbelangen geprägt.[180] Dies hat insbesondere die Rechtsprechung des BGH, etwa im Bereich der Erklärungsfahrlässigkeit, immer wieder deutlich gemacht.[181] So lassen sich eine Reihe der zentralen Streitfragen der Rechtsgeschäftslehre auf den Widerstreit von (negativer) Privatautonomie einerseits und Verkehrsschutz andererseits zuspitzen.[182] Bei datengetriebenen Austauschprozessen tritt zu diesen beiden bestimmenden Grundsätzen nun noch das (mit horizontaler Direktwirkung ausgestattete[183]) unionale Datenschutzgrundrecht hinzu. Es verstärkt tendenziell die Position desjenigen, der über seine Daten privatautonom verfügt. Dies zwingt zu einer Neubewertung einiger klassischer Streitfragen der Rechtsgeschäftslehre und des Vertragsrechts im Kontext digitaler Austauschprozesse.

Zugleich muss geklärt werden, inwieweit auf die Normen und Konzepte des BGB im Kontext des Datenprivatrechts im Lichte der soeben erörterten Verhältnisbestimmung von unionalem und mitgliedstaatlichem Recht überhaupt zurückgegriffen werden kann. Für die Erlaubniswirkung der Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO und jene des Vertrags nach Art. 6 Abs. 1 lit. b DS-GVO ist jeweils entscheidend, dass der Tatbestand der Einwilligung bzw. des Vertragsschlusses einer allgemeinen Rechtsgeschäftslehre bzw. Vertragslehre entspricht, die entweder aus dem BGB oder dem Unionsrecht, speziell der DS-GVO, entwickelt werden muss. Dem gehen die folgenden Ausführungen für die Einwilligung (II.) und für den Vertrag nach (III.), nachdem die grundsätzliche Tauglichkeit von Einwilligung und Datenüberlassung als Gegenleistung geklärt wurde.

---

[179] Siehe oben, Text und Nachweise in § 4 B.I.3.a)dd)(5)(a)(aa)a; ausführlich *Hacker*, ZfPW 2019, 148 (170 ff.); siehe ferner oben, § 4 B.I.3.b)bb)(3)(b).

[180] *Bydlinski*, Privatautonomie und objektive Grundlagen des verpflichtenden Rechtsgeschäfts, 1967, 123 ff.; *Bydlinski*, JZ 1975, 1 (4 ff.); *von Craushaar*, AcP 174 (1974), 2 (5 ff.); *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 119 Rn. 100; zur Kontroverse eingehend *Singer*, Selbstbestimmung und Verkehrsschutz im Recht der Willenserklärungen, 1995, 97 ff.; ferner die Nachweise unten in § 5, Fn. 270.

[181] Dazu unten, Text bei § 5, Fn. 416 ff.

[182] Vgl. *Ohly*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, 2002, 365.

[183] Dazu ausführlich unten, Text bei § 5, Fn. 1074 ff.

I. Einwilligung und Datenüberlassung als Gegenleistung

Vertragspartner können nach hier vertretener Auffassung ohne Weiteres, freilich zugleich im Rahmen der gesetzlichen Grenzen, eine Verpflichtung zur Überlassung von Daten oder auch zur Abgabe einer Einwilligungserklärung, kumulativ oder alternativ, zum Gegenstand einer Gegenleistungspflicht machen.[184] Zwar ist diese Position nicht unumstritten;[185] für sie sprechen jedoch eine Reihe von Gründen.[186] Diese wurden bereits in § 4,[187] und ausführlich andernorts,[188] ausgeführt, so dass es an dieser Stelle mit einer Erörterung der wesentlichen Argumente sein Bewenden haben kann.

Zunächst ist in Ansehung der Vertragsfreiheit schon grundsätzlich nicht ersichtlich, warum personenbezogene Daten nicht ebenso wie andere werthaltige Objekte den Charakter einer Gegenleistung annehmen können. Dass damit kein rechtlicher Blankoscheck für jegliche Kommerzialisierung von Daten droht,[189] dürfte schon aufgrund der Unabhängigkeit der DS-GVO von der schuldrechtlichen Einordnung offensichtlich sein.[190] Ferner spricht auch die Gleichbehandlung von Zahlungen einerseits mit Geld und andererseits mit Daten dafür, in beiden Fällen eine Gegenleistung annehmen zu können.[191] Da, bei allen Unterschieden zwischen Geld und Daten,[192] deren Überlassung jeweils, wie in § 3 gesehen,[193] eine ökonomisch vergleichbare Funktion übernimmt, sollte auch die rechtliche Behandlung so weit als möglich angenähert werden.

---

184 Zur Pflicht zur Werbeexposition als Gegenleistung siehe oben, § 4 B.I.3.b)bb)(3)(a).

185 *European Data Protection Supervisor*, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 2017, 9 f.; wohl auch *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8.10.2019, Rn. 54; nunmehr auch KG BeckRS 2019, 8570 Rn. 43 (dazu sogleich genauer).

186 Im Ergebnis ebenso *Metzger*, AcP 216 (2016), 817; *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 43; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 200; vgl. auch *Langhanke*, Daten als Leistung, 2018, 99, 110 ff.; *Metzger et al.*, 9 JIPITEC 2018, 90 Rn. 19; *Metzger*, in: Festschrift Basedow, 2018, 131 (133); *Indenhuck/Britz*, BB 2019, 1091 (1095); *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen).

187 Siehe oben, Text und Nachweise in § 4 B.I.2. und § 4 B.I.3.b)bb)(3)(a).

188 *Hacker*, ZfPW 2019, 148 (158 ff.).

189 Siehe aber *European Data Protection Supervisor*, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 2017, 9 f.; wohl auch *European Data Protection Board*, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8.10.2019, Rn. 54.

190 Siehe auch oben, Text bei § 4, Fn. 679.

191 Siehe nur *Metzger*, AcP 216 (2016), 817 (833 f.).

192 Siehe oben, § 3 B.II.1.d); *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (275 f.); Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 569 ff.

193 Siehe oben, insbesondere § 3 B.I.1.c).

In rechtlicher Hinsicht sind freilich, wie in § 4 ausführlich erörtert, die besonderen Voraussetzungen für die rechtmäßige Verarbeitung von Daten ein wesentlicher Unterschied zum klassischen Erhalt von Geld als Gegenleistung. Insbesondere die jederzeitige Widerrufbarkeit der datenschutzrechtlichen Einwilligung stellt insoweit gewissermaßen eine Sollbruchstelle für die Gleichbehandlung von monetären und datenbasierten Austauschverhältnissen dar. So hat das KG,[194] wenngleich in einer äußerst knappen und etwas kryptischen Passage,[195] im Jahr 2019 geurteilt, dass die Überlassung von personenbezogenen Daten insofern nicht den Charakter einer Gegenleistung beanspruchen könne, als die darauf bezogene Einwilligung jederzeit widerrufen werden kann. Zugleich hat das KG jedoch bekräftigt, dass die Einwilligungserklärung selbst eine Gegenleistung darstellen könne, wenn sich die betroffene Person zu ihrer Abgabe schuldrechtlich verpflichtet.[196] Diese Ausführungen stehen allerdings in einem Spannungsverhältnis zu den vom KG nicht diskutierten Erwägungen des BGH, wonach schon grundsätzlich nicht nur die Einwilligung, sondern auch die Überlassung von Daten Gegenleistungscharakter haben kann.[197] Wie bereits bemerkt,[198] hat der EuGH dies noch klarer bejaht.[199]

Man wird der einschränkenden, auf der Widerruflichkeit der Einwilligung gründenden Lesart des KG letztlich nicht beitreten können. Dass eine Gegenleistungs*pflicht* nur besteht, wenn sich eine Vertragspartei dazu wirksam schuldrechtlich verpflichtet hat, ist evident. Das KG scheint in Ansehung von Art. 7 Abs. 3 S. 1 DS-GVO jedoch der Auffassung zu sein, dass eine wirksame schuldrechtliche Verpflichtung zur Überlassung von personenbezogenen Daten und in der Folge auch eine dahingehende Gegenleistung ausscheiden.[200] Dabei übersieht es zunächst, dass eine Gegenleistung auch in einer konditionalen oder kausalen Verknüpfung bestehen kann, bei der jeweils schon von vornherein kein schuldrechtlicher Anspruch auf die Gegenleistung besteht.[201] Die Fokussierung auf die Einwilligung, und deren Widerruflichkeit, übergeht zudem, dass jedenfalls grundsätzlich auch andere Erlaubnistatbestände nach

---

194 KG BeckRS 2019, 8570 Rn. 43.

195 Unklar ist insbesondere, weshalb die Verpflichtung zur Abgabe einer Einwilligungserklärung (nur?) diese in den Rang einer Gegenleistung erheben soll; denn die Widerruflichkeit der Einwilligung bleibt davon nach herrschender Meinung unberührt (siehe oben, § 4 B.I.3.b)bb)(2)). Zudem müsste, wenn die Verpflichtung zur Einwilligung nach dem KG zur Qualifikation als Gegenleistung führt, selbiges für den Fall gelten, dass eine Vertragspartei sich zur Überlassung von Daten schuldrechtlich wirksam verpflichtet.

196 KG BeckRS 2019, 8570 Rn. 43.

197 BGH NJW 2017, 2119 Rn. 22 – Robinson Liste.

198 § 4 B.I.3.b)bb)(3)(a).

199 EuGH, Urt. v. 29.7.2019 – Rs. C-40/17 (*Fashion ID*) – Rn. 80; siehe auch LG Berlin MMR 2018, 328 Rn. 51.

200 KG BeckRS 2019, 8570 Rn. 43: „Eine ‚Leistung', die der Betroffene jederzeit zurückziehen kann, ist aber kein taugliches Entgelt."

201 Siehe nur *Emmerich*, in: MüKo, BGB, 8. Aufl. 2019, Vor § 320 Rn. 7 ff.; mit Bezug auf Daten als Gegenleistung *Hacker*, ZfPW 2019, 148 (167 ff.).

Art. 6 Abs. 1 DS-GVO für eine Verarbeitung in Betracht kommen,[202] sodass der Widerruf der Einwilligung nicht notwendig zur Unrechtmäßigkeit der Verarbeitung führen muss.[203]

Allerdings kann nach hier vertretener Auffassung, (wohl) entgegen dem KG,[204] die Verpflichtung zur Überlassung von personenbezogenen Daten auch dann eine Gegenleistungspflicht konstituieren, wenn ihre Verarbeitung nur auf eine Einwilligung gestützt werden kann. Dies folgt aus drei Unterargumenten. Erstens besitzen die bis zum Widerruf überlassenen Daten unbestreitbar wirtschaftlichen Wert.[205] Zweitens können sie auch rechtmäßig verarbeitet werden, da ein Widerruf nach Art. 7 Abs. 3 S. 2 DS-GVO immer nur ex nunc wirkt. Schließlich wurde drittens bereits oben genauer ausgeführt, dass auch eine genuine Verpflichtung zur Überlassung von Daten, die lediglich auf Basis einer Einwilligung verarbeitet werden können, trotz deren Widerruflichkeit wirksam und durchsetzbar ist, solange die Einwilligung nicht tatsächlich rechtswirksam widerrufen wurde.[206] Dafür spricht, trotz grundsätzlichen Bestehens der *dolo agit*-Einrede, entscheidend, dass andernfalls bei jeglichen Verträgen, bei denen einer Partei ein anlassloses Vertragslösungsrecht zusteht (etwa bei Verbraucherverträgen mit Widerrufsrecht), der Gegenleistungscharakter (und damit die Entgeltlichkeit nach § 312 Abs. 1 BGB) verneint werden müsste.[207] Dies vertritt bislang zu Recht, soweit ersichtlich, niemand; es wäre auch mit der gesetzlichen Systematik der §§ 312 ff. BGB nicht vereinbar.

Zutreffend ist allerdings, dass der Gegenleistungscharakter auch bei der Überlassung von Daten nicht pauschal angenommen werden kann. Dies ist relevant nicht nur für die Frage der Entgeltlichkeit der Transaktion, sondern auch für die Anwendbarkeit einer Reihe von Normen des allgemeinen Schuldrechts (z. B. §§ 320 ff. BGB),[208] besonders für die Frage der Kontrollfähigkeit nach § 307 Abs. 3 S. 1 BGB.[209] Hier muss nach den einzelnen ökonomischen Modellen differenziert werden;[210] gerade beim data on top-Modell kann gegenüber der monetären Gegenleistung die Bedeutung sowohl der Einwilligung als auch der Überlassung von Daten so in den Hintergrund treten, dass darin lediglich eine Nebenleistungspflicht (oder eine Nebenbedingung bei konditionaler Verknüpfung) zu sehen ist.[211] Auch dies wurde an anderer Stelle genauer ausgeführt.[212]

---

[202] § 4 B.I.3.b)bb)(3)(a)(aa)a(a).
[203] Siehe oben, § 4 B.I.3.b)bb)(1).
[204] Siehe oben, § 5, Fn. 195.
[205] Vgl. *Hacker*, ZfPW 2019, 148 (159 ff.).
[206] § 4 B.I.3.b)bb)(3)(a)(aa)a(b).
[207] Dies würde in der Tat aus der oben, § 5, Fn. 200, zitierten Passage des KG-Urteils folgen.
[208] Siehe *Hacker*, ZfPW 2019, 148 (149 f.).
[209] Siehe genauer unten, § 5 C.II.1.e)aa).
[210] *Hacker*, ZfPW 2019, 148 (162 ff., 168 ff.).
[211] Zu allgemeinen Abgrenzungsschwierigkeiten zwischen Haupt- und Nebenleistungs-

II. Privatrechtliche Rechtsgeschäftslehre und datenschutzrechtlicher Einwilligungstatbestand

Kann demnach eine Einwilligung grundsätzlich eine schuldrechtliche Gegenleistung darstellen, so stellt sich umso dringlicher die Frage des Verhältnisses von privatrechtlicher Rechtsgeschäftslehre und datenschutzrechtlichem Einwilligungstatbestand. Die DS-GVO formuliert zwar eine Reihe von Wirksamkeitsvoraussetzungen für die Einwilligung, enthält jedoch, anders als das BGB in den §§ 104 ff., keine vollentwickelte Rechtsgeschäftslehre. So sind gerade die Ausführungen zu in der Person des Betroffenen begründeten Wirksamkeitsvoraussetzungen und Einwendungen in der DS-GVO spärlich, wenn man von der Regelung der Freiwilligkeit (Art. 4 Nr. 11, Art. 7 Abs. 4 DS-GVO) und der Erwähnung der Abgabe der Willenserklärung (Art. 4 Nr. 11 DS-GVO) einmal absieht. Zu sonstigen Willensmängeln (§§ 119 ff. BGB), der Einwilligungsfähigkeit von Geschäftsunfähigen (§§ 104 ff. BGB, mit Ausnahme der Minderjährigen), zu Fragen des Zugangs (§§ 130 ff. BGB) und auch der Stellvertretung (§§ 164 ff. BGB) schweigt die DS-GVO. Ob in dieser Hinsicht ein Rückgriff auf das BGB möglich ist, hängt auch von der Rechtsnatur der Einwilligung ab. Bei der Beantwortung dieser Frage können jedoch begriffliche Erwägungen nicht allein entscheidend sein; es muss vielmehr immer die Wirkung einer Lösung auf nationaler Ebene für den europäischen Harmonisierungsprozess im Bereich der datengetriebenen Austauschprozesse, den die DS-GVO entscheidend vorangebracht hat, mitgedacht werden.

1. Die Rechtsnatur der Einwilligung und der Rückgriff auf nationales Recht

Die Rechtsnatur der datenschutzrechtlichen Einwilligung war bereits unter der Geltung des BDSG aF heftig umstritten.[213] In faktischer Hinsicht ist der Streit zumindest insofern abgemildert, als der wohl häufigste praktische Anwendungsfall nach altem Datenschutzrecht, die Frage der Einwilligungsfähigkeit von Minderjährigen,[214] nunmehr explizit in Art. 8 DS-GVO geregelt ist. Aber in anderen Punkten wäre, wie soeben skizziert, ein Rückgriff auf die Regeln des BGB zu Willenserklärungen durchaus denkbar. Seit Erlass der DS-GVO zeichnen sich hier nun zwei Positionen in der Literatur ab.

---

pflichten *Medicus/Petersen*, BGB AT, 11. Aufl. 2016, Rn. 206 ff.; *Bachmann*, in: MüKo, BGB, 8. Aufl. 2019, § 241 Rn. 29 f.

[212] *Hacker*, ZfPW 2019, 148 (162 ff.); siehe zu AGB-rechtlichen Folgen unten, § 5 C.II.1.e) aa)(3)(a)(aa).

[213] Dazu ausführlich *Kohte* AcP 185 (1985), 105; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 236 ff.; *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 37 ff.; *Langhanke*, Daten als Leistung, 2018, 42 f.; *Klass*, AfP 2005, 507 (511); zur Rechtsnatur der Einwilligung allgemein *Ohly*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, 2002, 201 ff.

[214] Dazu etwa *Kohte* AcP 185 (1985), 105 (143 ff.).

a) Die Einwilligung als geschäftsähnliche Handlung

Nach einem Teil der Literatur soll die Einwilligung nunmehr ein europarechtliches Institut sui generis darstellen,[215] sodass ein Rückgriff auf das BGB, auch im Wege der Analogie, ausgeschlossen ist.[216] Dafür wird angeführt, dass die Einwilligung durch die Definition in Art. 4 Nr. 11 DS-GVO und ihre weitere Ausgestaltung besonders in den Art. 6–9 DS-GVO ein genuiner Begriff des Unionsrechts geworden ist, der dort abschließend geregelt und autonom auszulegen ist.[217] Ferner droht in der Tat bei Rückgriff auf jeweils nationale Rechtsgeschäftslehren eine Rechtszersplitterung hinsichtlich der Wirksamkeitsvoraussetzungen der Einwilligung, die dem Desiderat der DS-GVO, einen EU-weit einheitlichen Rechtsrahmen für die Verarbeitung von personenbezogenen Daten zu schaffen,[218] zuwiderläuft.[219]

Andere Teile der Literatur hingegen erblicken in der Einwilligung eine rechtsgeschäftliche Erklärung[220] oder eine geschäftsähnliche Handlung,[221] auf welche die Wirksamkeitsvoraussetzungen des BGB für Willenserklärungen zu Lückenfüllungszwecken (analog) angewendet werden können.[222] Bisweilen wird die Einwilligung jedoch auch als Realakt qualifiziert, auf den die Regelungen des BGB nicht einmal analog angewendet werden könnten.[223]

---

[215] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 1a; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 83; *Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 Rn. 29.

[216] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 1a; *Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 Rn. 29.

[217] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 1a; *Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 Rn. 29; zur autonomen Auslegung des Unionsrechts allgemein statt vieler EuGH, Urt. v. 1.12.2016 – Rs. C-395/15 (*Daouidi*) – Rn. 50; Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 47; *Kaufmann*, in: Dauses/Ludwigs (Hrsg.), Handbuch des EU-Wirtschaftsrechts, 48. EL 2019, P. II. Vorabentscheidungsverfahren Rn. 60; *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 475 ff.

[218] Siehe nur den zehnten und den 123. Erwägungsgrund der DS-GVO.

[219] *Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 Rn. 29.

[220] Zur Rechtslage vor Geltung der DS-GVO *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 40; *Langhanke*, Daten als Leistung, 2018, 50, 226; zur zivilrechtlichen Einwilligung allgemein *Bayreuther*, in: MüKo, BGB, 8. Aufl. 2018, § 182 Rn. 2.

[221] *Gierschmann* in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung, 2017, Art. 7 Rn. 46; für die Einwilligung nach § 7 Abs. 2 UWG *Köhler*, in: Köhler/Bornkamm/Feddersen, UWG, 38. Aufl. 2020, § 7 Rn. 143; OLG Karlsruhe NJW-RR 2018, 1263 Rn. 17; bereits früh für die medizinische Einwilligung BGH NJW 1959, 811.

[222] *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 2019, Art. 7 DS-GVO Rn. 27 f.; *Gierschmann* in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung, 2017, Art. 7 Rn. 46.

[223] *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 9.

Daran ist richtig, dass die Einwilligung in der Tat keine Willenserklärung darstellt, da ihre Rechtsfolgen nicht nur deshalb eintreten, weil sie gewollt sind;[224] vielmehr erklärt der Einwilligende sich mit der Datenverarbeitung lediglich einverstanden, die Erlaubniswirkung tritt dann kraft Gesetzes ein (Art. 6 Abs. 1 lit. a DS-GVO). Denn die Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO sind abschließend und für die Erlaubniswirkung konstitutiv. Dies zeigt sich insbesondere daran, dass die Erlaubniswirkung nach Art. 6 Abs. 1 DS-GVO nicht durch dort nicht aufgeführte rechtsgeschäftliche Vereinbarungen, etwa eine schuldrechtliche Gestattung, herbeigeführt werden kann, auch wenn der Wille der Parteien der Vereinbarung übereinstimmend darauf gerichtet ist.[225] Daher stellt die datenschutzrechtliche Einwilligung lediglich eine geschäftsähnliche Handlung dar,[226] die jedoch, noch stärker als nach dem alten Datenschutzrecht, unionsrechtlich vorgeprägt ist.

b) Punktuelle Rückgriffsmöglichkeit

Nach hier vertretener Auffassung wird man daher vermittelnd anerkennen müssen, dass die Wirksamkeitsvoraussetzungen der Einwilligung unionsrechtlich determiniert und damit autonom auszulegen sind[227] – soweit sie denn in der DS-GVO oder anderen Unionsrechtsakten niedergelegt sind. Ein Mangel an positiver Regelung kann dabei eine ausfüllungsbedürftige Regelungslücke darstellen, wenn eine planwidrige Unvollständigkeit des Unionsrechts vorliegt.[228] In der Tat weist das Regelungsgefüge der DS-GVO Lücken im Bereich der Einwilligung auf,[229] wie sogleich noch im Einzelnen zu zeigen ist.[230]

Da jedoch das Unionsrecht, anders als das deutsche Privatrecht, schon aufgrund der Prinzipien der begrenzten Einzelermächtigung und der Subsidiarität (Art. 5 Abs. 1–3 EUV) lediglich eine Teilrechtsordnung darstellt[231] und gerade im Privatrecht trotz Systematisierungsmöglichkeiten[232] nur lückenhaft

---

224 Dazu etwa Armbrüster, MüKoBGB, BGB, 8. Aufl. 2018, Vor §§ 116 Rn. 3; Mot. I 126.

225 Siehe oben, § 4 B.I.3.b)bb)(2).

226 So auch die Nachweise in § 5, Fn. 221.

227 Zur autonomen Auslegung statt vieler EuGH, Urt. v. 1.12.2016 – Rs. C-395/15 (*Daouidi*) – Rn. 50; EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 47; *Kaufmann*, in: Dauses/Ludwigs (Hrsg.), Handbuch des EU-Wirtschaftsrechts, 48. EL 2019, P. II. Vorabentscheidungsverfahren Rn. 60; *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 475 ff.

228 *Neuner*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 245 (255 Rn. 27 f.), unter Rückgriff auf *Canaris*, Die Feststellung von Lücken im Gesetz, 1983, 39; ähnlich *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 68; *Basedow*, ZEuP 2014, 402 (402 f.); grundsätzlich zum Lückenbegriff auch *Bydlinski*, Juristische Methodenlehre und Rechtsbegriff, 1991, 472 ff.

229 *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 2018, Art. 7 DS-GVO Rn. 28.

230 Siehe unten, § 5 B.II.2.

231 Begriff bei *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 605.

232 Grundlegend *Grundmann*, in: Grundmann (Hrsg.), Systembildung und System-

ausgebildet ist,[233] kommt eine Lückenfüllung durch zwei auf unterschiedlichen Ebenen gelagerte Rechtsordnungen in Betracht: durch Unionsrecht, im Wege der richterlicher Rechtsfortbildung, und durch nationales Recht.[234] Sofern eine Lücke durch Unionsrecht geschlossen wird, käme eine abweichende nationale Regelung einer direkten Kollision gleich und wäre daher präkludiert.

aa) Keine allgemeine Rechtsgeschäftslehre in der DS-GVO

Eine Ausfüllung durch Unionsrecht ist zwar grundsätzlich insofern präferabel, als dadurch die Harmonisierungswirkung des jeweiligen unionalen Rechtsinstruments gewahrt und eine zersplitterte Lückenfüllung durch voneinander abweichende nationale Rechtsnormen verhindert werden kann.[235] Doch nicht jede Lücke kann unter Rekurs auf die gewünschte Harmonisierungswirkung geschlossen werden. Vielmehr setzt eine Ausfüllung durch Unionsrecht zunächst eine Regelungskompetenz der EU voraus.[236] Diese ist im Datenschutzprivatrecht nach Art. 16 Abs. 2 AEUV oder Art. 114 AEUV grundsätzlich gegeben. Ferner muss gerade eine abschließende Regelung durch den Unionsgesetzgeber gewollt sein.[237] Dabei ist der Subsidiaritätsgrundsatz (Art. 5 Abs. 3 EUV) zu beachten, da die Gesetzgebungszuständigkeiten im Datenschutzprivatrecht (mit Ausnahme des Kartellrechts) generell konkurrierend sind.[238]

Eine unionale Regelung kommt insbesondere dann in Betracht, wenn der Gleichbehandlungsgrundsatz nach Art. 20 f. GRCh eine einheitliche Regelung, und nicht wie beim *argumentum e contrario* eine differente, erfordert. Der Gleichbehandlungsgrundsatz ist dann auch nach unionsrechtlichem Me-

lücken in Kerngebieten des Europäischen Privatrechts, 2000, 1; *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 52 ff.

[233] *Riesenhuber*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 199 (216 Rn. 43); zur Genese der begrenzten Harmonisierung des Privatrechts *Grundmann*, Europäisches Schuldvertragsrecht, 1999, 1. Teil, § 1 Rn. 24 ff.; siehe ferner *Kilian*, in: Grundmann (Hrsg.), Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts, 2000, 427 (436).

[234] *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 69; *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 606; vgl. auch *Huthmacher*, Der Vorrang des Gemeinschaftsrechts bei indirekten Kollisionen, 1985, 183 ff.; *Grundmann*, in: Grundmann (Hrsg.), Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts, 2000, 1 (2 f.). Wenn man den Begriff der Lücke jedoch an den unionsrechtlichen Regelungsplan anbindet, so besteht im Falle der Regelung durch nationales Recht streng begrifflich keine Lücke im Unionsrecht (vgl. *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 69). Dies ist in der Sache jedoch unerheblich.

[235] *Basedow*, ZEuP 2014, 402 (406).

[236] *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 69; *Neuner*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 245 (256 Rn. 29); *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 609.

[237] *Neuner*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 245 (256 Rn. 30); *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 57 („Harmonisierungskonzept").

[238] *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 16 Rn. 4; *M. Schröder*, in: Streinz, EUV/AEUV, 3. Aufl. 2018, AEUV, Art. 16 Rn. 8.

thodenverständnis Grundlage für eine Analogie.[239] Ferner kann auch das sonstige Primärrecht Grundlage für eine rechtsfortbildende Lückenfüllung sein.[240] Im Rahmen des Datenschutzprivatrechts ist hier insbesondere an Ausfüllungsimpulse zu denken, die vom Datenschutzgrundrecht in Art. 8 GRCh, Art. 16 Abs. 1 AEUV ausgehen. Wie im deutschen Recht jedoch kommt eine Analogie bei unmittelbar den Einzelnen belastenden Normen (z. B. Sanktionen) infolge eines Analogieverbots nicht in Betracht.[241] Umgekehrt liegt eine Ausfüllung der Lücke durch nationales Recht nahe, wenn die unionsrechtlichen Bestimmungen kaum Anhaltspunkte für die Bewältigung der aufgeworfenen Sachprobleme bereithalten.[242]

Danach ist bezüglich der hier in Rede stehenden Frage einer einwilligungsbezogenen Rechtsgeschäftslehre eine Regelung auf unionsrechtlicher Ebene zwar durchaus denkbar, um die Harmonisierungsvorteile für Verantwortliche auch auf allgemeine Wirksamkeitsvoraussetzungen der Einwilligung zu erstrecken. Die Wahl der Rechtsform der Verordnung spricht auch dafür, Lücken grundsätzlich auf unionsrechtlicher Ebene zu schließen, da hiermit gerade unmittelbar geltendes Einheitsrecht ins Werk gesetzt werden soll.[243] Jedoch scheint es mit Blick auf die hiesige Streitfrage zu eng, eine *abschließende* Regelung *aller* mit der Einwilligung zusammenhängender und ihre Wirksamkeit betreffender Teilfragen auf unionsrechtlicher Ebene, zumal in der DS-GVO, ausmachen zu wollen. Denn es bestehen schlichtweg keine Anhaltspunkte für

---

[239] Ausdrücklich den Begriff „analog" als Folge des Gleichbehandlungsgrundsatzes verwendend EuGH, Urt. v. 12.12.1985 – Rs. 165/84 (*Krohn*) – Rn. 23, 27; aus der neueren Rechtsprechung EuGH, Urt. v. 26.9.2013 – Rs. C-509/11 (*ÖBB-Personenverkehr*) – Rn. 46–48; ferner eine Analogie erwägend EuGH, Urt. v. 11.5.2006 – Rs. C-340/04 (*Carbotermo und Consorzio Alisei*) – Rn. 51–55; siehe auch *Anweiler*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997, 318 f. Der EuGH fordert in seinem methodischen Grundsatzurteil *Krohn* als Voraussetzung für eine Analogie, „daß die für [die Adressaten eigentlich] geltende Regelung – zum einen der Regelung, auf deren analoge Anwendung sie sich berufen, weitgehend entspricht, und – zum anderen eine Lücke enthält, die mit einem allgemeinen Grundsatz des Gemeinschaftsrechts unvereinbar ist und die durch die entsprechende Anwendung geschlossen werden kann" (Rn. 14). Der erste vom EuGH genannte Schritt weicht jedoch in der neueren Rechtsprechung einem Vergleich der Lage zwischen den erfassten und den für eine Analogie in Rede stehenden Fällen; siehe die eben zitierten Stellen aus den Rechtssachen *ÖBB-Personenverkehr* und *Carbotermo und Consorzio Alisei* sowie EuGH, Urt. v. 19.11.2009 – verb. Rs. C-402/07 und C-432/07 (*Sturgeon*) – Rn. 48 ff.; *Neuner*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 245 (256 Rn. 32).

[240] Siehe bereits EuGH, Urt. v. 12.12.1985 – Rs. 165/84 (*Krohn*) – Rn. 23 („mit einem allgemeinen Grundsatz des Gemeinschaftsrechts unvereinbare Lücke"); *Neuner*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 245 (259 Rn. 36–38); *Anweiler*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997, 319 f.

[241] *Anweiler*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, 1997, 402 f.; zum nationalen Recht etwa *Canaris*, Die Feststellung von Lücken im Gesetz, 1983, 180 ff.

[242] *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 606.

[243] *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 608.

Wertungen, nach denen alle Rechtsfragen, die der allgemeine Teil des BGB hinsichtlich der Wirksamkeit von Willenserklärungen beantwortet, auf unionaler Ebene im Wege der richterlichen Rechtsfortbildung einer eigenständigen Regelung zugeführt werden könnten. Auch die Natur der Sache oder eine allgemeine Rechtsidee der Einwilligung bieten hier keinen Ausweg,[244] sondern würden auf bloße Fiktionen hinauslaufen. Aus der DS-GVO kann schlechterdings kein allgemeiner Teil einer unionalen Rechtsgeschäftslehre entwickelt werden.

bb) Keine vollständige Präklusion nationaler Regelungen: Wahrung des Effektivitätsgrundsatzes

Andererseits hat die obige Analyse gezeigt, dass die Lückenfüllung durch mitgliedstaatliches Recht den Effektivitätsgrundsatz des Unionsrechts nicht verletzen darf.[245] Insoweit ließe sich argumentieren, dass die wirksame Durchsetzung der unionsrechtlichen Zielsetzung, einen einheitlichen Rechtsrahmen für Einwilligungserklärungen zu bieten, durch jeglichen Rückgriff auf das BGB übermäßig erschwert wird und daher eine indirekte Kollision zwischen Unionsrecht und nationalem Recht, mit der Folge der Unanwendbarkeit der nationalen Regelung, vorliegt.[246] Hierfür lässt sich insbesondere anführen, dass eines der Ziele einer Regelung der Einwilligungserfordernisse auf Unionsebene die Herstellung von unionsweiter Rechtssicherheit für Verantwortliche darstellt.[247]

Allerdings ist eine Lückenfüllung durch nationale Vorschriften der Rechtssicherheit keineswegs grundsätzlich abträglich, denn in Ermangelung eines unionsrechtlichen Maßstabs zur Beurteilung dieser Fragen ist es zumal für Verantwortliche nicht notwendigerweise nachteilig, mit den bekannten, wenn auch zwischen den einzelnen Rechtsordnungen bisweilen divergierenden Kriterien der nationalen Rechtsordnung zu operieren. Die Alternative wäre eine erhebliche Unklarheit hinsichtlich der unionsrechtlich für die Lückenfüllung maßgeblichen Kriterien und Inhalte, welche der EuGH womöglich schlussendlich doch wieder unter Rekurs auf eine repräsentative Auswahl oder Gesamtschau der nationalen Vertragsordnungen gewinnen würde.[248] Der Gewinn an Rechtsvereinheitlichung durch eine allein auf die DS-GVO ausgerichtete Beantwortung dieser Fragen, der sich ohnehin nur mit erheblicher zeitlicher

[244] Dies grundsätzlich zur Lückenfüllung erwägend *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 71.

[245] Siehe oben, § 5 A.I.2.

[246] Siehe dazu allgemein oben, § 5 A.I.2.a).

[247] 7. Erwägungsgrund DS-GVO.

[248] Vgl. *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 71 (Rechtsvergleichung als *ultima ratio* der Rechtsgewinnungsquelle auf unionsrechtlicher Ebene); *Grundmann*, Europäisches Schuldvertragsrecht, 1999, 1. Teil, § 3 Rn. 191; *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 631–633, 637; *Bengoetxea*, The legal reasoning of the European Court of Justice, 1993, 245; *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, 363.

Verzögerung einstellen würde, wird daher durch den jedenfalls mittelfristigen Verlust an Rechtssicherheit aufgewogen. Dass die DS-GVO selbst den Wert der Rechtsvereinheitlichung keineswegs verabsolutiert, zeigen wiederum die zahlreichen Öffnungsklauseln zugunsten der Mitgliedstaaten.[249]

cc) Die Bedeutung der Rechtssachen *Rabobank* und *Schyns*

Vor allem ist in dem Streit um die Rückgriffsmöglichkeit auf nationales Recht jedoch bislang zu wenig beachtet worden, dass auch aus unionsrechtlicher Sicht der Rückgriff auf nationale Vertragsordnungen zur Lückenfüllung durchaus angezeigt erscheinen kann.[250] Eine dahin deutende Entscheidung ist die des EuGH in der Rechtssache *Rabobank*.[251] Inhaltlich ging es um die Frage, inwiefern eine niederländische Regelung zu Interessenkonflikten bei der Vertretung von Kapitalgesellschaften mit dem Stellvertretungsregime der ersten gesellschaftlichen Richtlinie in Einklang stand. Der EuGH befand in einem ersten Schritt, dass die Richtlinie für die Frage der Interessenkonflikte keinerlei Regelung enthielt.[252] Dieses konkrete Ergebnis ist zwar inhaltlich durchaus fragwürdig,[253] was jedoch im hiesigen Kontext nicht weiterverfolgt werden muss. Entscheidend ist in methodischer Hinsicht, dass er in einem zweiten Schritt feststellte, dass die Lücke im Richtlinienregime gerade durch Rückgriff auf die Regelung aus dem nationalen Stellvertretungsrecht geschlossen wird.[254] Implizit wird damit der Herausbildung eines „allgemeinen Teils" des Unionsprivatrechts allein auf Grundlage richterlicher Rechtsfortbildung eine Absage erteilt.[255] In ganz ähnlicher Weise ermöglichte der EuGH in der Rechtssache *Schyns* den Rückgriff auf nationales Recht für die Bestimmung der Rechtsfolgen des negativen Ausgangs einer Kreditwürdigkeitsprüfung im Rahmen der Vergabe eines Verbraucherkredits.[256]

Dass es sich bei der DS-GVO um eine Verordnung, nicht um eine Richtlinie handelt, kann einen methodischen Unterschied hier nicht rechtfertigen. Jeweils geht es um die Frage, inwiefern eine mangelnde unionsrechtliche Determination durch nationale Regelungen ergänzt werden kann und muss. Dabei spielt es

[249] Siehe z. B. Art. 6 Abs. 2 f.; Art. 8 Abs. 1 UAbs. 2; Art. 9 Abs. 2 lit. a, b, g–j und Abs. 4; Art. 26 Abs. 1; Art. 36 Abs. 5; 58 Abs. 6; Art. 85; Art. 87 f.; Art. 91 DS-GVO.

[250] *Huthmacher*, Der Vorrang des Gemeinschaftsrechts bei indirekten Kollisionen, 1985, 183 ff.

[251] EuGH, Urt. v. 16.12.1997 – Rs. C-104/96 (*Rabobank*); siehe auch bereits oben, Text bei § 5, Fn. 34.

[252] EuGH, Urt. v. 16.12.1997 – Rs. C-104/96 (*Rabobank*) – Rn. 22.

[253] Zustimmend etwa *Steindorff*, 36 Common Market Law Review 191, 199 ff. (1999); ablehnend etwa *Schmid*, AG 1998, 127 (130); *Grundmann*, Europäisches Gesellschaftsrecht, 2011, Rn. 226.

[254] EuGH, Urt. v. 16.12.1997 – Rs. C-104/96 (*Rabobank*) – Rn. 24.

[255] Im Ergebnis auch *Huthmacher*, Der Vorrang des Gemeinschaftsrechts bei indirekten Kollisionen, 1985, 188.

[256] EuGH, Urt. v. 6.6.2019 – Rs. C-58/18 (*Schyns*) – Rn. 42–49; siehe dazu bereits oben, Text bei § 5, Fn. 36 und 80.

keine Rolle, ob diese unionsrechtliche Vorgabe wie bei der Verordnung unmittelbar geltendes oder aber wie bei der Richtlinie grundsätzlich noch umzusetzendes Recht darstellt. Denn es ging weder in *Rabobank* noch in *Schyns* um solche Umsetzungsspielräume, die nur eine Richtlinie den nationalen Gesetzgebern überantwortet, sondern um schlechthin auf unionsrechtlicher Ebene nicht geregelte Rechtsfragen im Kontext von im Übrigen vollharmonisierenden Richtlinien.

dd) Punktuelle Ergänzung der DS-GVO durch nationales Recht

Zur entscheidenden Weichenstellung wird damit, inwiefern eine bestimmte nationale Regelung, bei gleichzeitiger Wahrung der Ziele der unionsrechtlichen Regelungen, zur Lückenfüllung erforderlich ist.[257] Wie gesehen ist die Unionsrechtsordnung als Teilrechtsordnung auf Ergänzung durch nationales Recht nicht nur angelegt, sondern sogar angewiesen.[258] Die Grenze wird sich nicht in allen Fällen trennscharf bestimmen lassen. Jedenfalls dann aber, wenn keinerlei Anhaltspunkte für Beurteilungsmaßstäbe in der DS-GVO oder anderen Unionsrechtsakten enthalten sind, wird man von einer durch nationales Vertragsrecht auszufüllenden Regelungslücke ausgehen müssen. Letztlich muss daher jeweils für die unterschiedlichen Sachfragen einzeln untersucht werden, inwiefern tatsächlich eine Regelungslücke vorliegt und ob diese auf unionaler Ebene durch Auslegung der DS-GVO oder durch den Rückgriff auf das BGB ausgefüllt werden soll.

Beim Rückgriff auf das BGB ist dabei nach dem oben Erörterten[259] nicht nur eine direkte, sondern auch eine indirekte Kollision zu vermeiden, indem der Äquivalenz- und der Effektivitätsgrundsatz des Unionsrechts beachtet werden. Dadurch werden die Konsequenzen des Streits in rechtlicher Hinsicht entschärft: Die Wertungen der DS-GVO dürfen jedenfalls durch die analoge Anwendung der nationalen Regelungen auf die Einwilligung nicht unterlaufen werden.[260] Dies impliziert insbesondere, dass die oben entwickelte zweistufige Prüfung angewandt werden muss.[261] Daher ist jeweils zu fragen, ob die nationale Norm ein in der DS-GVO nicht adressiertes Risiko spezifisch regelt und mit den Zielen der DS-GVO kompatibel ist. Mit Blick auf die Einwilligung muss dabei beachtet werden, dass eine nationale Regelung insbesondere auch dann entbehrlich sein kann, wenn die Möglichkeit des Widerrufs der Einwilligung die Interessen der betroffenen Person hinreichend vor den relevanten Risiken schützt. Daher ist nicht generell, sondern immer nur punktuell und

[257] *Huthmacher*, Der Vorrang des Gemeinschaftsrechts bei indirekten Kollisionen, 1985, 189.

[258] Grundlegend EuGH, Urt. v. 21.9.1983, verb. Rs. 205 bis 215/82 (*Deutsche Milchkontor*) – Rn. 21.

[259] Siehe oben, § 5 A.I.

[260] *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 2018, Art. 7 DS-GVO Rn. 28.

[261] Siehe oben, § 5 A.I.2.b)aa).

nach sorgfältiger Prüfung der unionsrechtlich vorgegebenen Voraussetzungen ein Rückgriff auf den allgemeinen Teil des BGB zur Bestimmung der Wirksamkeit einer Einwilligung nach der DS-GVO möglich.[262]

2. *Einzelne Probleme der Rechtsgeschäftslehre*

Es muss daher für jede rechtsgeschäftliche Wirksamkeitsvoraussetzung des BGB einzeln entschieden werden, inwiefern ein Rückgriff auf die Norm, in entsprechender Anwendung, neben dem Einwilligungsregime der DS-GVO stattfinden kann. Dabei können in den folgenden Abschnitten nur die wichtigsten Probleme dargestellt werden. Dies betrifft zunächst die Frage der Einwilligungsfähigkeit (a)), sodann den subjektiven Tatbestand der Einwilligung und dort besonders das Einwilligungsbewusstsein (b)), zudem Regeln zu Abgabe und Zugang der Einwilligung (c)) sowie die Möglichkeit einer Stellvertretung (d)) und schließlich die besonders umstrittene Regelung von Willensmängeln (e)). Die Behandlung der §§ 107 ff. BGB erfolgte bereits oben im Rahmen von Art. 8 DS-GVO.[263]

a) Einwilligungsfähigkeit

Schon nach dem alten Datenschutzrecht war die Einwilligungsfähigkeit ungeschriebene Wirksamkeitsvoraussetzung für die Einwilligung.[264] Regeln über die Behandlung von Fällen, für welche das BGB Geschäftsunfähigkeit nach § 104 Nr. 2 BGB oder § 105 Abs. 2 BGB anordnet, sucht man in der DS-GVO jedoch vergebens. Daher wäre es denkbar, auf diese Normen in analoger Anwendung zur Bestimmung der Einwilligungsfähigkeit zurückzugreifen.

Allerdings erscheint es vorzugswürdig, aus der Systematik der DS-GVO das Kriterium der Einwilligungsfähigkeit und bestimmte Fallgruppen zu entwickeln. Dies scheint deshalb möglich, weil mit Art. 8 Abs. 1 DS-GVO eine Regelung der Einwilligungsfähigkeit von Minderjährigen erfolgt ist und in Anlehnung an diese Wertung besonders schwere Formen der medizinisch relevanten kognitiven oder voluntativen Beeinträchtigung *a fortiori* erfasst werden können.[265] Letztlich ist dafür die individuelle Einsichtsfähigkeit entscheidend.[266]

---

[262] Ähnlich *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 13.

[263] Siehe oben, § 4 B.I.3.b)bb).

[264] *Artikel-29-Datenschutzgruppe*, Stellungnahme 15/2011 zur Definition von Einwilligung, WP 187, 2011, 33 f., 41; für die Einwilligung allgemein *Ohly*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, 2002, 293 ff. und 452.

[265] *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 83 und Art. 8 Rn. 9.

[266] *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 8 DS-GVO Rn. 10; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 70; *Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 Rn. 32; *Buchner*, WRP 2018, 1283 (1287).

Die Einwilligung von schwer intoxizierten oder an einer die Willensbildung beeinträchtigenden psychischen Krankheit leidenden Personen kann daher analog Art. 8 Abs. 1 DS-GVO nur durch einen Vertreter abgegeben werden.[267] Für die Vertretungsregeln selbst muss jedoch auf das jeweilige nationale Recht (z. B. §§ 1896 ff. BGB) zurückgegriffen werden, da etwa für die Entwicklung eines unionalen Betreuungsrechts aus der DS-GVO jegliche Anhaltspunkte fehlen.[268] Dieser Rückgriff ist aufgrund der spezifischen durch die Vertretung Geschäftsunfähiger zu adressierenden Risiken erforderlich und auch sachgerecht; ein Anwendungsvorrang des Unionsrechts besteht insofern nicht.

b) Subjektiver Tatbestand, insbesondere Einwilligungsbewusstsein

Der objektive Tatbestand der Einwilligung ist in Art. 4 Nr. 11 DS-GVO und dem 32. Erwägungsgrund der DS-GVO verhältnismäßig klar ausgearbeitet. Damit ist jedoch noch nicht geklärt, wie es um den subjektiven Tatbestand der Einwilligung bestellt ist. Die herrschende Meinung der deutschen Rechtsgeschäftslehre fordert als subjektiven Minimaltatbestand einer Willenserklärung bekanntlich Handlungswillen und Erklärungsbewusstsein,[269] wobei letzteres aus Verkehrsschutzgesichtspunkten überwunden werden kann, wenn der Erklärende bei Anwendung der im Verkehr erforderlichen Sorgfalt zumindest hätte erkennen und vermeiden können, dass seine Handlung nach der Verkehrssitte als Willenserklärung aufgefasst werden darf und sie der Empfänger auch tatsächlich so verstanden hat.[270]

Dass auch die Einwilligung von einem Handlungswillen getragen sein muss, dürfte unstreitig sein. Denn sonst kann eine Zurechnung zu der betroffenen

---

[267] Zur Stellvertretung allgemein sogleich, unter § 5 B.II.2.d).

[268] Siehe zu den Vertretungsregeln im Hinblick auf die Einwilligung allgemein *Ohly*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, 2002, 452 ff.; vgl. ferner auch AG Altötting ZD 2020, 258.

[269] Siehe nur *Singer*, in: Staudinger, BGB, 2017, Vorbem §§ 116 ff Rn. 27–29; *Musielak*, AcP 211 (2011), 769 (777 f.); weitergehend etwa (auch Geschäftswille, verstanden als Rechtsfolgewille) *Eisenhardt*, JZ 1986, 875 (879); enger *Lorenz*, Der Schutz vor dem unerwünschten Vertrag, 1997, 220 (nur Handlungswille).

[270] BGH NJW 1984, 2279; BGH NJW 1990, 454 (456) für schlüssiges Verhalten; BGH NJW 1995, 953; *Medicus/Petersen*, BGB AT, 11. Aufl. 2016, Rn. 607; *Lorenz*, Der Schutz vor dem unerwünschten Vertrag, 1997, 223 ff.; *Wendtland*, in: BeckOK BGB, 50. Ed. 2019, § 133 Rn. 6; *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, Vor §§ 116 Rn. 27; *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 119 Rn. 104; *Eisenhardt*, JZ 1986, 875 (880); *Flume*, AT II, 4. Aufl. 1992, 449 f.; differenziert (im Sinne einer objektiven Theorie) *de la Durantaye*, Wille und Erklärung, 2020, 37 ff.; aA (Vorrang der negativen Privatautonomie) *Canaris*, NJW 1984, 2281; *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, 1971, 427 f., 548 ff.; *Wolf/Neuner*, BGB AT, 11. Aufl. 2016, § 32 Rn. 22 f.; *Singer*, Selbstbestimmung und Verkehrsschutz im Recht der Willenserklärungen, 1995, 169 ff.; *Singer*, in: Staudinger, BGB, 2017, Vorbem §§ 116 ff Rn. 37 ff.; *Musielak*, AcP 211 (2011), 769 (801); weitergehend hingegen die objektive Theorie, etwa *von Craushaar*, AcP 174 (1974), 2 (5 ff.) (Erklärungsbewusstsein grundsätzlich nicht notwendig).

Person schlechthin nicht stattfinden.[271] Nicht ausdrücklich ist jedoch in der DS-GVO geregelt, ob ein Einwilligungsbewusstsein der betroffenen Person notwendige Voraussetzung für eine wirksame Einwilligung ist. Zwar wird teilweise vertreten, dass ein derartiges Kriterium in Art. 4 Nr. 11 DS-GVO und dem 32. Erwägungsgrund der DS-GVO, vor allem dem Merkmal der Unmissverständlichkeit, enthalten sei.[272] Dem ist jedoch entgegenzuhalten, dass Unmissverständlichkeit schon begrifflich nicht auf den subjektiven Horizont des Erklärenden, sondern das Verständnis eines kommunikativen Gegenübers abstellt. Dies trifft auch auf die exemplarische Präzisierung dieses Merkmals im 32. Erwägungsgrund der DS-GVO zu. Unmittelbar ist damit für die Frage der Notwendigkeit subjektiven Erklärungsbewusstseins nichts gewonnen.

Dennoch muss nach hier vertretener Auffassung die Abgabe einer datenschutzrechtlichen Einwilligung bewusst erfolgen, weil damit zugleich der Eingriff in das Datenschutzgrundrecht legitimiert wird. Wenn Unmissverständlichkeit hinsichtlich der Setzung eines objektiven Erklärungstatbestands gefordert wird (Art. 4 Nr. 11 und 32. Erwägungsgrund der DS-GVO), dann ist dies zumindest Ausfluss des Desiderats, dass dem Einwilligenden die Rechtserheblichkeit der Erklärung bewusst wird.[273] Dies ist schon deshalb notwendig, weil nicht nur die negative Privatautonomie, sondern auch der Stellenwert des unionalen Datenschutzgrundrechts dafür streitet, eine Disposition über personenbezogene Daten gerade qua Einwilligung nur dann anzunehmen, wenn diese Entscheidung bewusst erfolgt. Denn nur so kann dem im siebten Erwägungsgrund prominent formulierten Ziel, der betroffenen Person Kontrolle über ihre Daten zu gewähren, entsprochen werden. Ohne Bewusstsein einer Disposition ist eine rationale Entscheidung darüber schlechthin unmöglich. Daher ist richtigerweise ein Einwilligungsbewusstein als unionsrechtliche Voraussetzung einer wirksamen Einwilligung zu fordern.[274]

Anders als das rechtsgeschäftliche Erklärungsbewusstsein kann das Fehlen des Einwilligungsbewusstseins nach hier vertretener Auffassung auch nicht aus Verkehrsschutzgründen überwunden werden.[275] Dafür spricht weniger der Umstand, dass der Tatbestand der Einwilligung nicht mit Verschuldenselementen vermengt werden sollte.[276] Denn Verkehrsschutzgesichtspunkte sind

[271] Vgl. nur *Medicus/Petersen*, BGB AT, 11. Aufl. 2016, Rn. 606; *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, Vor §§ 116 Rn. 22; *Singer*, in: Staudinger, BGB, 2017, Vorbem §§ 116 ff Rn. 27.

[272] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 57.

[273] Vgl. *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 57.

[274] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 56; *Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 Rn. 33.

[275] Zur Frage mangelnden Erklärungsbewusstseins bei Abschluss eines Nutzungsvertrags, der Wirkung nach Art. 6 Abs. 1 lit. b DS-GVO entfaltet, unten, Text bei § 5, Fn. 415 ff.

[276] So für die Willenerklärung aber *Wolf/Neuner*, BGB AT, 11. Aufl. 2016, § 32 Rn. 23.

auch der DS-GVO keinesfalls fremd; wie gesehen ist eines ihrer Ziele der freie Datenverkehr.[277] Vielmehr sind zwei Erwägungen entscheidend. Erstens steht, anders als im Rahmen einer allgemeinen rechtsgeschäftlichen Erklärung, den Verkehrsschutzbelangen nicht nur die negative Privatautonomie, sondern auch das unionale Datenschutzgrundrecht entgegen. Dies stärkt die Position der betroffenen Person. Zweitens ist in funktionaler Betrachtung das Ziel der Einwilligung für den Verantwortlichen, die Rechtmäßigkeit der Datenverarbeitung herbeizuführen. Verkehrsschutzinteressen des Verantwortlichen können jedoch systematisch besser im Rahmen der Interessenabwägung von Art. 6 Abs. 1 lit. f DS-GVO Berücksichtigung finden. Anders als in der allgemeinen Rechtsgeschäftslehre ist also die Zuerkennung einer privatautonomen Bindung nicht alternativlos. Daher muss insgesamt das Einwilligungsbewusstsein positiv vorliegen, wenngleich bei Erfüllung des objektiven Erklärungstatbestands der Mangel des Einwilligungsbewusstseins durch die betroffene Person darzulegen und zu beweisen ist.[278]

c) Abgabe und Zugang

Vor Geltungsbeginn der DS-GVO bestand nach herrschender Meinung ein Abgabe- und Zugangserfordernis für die datenschutzrechtliche Einwilligung, für das auf die Regelungen des BGB zurückgegriffen wurde.[279] Dies lässt sich für die Einwilligung nach der DS-GVO nun nach hier vertretener Auffassung nicht mehr halten.

aa) Abgabe

Eine Abgabe der Einwilligung ist weiterhin erforderlich, richtet sich nun aber nach der DS-GVO. Denn gemäß Art. 4 Nr. 11 DS-GVO ist die Einwilligung definiert als eine „abgegebene Willensbekundung". Daraus erhellt einerseits die Notwendigkeit der Abgabe der Einwilligung; andererseits ist die Abgabe damit zugleich ein autonom auszulegender Begriff des Unionsrechts.[280] Die Abgabe ist freilich auch im BGB nur unvollständig geregelt.[281] Die Wertungen der Diskussionen um die Abgabe einer Willenserklärung nach dem BGB können jedoch als argumentativer Fundus auf die Abgabe der Einwilligung nach der DS-GVO übertragen werden.

---

[277] Siehe oben, § 5 A.I.2.c)aa).

[278] Vgl. BGH NJW-RR 1986, 415 (415) zum rechtsgeschäftlichen Erklärungsbewusstsein.

[279] Für die Rechtslage vor Inkrafttreten der DS-GVO *Kohte* AcP 185 (1985), 105 (121 f.); *Klass*, AfP 2005, 507 (511).

[280] Vgl. EuGH, Urt. v. 1.12.2016 – Rs. C-395/15 (*Daouidi*) – Rn. 50; EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 47; *Kaufmann*, in: Dauses/Ludwigs (Hrsg.), Handbuch des EU-Wirtschaftsrechts, 48. EL 2019, P. II. Vorabentscheidungsverfahren Rn. 60; *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 475 ff.

[281] *Medicus/Petersen*, BGB AT, 11. Aufl. 2016, Rn. 257 f.

Allerdings dürfte der Rechtsschein der Abgabe, der nach wohl herrschender Literaturansicht nach deutschem Zivilrecht für die Abgabe ausreicht,[282] dem Abgabeerfordernis der DS-GVO nicht Genüge tun. Hinsichtlich des subjektiven Tatbestands der Einwilligung muss, wie soeben erörtert, ein Einwilligungsbewusstsein positiv vorliegen. Genauso muss jedoch das Bewusstsein der Abgabe vorhanden sein, da sonst die Entscheidung über die Legitimation der Verarbeitung gerade nicht durch die betroffene Person selbst getroffen wird. Auch dies ist Ausfluss der durch das Einwilligungsregime angestrebten Kontrolle der betroffenen Person über die Verwendung ihrer Daten.[283]

Daher reicht es nicht aus, dass die Einwilligung jederzeit widerrufen werden kann und der Verantwortliche die betroffene Person über die Datenverarbeitung auf Grundlage der Einwilligung informieren muss (Art. 13 Abs. 1 lit. c DS-GVO). Denn erstens könnte der Widerruf die Rechtmäßigkeit der Datenverarbeitung, die zwischen Abgabe und Widerruf erfolgt, nicht mehr beeinflussen. Zweitens besteht die Widerrufmöglichkeit besteht auch bei vorangekreuzten Kästchen und ähnlichen objektiv zweideutigen Handlungen, führt jedoch auch dort nicht zu einer wirksamen Einwilligung.[284] Drittens können auch beim Rechtsschein der Abgabe die Verkehrsschutzinteressen des Verantwortlichen systematisch stimmiger bei Art. 6 Abs. 1 lit. f DS-GVO berücksichtigt werden. Daher ist letztlich eine bewusste Entäußerung für eine Abgabe zu fordern.

bb) Zugang

Nicht geregelt ist in der DS-GVO hingegen, ob für das Wirksamwerden der Einwilligung deren Zugang beim Verantwortlichen notwendig ist. Nach § 130 Abs. 1 S. 1 BGB ist der Zugang für das Wirksamwerden einer Willenserklärung unter Abwesenden bekanntlich Voraussetzung und verlangt, dass der Empfänger von der Willenserklärung tatsächlich Kenntnis nimmt oder diese so in seinen Machtbereich gelangt, dass mit der Kenntnis unter gewöhnlichen Umständen zu rechnen ist.[285] Diese Formel kann jedoch nach hier vertretener Auffassung auf die datenschutzrechtliche Einwilligung nach der DS-GVO nicht übertragen werden. Denn aus einer systematischen und teleologischen Auslegung der DS-GVO erhellt, dass ein Zugang der Einwilligung beim Ver-

[282] *Medicus/Petersen*, BGB AT, 11. Aufl. 2016, Rn. 267; *Einsele*, in: MüKo, BGB, 8. Aufl. 2018, § 130 Rn. 14; *Wendtland*, in: BeckOK BGB, 50. Ed. 2019, § 130 Rn. 6; aA *Canaris*, JZ 1976, 132 (133); *Wolf/Neuner*, BGB AT, 11. Aufl. 2016, § 32 Rn. 17 f.; *Singer*, in: Staudinger, BGB, 2017, Vorbem §§ 116 ff Rn. 49; differenzierend *de la Durantaye*, Wille und Erklärung, 2020, 47 f.; jedenfalls für die abhanden gekommene Vollmachtsurkunde einen Rechtsschein ablehnend BGH NJW 1975, 2101 (2102 f.); aA insoweit *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, 1971, 427.

[283] Siehe nur den 7. Erwägungsgrund der DS-GVO.

[284] Siehe oben, § 4 B.I.3.a)aa).

[285] Siehe nur BGH NJW 1977, 194; *Einsele*, in: MüKo, BGB, 8. Aufl. 2018, § 130 Rn. 16; *Singer/Benedict*, in: Staudinger, BGB, 2017, 130 Rn. 39 ff.

antwortlichen bereits keine Wirksamkeitsvoraussetzung darstellt. Daher gilt für die Einwilligung die Entäußerungstheorie.[286]

Der EuGH hat allerdings in einer frühen, vereinzelt gebliebenen Entscheidung den „in allen Ländern der Gemeinschaft anerkannte[n] Rechtsgrundsatz [angewandt], wonach eine schriftliche Willenserklärung wirksam wird, sobald sie ordnungsgemäß in den Machtbereich des Empfängers gelangt ist."[287] Im Kontext der Entscheidung, in dem es um einen Bußgeldbescheid einer Behörde an ein Unternehmen ging, der an den Geschäftssitz des Unternehmens übermittelt wurde, hat der EuGH damit jedoch nur deutlich gemacht, dass es für die Wirksamkeit nicht darauf ankommen kann, ob der Bescheid an eine Betriebsniederlassung des Unternehmens weitergeleitet wurde.[288] *Jedenfalls* der Empfang des Schreibens führt daher zum Wirksamwerden einer schriftlichen Willenserklärung.[289] Damit ist jedoch nichts darüber gesagt, ob der Zugang auch *erforderlich* ist.

In teleologischer Hinsicht ist ein Zugang nicht zwingend notwendig, da für den Empfänger die Wirksamkeit der Einwilligung lediglich Vorteile birgt[290] und die informationelle Selbstbestimmung der betroffenen Person auch gewahrt wird, wenn die Einwilligung lediglich von ihr abgegeben wurde und der Verantwortliche im Rahmen der Einwilligung tätig wird, ohne dass diese ihm zugegangen ist. Dies kann etwa der Fall sein, wenn der Verantwortliche vermutet, dass eine Einwilligung erfolgt, diese aber noch nicht bei ihm eingegangen ist. Auch in ökonomischer Hinsicht ist nicht ersichtlich, dass die in § 3 genannten Typen von Marktversagen oder sonstige Risiken[291] verstärkt würden, wenn die Einwilligung lediglich abgegeben wurde, jedoch nicht zugegangen ist. Vielmehr manifestieren sich die Probleme der Informationsasymmetrie, der verhaltensökonomischen Effekte, der Externalitäten und auch der Unschärfe des Datenpreises allesamt bei der Entscheidung des Nutzers über den Umfang, in dem er Datenverarbeitungen zulassen möchte. Diese Entscheidung kulminiert jedoch in der Abgabe, nicht im Zugang der Einwilligungserklärung.

Da die Einwilligungserklärung praktisch immer vom Verantwortlichen vorformuliert wird, wird er über deren Inhalt kaum in Unkenntnis sein. Er

---

[286] Zu dieser Theorie *Medicus/Petersen*, BGB AT, 11. Aufl. 2016, Rn. 269; *Singer/Benedict*, in: Staudinger, BGB, 2017, 130 Rn. 3; *Einsele*, in: MüKo, BGB, 8. Aufl. 2018, § 130 Rn. 8.

[287] EuGH, Urt. v. 10.12.1957 – Rs. 8/56 (*A.L.M.A.*), Slg. 1957, 191 (200); in der Sache trifft dies nicht zu, da etwa in Deutschland der Zugang, nicht der bloße Empfang, zum Wirksamwerden einer Willenserklärung unter Abwesenden führt.

[288] Vgl. EuGH, Urt. v. 10.12.1957 – Rs. 8/56 (*A.L.M.A.*), Slg. 1957, 191 (200).

[289] Siehe auch *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, 328 (Anwendung der Empfangstheorie).

[290] Andere Willenserklärungen hingegen können für den Empfänger mit Nachteilen verbunden sein, weshalb ihm das Risiko der Verzögerung und des Verlusts nicht grundsätzlich auferlegt werden, siehe *Medicus/Petersen*, BGB AT, 11. Aufl. 2016, Rn. 269.

[291] Siehe oben, § 3 B.II.

trägt lediglich das Risiko, dass die Einwilligung entgegen seiner Erwartung doch nicht abgegeben wurde und daher die legitimierende Wirkung von Art. 6 Abs. 1 lit. a DS-GVO entfällt. Für die informationelle Selbstbestimmung der betroffenen Person ist es jedoch irrelevant, ob die Einwilligung tatsächlich zugegangen oder auf der Datenautobahn verloren gegangen ist. Man wird auch nicht behaupten können, dass gerade der Zugang der Einwilligung auf den Verantwortlichen datenschutzrechtlich disziplinierend wirke[292] – eher ist das Gegenteil anzunehmen.

Auch in systematischer Hinsicht sprechen die besseren Argumente gegen eine Zugangsnotwendigkeit. Art. 7 Abs. 1 DS-GVO verlangt zwar, dass der Verantwortliche die Einwilligung der betroffenen Person nachweisen muss. Dies setzt typischerweise, wenngleich nicht notwendig, den Zugang der Einwilligung voraus. Jedoch stellt Art. 7 Abs. 1 DS-GVO lediglich eine Beweislastregel[293] oder allenfalls eine formale Verfahrensvorschrift dar,[294] deren Verletzung jedenfalls nicht zur materiellen Unwirksamkeit der Einwilligung führt.[295] Ähnliches gilt für die nach Art. 13 Abs. 1 lit. c DS-GVO erforderliche Angabe, dass die Datenverarbeitung auf der Einwilligung basiert. Sofern die Einwilligung abgegeben wurde, ist die entsprechende Information zutreffend; wurde sie nicht abgegeben, ist die Information fehlerhaft und kann zu diesbezüglichen Sanktionen führen. Beides berührt aber nicht die Frage der Wirksamkeit der Einwilligung. Entscheidend dürfte schließlich in systematischer Hinsicht gegen das Zugangserfordernis streiten, dass Art. 4 Nr. 11 DS-GVO lediglich von der Abgabe, nicht jedoch dem Zugang der Einwilligung spricht. Weder der Wortlaut noch die Systematik oder der Sinn und Zweck des Einwilligungsregimes erfordern daher ihren Zugang. Er ist damit entbehrlich.

d) Stellvertretung

Eine weitere Frage, zu der sich die DS-GVO nicht explizit verhält, ist die Möglichkeit der Stellvertretung bei der Abgabe der Einwilligung.[296] In der Literatur wird dies teilweise wegen der vermeintlichen Höchstpersönlichkeit der Einwilligung ausgeschlossen,[297] wobei die Vertreter dieser Auffassung eine

---

[292] So könnte man *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 42 verstehen, allerdings unmittelbar lediglich mit Bezug auf Art. 7 Abs. 1 DS-GVO.

[293] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 23.

[294] So *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 45.

[295] *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 45.

[296] Zur Rechtslage vor Geltung der DS-GVO *Langhanke*, Daten als Leistung, 2018, 45 ff.

[297] *Ernst*, ZD 2017, 110 (111); *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 8 f.; für die Rechtslage vor Geltung der DS-GVO etwa *Kohte* AcP 185 (1985), 105 (142).

Botenschaft (bzw. eine nicht näher aufgeschlüsselte „botenähnliche Figur") für zulässig halten.[298]

Vorzugswürdig erscheint es demgegenüber jedoch, eine Stellvertretung zuzulassen, sofern an die Vollmacht dieselben Anforderungen wie an die Einwilligung gestellt werden, auch hinsichtlich ihrer Bestimmtheit.[299] Denn der bloße Akt der Delegation ändert nichts an den datenschutzspezifischen Risiken, sodass ein grundsätzlicher Ausschluss der Stellvertretung mit dem Ziel des Einwilligungsregimes, der betroffenen Person Kontrolle über die Disposition ihrer Daten zu geben, und dem Grundsatz der Privatautonomie kollidiert. Insbesondere wird die betroffene Person durch das jederzeitige Widerrufsrecht hinsichtlich der Einwilligung und der Vollmacht geschützt.[300] Schließlich lässt sich aus Art. 8 Abs. 1 DS-GVO ableiten:[301] Wenn schon der gesetzliche Vertreter für den Minderjährigen, bei dem ein besonders hohes datenschutzrechtliches Gefährdungspotenzial besteht, eine Einwilligung abgeben kann, dann muss dies erst recht für voll Geschäftsfähige gelten, die eine freiwillige und informierte rechtsgeschäftliche Vollmacht erteilt haben.

Allerdings muss den in § 3 genannten Typen von Marktversagen auch im Rahmen der Stellvertretung Rechnung getragen werden. Die Informationspflichten sind daher jedenfalls gegenüber dem Vertretenen zu erfüllen, da diesen die Folgen der Entscheidung treffen und er über die Abgabe der Vollmacht, und damit auch die Möglichkeit der Einwilligung, entscheidet.[302] Dank des Offenkundigkeitsprinzips, § 164 Abs. 2 BGB, ist dem Geschäftspartner der Akt der Stellvertretung auch regelmäßig bekannt, sodass auf dessen Seite sichergestellt werden kann, dass der Vertretene tatsächlich die Möglichkeit der Kenntnisnahme der Pflichtinformationen hat. Der Verantwortliche muss daher nicht befürchten, unerkannt lediglich mit einem Stellvertreter zu interagieren und daher Informationspflichten zu verletzen. Aus ökonomischer Perspektive erscheint es jedoch darüber hinaus sinnvoll, auch dem Vertreter die Pflichtinformationen zukommen zu lassen, sofern dieser (trotz Bestimmtheit der Vollmacht) einmal signifikanten eigenen Gestaltungsspielraum hat. Allerdings

---

[298] *Ernst*, ZD 2017, 110 (111); *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 8 f.

[299] *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 31; *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 19; *Gierschmann* in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung, 2017, Art. 7 Rn. 47; wohl auch *Langhanke*, Daten als Leistung, 2018, 47 f. für die Rechtslage vor Geltung der DS-GVO; differenzierend für Eingriffe in höchstpersönliche Rechtsgüter allgemein *Ohly*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, 2002, 456 ff.

[300] Zur freien Widerrufbarkeit der Vollmacht *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 31.

[301] *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 19.

[302] *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 19.

ist dem Geschäftspartner dieser Umstand (Existenz eines signifikanten Gestaltungsspielraums) regelmäßig nicht bekannt. Vorzugswürdig erscheint es daher, grundsätzlich zu verlangen, dass die Pflichtinformationen auch gegenüber dem Stellvertreter erteilt werden, ein Unterlassen jedoch nicht zu sanktionieren, falls der Vertreter keinen Gestaltungsspielraum hatte. Dies führt auch nicht zu einer signifikanten Mehrbelastung des Verantwortlichen, da dieser ohnehin mit dem Stellvertreter interagiert und diesem bei dieser Gelegenheit auch die Pflichtinformationen übermitteln kann.

Schließlich gilt auch für die Vollmacht, was bereits für die Einwilligung thematisiert wurde: Das Fehlen konstitutiver Voraussetzungen der Vollmacht kann nicht durch eine Anscheins- oder Duldungsvollmacht überwunden werden.[303] Denn auch insoweit ist zu berücksichtigen, dass die Erklärung der Vollmacht eine bewusste Disposition über die durch das unionale Datenschutzgrundrecht geschützten personenbezogenen Daten darstellen muss und Verkehrsschutzgesichtspunkte im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO Berücksichtigung finden können.

e) Die Behandlung von Willensmängeln

Besonders umstritten ist schließlich, wie schon nach altem Recht,[304] die Frage, ob Einwilligungserklärungen nicht nur nach Art. 7 Abs. 3 DS-GVO widerrufen, sondern auch nach §§ 119 ff. BGB angefochten werden können. Dies ist insofern relevant, als der Widerruf gemäß Art. 7 Abs. 3 S. 2 DS-GVO nur ex nunc wirkt, die Anfechtung jedoch gemäß § 142 Abs. 1 BGB ex tunc.[305] Für die Analyse ist zwischen den einzelnen Willensmängeln zu differenzieren.

aa) Widerrechtliche Drohung

Klar verneint werden muss eine unionsrechtliche Lücke für den Fall einer widerrechtlichen Drohung im Sinne von § 123 Abs. 1 F2 BGB, welche den Erklärenden zur Abgabe der Einwilligung bewegt.[306] Diese Drohung zieht die Unfreiwilligkeit der Einwilligung nach Art. 4 Nr. 11 DS-GVO nach sich.[307]

---

[303] Zum Streit um die Rechtswirkungen der Anscheins- und Duldungsvollmacht im allgemeinen Stellvertretungsrecht *Wolf/Neuner*, BGB AT, 11. Aufl. 2016, § 50 Rn. 84 ff.; *Medicus/Petersen*, BGB AT, 11. Aufl. 2016, Rn. 969 ff.; *Schilken*, in: Staudinger, BGB, 2014, § 167 Rn. 30 ff.; *Canaris*, JZ 1976, 132 (133); *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, 1971, 39 ff., 191 ff.

[304] Zur Rechtslage vor Geltungsbeginn der DS-GVO *Kohte* AcP 185 (1985), 105 (139 ff.).

[305] *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 2018, Art. 7 DS-GVO Rn. 29; zur Rechtslage vor Geltung der DS-GVO *Langhanke*, Daten als Leistung, 2018, 90.

[306] Zum Schutz der Willensentschließungsfreiheit durch § 123 Abs. 1 F2 BGB *Lorenz*, Der Schutz vor dem unerwünschten Vertrag, 1997, 348.

[307] *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 2018, Art. 7 DS-GVO Rn. 29; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 33; *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 49; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019,

Denn eine hinreichend gewichtige Drohung führt dazu, dass der Erklärende eine freie Wahl wegen eines Mangels im Bereich der Willensbildung nicht mehr ausüben kann.[308] Dies ist jedoch nach dem 42. Erwägungsgrund der DS-GVO Voraussetzung für die Freiwilligkeit der Einwilligung. Rechtsfolge der Unfreiwilligkeit ist die Unwirksamkeit der Einwilligung, die entweder direkt wegen des Verstoßes gegen zwingendes Recht (Art. 4 Nr. 11 DS-GVO) oder, aus demselben Gedanken heraus, analog Art. 7 Abs. 2 S. 2 DS-GVO eintritt.[309] Im Regelfall bedarf es daher im Fall einer widerrechtlichen Drohung nicht der Anfechtung nach § 123 Abs. 1 BGB, um die Einwilligung zu Fall zu bringen.

(1) Fortbestehendes Interesse der betroffenen Person

Problematisch ist dabei jedoch, dass die Unfreiwilligkeit der Einwilligung grundsätzlich zu ihrer Unwirksamkeit führt, wohingegen die Rechtsfolge einer Drohung bei der Abgabe einer Willenserklärung bekanntermaßen lediglich deren Anfechtbarkeit ist. Diese erhielte dem Einwilligenden die Möglichkeit, von der Ausübung des Gestaltungsrechts abzusehen und so die Einwilligung gegen sich gelten zu lassen.[310] Dies ist insbesondere vor dem Hintergrund der herrschenden Meinung, wonach eine nachträgliche Genehmigung von Datenverarbeitungsvorgängen nicht möglich ist,[311] ein potenziell erheblicher Gesichtspunkt: Die unwirksame Einwilligung kann danach eben nicht mit Rechtswirkung für die Vergangenheit nachgeholt werden. Es ist nicht auszuschließen, dass der Einwilligende trotz Drohung oder Täuschung ein Interesse an der Legalität der Verarbeitung seiner Daten auch bis zum Zeitpunkt der möglichen Abgabe einer neuen, wirksamen Einwilligungserklärung haben kann.[312]

Allerdings lässt sich diese Fallgruppe durch eine Modifikation der Rechtsfolgen der Unfreiwilligkeit der Einwilligung bewältigen: Da die Sanktion der Unwirksamkeit primär die informationelle Selbstbestimmung des Einwilligenden schützen soll,[313] ist im Fall des fortbestehenden Interesses des Einwilligenden an der Erlaubniswirkung der Einwilligung ausnahmsweise von deren Wirksamkeit auszugehen. Dieses Interesse muss der Erklärende allerdings nach außen wirksam artikulieren. Mit der Dogmatik der Einwilligung

Art. 7 DS-GVO Rn. 93; wohl auch *Gierschmann* in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung, 2017, Art. 7 Rn. 48.

[308] *Singer/von Finckenstein*, in: Staudinger, BGB, 2017, § 123 Rn. 1.

[309] Für die Analogie zu Art. 7 Abs. 2 S. 2 DS-GVO *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 52; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 7, 78; *Gierschmann* in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung, 2017, Art. 7 Rn. 132; *Tavanti*, RDV 2016, 231 (238).

[310] Vgl. *Singer/von Finckenstein*, in: Staudinger, BGB, 2017, § 123 Rn. 1.

[311] Siehe oben, § 4 B.I.3.a)ee).

[312] Vgl. *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 123 Rn. 2.

[313] Vgl. den 42. Erwägungsgrund der DS-GVO.

ist diese Modifikation durchaus vereinbar, da auch nicht jede Verletzung der Informationspflichten nach Art. 13 f. DS-GVO zur Uninformiertheit der Einwilligung und damit zu deren Unwirksamkeit führt.[314] Daher sprechen letztlich die besseren Gründe dafür, bei fortdauerndem Interesse in teleologischer Reduktion (bzw., nach Diktion des EuGH: restriktiver Interpretation) von Art. 4 Nr. 11 DS-GVO die Unwirksamkeitsfolge des Unionsrechts entfallen zu lassen,[315] statt ein Anfechtungsrecht mit potenziell harmonisierungsfeindlicher Zersplitterung der Voraussetzungen zwischen den Mitgliedstaaten anzunehmen.

(2) Doppelwirkung im Mehrebenenrecht?

Wenn hingegen die Einwilligung wegen Unfreiwilligkeit nach Maßgabe der DS-GVO ex tunc unwirksam ist, so stellt sich die Frage, ob die nichtige Erklärung nicht dennoch durch den Erklärenden wegen Drohung gem. § 123 Abs. 1 BGB angefochten werden kann.[316] Dies würde zu einer Art Doppelwirkung[317] im Mehrebenensystem führen.[318] Allerdings ist nicht ersichtlich, dass für den Erklärenden damit gegenüber der unionsrechtlichen Unwirksamkeit irgendein Vorteil verbunden wäre. Dies ist aber für die Anerkennung der Ausübung eines Gestaltungsrechts in Bezug auf ein unwirksames Rechtsgeschäft entscheidend.[319] Zugleich sind die Rechtsfolgen einer Anfechtung unionsrechtlich nicht geregelt, sodass divergierende Bestimmungen zwischen den Mitgliedstaaten die Harmonisierungswirkung der DS-GVO gefährden können. Eine Anfechtung der unwirksamen Einwilligung würde daher kein spezifisches, in der DS-GVO nicht adressiertes Risiko bewältigen, jedoch po-

[314] *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 15; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 59; *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 36.

[315] Zur restriktiven Interpretation im Unionsrecht EuGH, Urt. v. 1.4.2008 – verb. Rs. C-14/06 und C-295/06 (*Parlament/Kommission*) – Rn. 65 ff., 71; Urt. v. 4.10.1991 – Rs. C-183/90 (*van Dalfsen*) – Rn. 19; allgemein *Neuner*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 245 (258 Rn. 33).

[316] Die Anfechtbarkeit eines unwirksamen Rechtsgeschäfts grundsätzlich bejahend BGH NJW 2009, 3655 (3656); *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 142 Rn. 12; *Wendtland*, in: BeckOK BGB, 50. Ed. 2019, § 142 Rn. 4; siehe auch BGH NJW 2010, 610 Rn. 16 ff. zum Widerruf eines unwirksamen Vertrags; kritisch dazu *Möller*, NJW 2010, 612; *Schreiber*, AcP 211 (2011), 35 (43 ff.).

[317] Eine Doppelwirkung im Sinne des deutschen Zivilrechts liegt jedoch nur vor, wenn aus zwei unterschiedlichen Gründen dieselbe Rechtsfolge eintritt, siehe *Schreiber*, AcP 211 (2011), 35 (38). Dies ist aufgrund der national z. T. potenziell abweichenden Rechtsfolgen einer Anfechtung nicht gesichert. Für § 123 Abs. 1 BGB gilt dies freilich durchaus, da insbesondere ein Anspruch nach § 122 BGB nicht in Betracht kommt.

[318] Grundlegend *Kipp*, in: Festschrift der Berliner Juristischen Fakultät für Ferdinand von Martitz zum fünfzigjährigen Doktorjubiläum am 24. Juli 1911, 1911, 211; dazu etwa *Schreiber*, AcP 211 (2011), 35 (37 ff.); *Würdinger*, JuS 2011, 769; *Herbert*, JZ 2011, 503.

[319] Siehe BGH NJW 2010, 610 Rn. 17.

tenziell zu einer Wirksamkeitseinbuße führen. Daher ist sie mit dem Effektivitätsgrundsatz des Unionsrechts nicht vereinbar.

bb) Arglistige Täuschung

Ganz identisch ist bei einer arglistigen Täuschung gem. §123 Abs. 1 F1 BGB zu entscheiden. Diese beeinträchtigt „die freie Selbstbestimmung auf rechtsgeschäftlichem Gebiete“[320] und damit zumindest die Informiertheit der Einwilligung, da sie einer faktenbasierten Willensbildung entgegensteht.[321] Insofern besteht, genau wie bei der Drohung, keine Lücke im Unionsrecht. Diesen Befund bestätigt auch die herrschende Meinung zur medizinischen Einwilligung, die nach §630d Abs. 3 BGB ebenfalls jederzeit widerrufbar ist, bei der jedoch Drohung und Täuschung gleichwohl zur Unwirksamkeit führen.[322]

cc) Erklärungs- und Inhaltsirrtum

Anders hingegen stellt sich die Sachlage im Fall eines Erklärungs- oder Inhaltsirrtums nach §119 Abs. 1 BGB dar. Dieser Irrtum beeinträchtigt die informierte Willensausübung.[323] Er berührt jedoch nach hier vertretener Auffassung die Informiertheit der Einwilligung nach der DS-GVO nicht,[324] da insofern ausreichend ist, dass die notwendigen Informationen korrekt bereitgestellt werden und der Einwilligende die zumutbare Möglichkeit der Kenntnisnahme hat.[325] Ob er diese Informationen kognitiv überhaupt zur Kenntnis nimmt oder richtig verarbeitet, ist für die Informiertheit der Einwilligung unerheblich, wie die datenschutzrechtliche Analyse gezeigt hat. Daher besteht im

---

[320] Mot. I, 204; zur Freiheit der Willensentschließung als Schutzgut von §123 Abs. 1 F1 BGB *Lorenz*, Der Schutz vor dem unerwünschten Vertrag, 1997, 314.

[321] Offen gelassen (Mangel der Freiwilligkeit oder Informiertheit) von *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 33; *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 49; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 83; *Gierschmann* in: Gierschmann/Schlender/Stentzel/Veil, Kommentar Datenschutz-Grundverordnung, 2017, Art. 7 Rn. 48; aA *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 2018, Art. 7 DS-GVO Rn. 29 (lediglich Anfechtbarkeit); letztlich wird man die Täuschung als Mangel der Informiertheit, nicht der Freiwilligkeit, werten müssen, da andernfalls, wenn jeder Mangel der Informationsgrundlage einer Entscheidung zugleich die Freiwilligkeit entfallen ließe, das Kriterium der Informiertheit in Art. 4 Nr. 11 DS-GVO obsolet wäre; im Ergebnis ebenso für die Rechtslage vor Geltungsbeginn der DS-GVO *Riesenhuber*, RdA 2011, 257 (259).

[322] OLG Nürnberg VersR 1988, 299; *Katzenmeier*, in: BeckOK BGB, 50. Ed. 2019, §650d Rn. 7.

[323] *Singer/von Finckenstein*, in: Staudinger, BGB, 2017, §123 Rn. 1; *Singer/von Finckenstein*, in: Staudinger, BGB, 2017, §123 Rn. 1; *Klass*, AfP 2005, 507 (514).

[324] So wohl auch *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 93; aA *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 33.

[325] Siehe oben, §4 B.I.3.a)cc)(2).

Fall von § 119 Abs. 1 BGB durchaus eine Lücke im unionsrechtlichen Einwilligungsregime.[326]

(1) Grundsätzliche Entbehrlichkeit neben dem Widerruf

Daher ist in einem nächsten Schritt im Rahmen der zweistufigen Prüfung zu fragen, ob die BGB-Norm ein spezifisches, in der DS-GVO nicht geregeltes Risiko adressiert und ob diese Regelung, auch mit Blick auf die Zielsetzungen der DS-GVO, sachgerecht ist. Die Risikospezifizität ist zu bejahen, da die DS-GVO auch außerhalb von Art. 4 Nr. 11 und Art. 12–14 DS-GVO die Gefahr eines Erklärungs- oder Inhaltsirrtums in keiner Weise adressiert.

Allerdings ist die Gewährung eines Anfechtungsrechts nach § 119 Abs. 1 BGB neben der jederzeitigen Widerrufsmöglichkeit nach Art. 7 Abs. 3 DS-GVO jedenfalls grundsätzlich nicht erforderlich und daher letztendlich nicht sachgerecht.[327] Durch diese Möglichkeit sind die relevanten Risiken zumindest indirekt abgedeckt. Dahingegen würde durch die Zubilligung eines Anfechtungsrechts, wie bereits mehrfach erwähnt, die Gefahr divergierender nationaler Regelungsordnungen geschaffen, welche dem Harmonisierungsziel des unionsrechtlichen Datenschutzregimes zuwiderlaufen.

Ein sachlicher Grund für die Anerkennung einer Anfechtbarkeit neben der Widerruflichkeit ist im Fall von Erklärungs- und Inhaltsirrtümern nicht ersichtlich. Denn erstens kommt dem Widerruf durch das rückwirkende Löschungsrecht in Art. 17 Abs. 1 lit. a DS-GVO eine partielle ex tunc-Wirkung zu. Zweitens ist der Empfänger der Einwilligungserklärung, anders als im Falle einer widerrechtlichen Drohung oder einer arglistigen Täuschung, schutzwürdig.[328] Denn er kann den Inhalts- oder Erklärungsirrtum typischerweise nicht erkennen und darf daher, wie auch Dritte, auf die Rechtmäßigkeit der Datenverarbeitung vertrauen. Diese würde durch die ex tunc-Wirkung der Anfechtung jedoch entfallen.[329] Zwar ließe sich auf eine rückwirkende Unrechtmäßigkeit wohl weder ein zivilrechtlicher Schadensersatzanspruch nach Art. 82 DS-GVO noch eine Geldbuße nach Art. 83 DS-GVO stützen.[330] Damit besteht jedoch auch kein anerkennenswertes Interesse des Erklärenden, die Einwilligung ex tunc zu Fall zu bringen. Drittens spricht dagegen auch die erhöhte Rechtsunsicherheit, welche mit der Möglichkeit einer Anfechtung, die auf rein internen Irrtümern basiert, einhergeht.

---

[326] Für eine Anerkennung von §§ 119–124 BGB als allgemeine negative Tatbestandsmerkmale, wie sie für die Rechtslage vor Geltungsbeginn der DS-GVO vertreten wurde (*Riesenhuber*, RdA 2011, 257 [260]), ist unter der DS-GVO kein Raum mehr.

[327] Eine Widerrufsmöglichkeit halten auch für ausreichend *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 33; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 93.

[328] Zu diesem Kriterium *Rogosch*, Die Einwilligung im Datenschutzrecht, 2013, 40.

[329] Siehe oben, § 5, Fn. 305.

[330] Vgl. *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 93.

(2) Anfechtung im Fall von § 142 Abs. 2 BGB

Anders kann sich die Lage allein im Fall von § 142 Abs. 2 BGB darstellen, wenn der Erklärungsempfänger die Anfechtbarkeit nach § 119 Abs. 1 BGB kannte oder kennen musste. Dann erscheint auch ein Schadensersatzanspruch des Betroffenen, der durch eine rückwirkende Unwirksamkeit der Einwilligung herbeigeführt wird, angemessen. Der Empfänger ist in diesem Fall nicht schutzwürdig und auch die Bedenken hinsichtlich der Rechtsunsicherheit greifen dann nicht durch. Daher stellt sich die Anfechtbarkeit analog § 119 BGB in diesen Fällen als sachgerechter Interessenausgleich dar, der auch den Zielen der DS-GVO, insbesondere dem freien Datenverkehr und dem Schutz der Grundrechte und Grundfreiheiten des Verantwortlichen, nicht zuwiderläuft. Denn der Kontext ist im Falle der Bösgläubigkeit des Erklärungsempfängers mit der Drohung und Täuschung zu vergleichen, die, wie gerade gesehen, schon unionsrechtlich zur Unwirksamkeit ex tunc führt. Allerdings muss die betroffene Person in Fällen des Irrtums die Anfechtung auch tatsächlich gem. § 143 Abs. 1 BGB erklären, da auch hier die Möglichkeit besteht, dass der Erklärende die Einwilligung trotz Irrtums gegen sich gelten lassen will.[331] In rechtstatsächlicher Hinsicht ist schließlich allerdings anzumerken, dass die Kenntnis der Anfechtbarkeit oder ihre fahrlässige Unkenntnis letztlich nur selten zu beweisen sein wird.[332]

dd) Beachtlicher Motivirrtum

Für den Fall eines beachtlichen Motivirrtums nach § 119 Abs. 2 BGB schließlich kann nichts anderes gelten als bei § 119 Abs. 1 BGB. Auch hier besteht eine Lücke im unionsrechtlichen Einwilligungsregime. Ein Rückgriff auf eine Anfechtung ist jedoch grundsätzlich infolge des Widerrufsrechts entbehrlich. Lediglich bei Kenntnis oder fahrlässiger Unkenntnis des Erklärungsempfängers von der Anfechtbarkeit kann der Anwendungsvorrang des Unionsrechts überwunden und ein Anfechtungsrecht gemäß § 119 Abs. 2 BGB zugebilligt werden.

3. Zusammenfassung zu Rechtsgeschäftslehre und Einwilligung

Die Einwilligung stellt nach hier vertretener Auffassung eine geschäftsähnliche Handlung dar, sodass grundsätzlich ein Rückgriff auf die Rechtsgeschäftslehre des BGB in entsprechender Anwendung möglich ist. Dies setzt jedoch mit Blick auf den Anwendungsvorrang des Unionsrechts voraus, dass kein An-

[331] Ebenso im Ergebnis zur Rechtslage vor Geltungsbeginn der DS-GVO *Kohte* AcP 185 (1985), 105 (141), auch zur Fristenproblematik; *Klass*, AfP 2005, 507 (514); anders der BGH zum erheblichen Irrtum bei einer Einwilligung in die Freiheitsentziehung: BGH NJW 1964, 1177 (1178) (ex lege Unwirksamkeit).

[332] Zur Wissenszurechnung beim Einsatz KI-gestützter Systeme durch den Empfänger siehe *Hacker*, RW 9 (2018), 243 (270ff.).

haltspunkt für eine Regelung der spezifischen Rechtsfrage durch die DS-GVO besteht (Risikospezifizität) und ein Rückgriff auf nationales Recht auch angesichts der Möglichkeit des Widerrufs der Einwilligung erforderlich erscheint (Zielkompatibilität). Nach diesen Kriterien ist eine analoge Anwendung der Rechtsgeschäftslehre des BGB nur in zwei Fällen möglich. Erstens ist die betroffene Person analog § 119 BGB zur Anfechtung berechtigt, wenn der Verantwortliche die Anfechtbarkeit kannte oder kennen musste (§ 142 Abs. 2 BGB). Zweitens ist eine Stellvertretung grundsätzlich möglich und es muss hinsichtlich des Stellvertretungsregimes auf die §§ 164 ff. BGB in analoger Anwendung zurückgegriffen werden.

Die übrigen hier verhandelten Fragen lassen sich hingegen auf unionaler Ebene lösen. Ein Zugang der Einwilligung ist für das Wirksamwerden der Einwilligung richtigerweise schon nicht notwendig, so dass sich eine analoge Anwendung von § 130 Abs. 1 S. 1 BGB erübrigt; vielmehr gilt auf Grundlage der DS-GVO die Entäußerungstheorie. Ferner können und müssen Kriterien für die Einwilligungsfähigkeit und die Abgabe der Einwilligung jeweils aus der DS-GVO selbst entwickelt werden. Dabei ist entscheidend zu erkennen, dass zu den Grundsätzen der Privatautonomie und des Verkehrsschutzes, welche die allgemeine Rechtsgeschäftslehre des BGB durchziehen, das unionale Datenschutzgrundrecht als weiterer Abwägungsfaktor hinzutritt. Dies führt im Ergebnis dazu, dass die Maßstäbe, nach denen ein fehlendes Erklärungsbewusstsein, eine fehlende Abgabe oder eine nicht bestehende Vollmacht nach Rechtsscheinsgrundsätzen im Rahmen des BGB durch die herrschende Meinung überwunden werden, nicht auf die parallel gelagerten Probleme bei der Einwilligung übertragen werden können. Vielmehr sind hier ein Erklärungsbewusstsein, eine Abgabe und das Bestehen einer Vollmacht positiv zu fordern. Das Verkehrsschutzinteresse des Verantwortlichen oder von Dritten kann bei Art. 6 Abs. 1 lit. f DS-GVO systemgerecht berücksichtigt werden.

Ferner zeigt sich, dass der Rückgriff auf die Anfechtungstatbestände des BGB grundsätzlich nicht möglich ist. Die widerrechtliche Drohung und die arglistige Täuschung lassen bereits die Freiwilligkeit bzw. Informiertheit der Einwilligung nach dem unionsrechtlichen Datenschutzregime entfallen. Irrtümer nach § 119 BGB berechtigen hingegen grundsätzlich nicht zur Anfechtung, da die Interessen des Erklärenden durch die Möglichkeit des Widerrufs nach Art. 7 Abs. 3 DS-GVO hinreichend gewahrt werden und ein darüberhinausgehendes Anfechtungsrecht der Harmonisierungswirkung der DS-GVO zuwiderlaufen würde. Dieses ist daher durch den Anwendungsvorrang des Unionsrechts, genauer: den Effektivitätsgrundsatz, gesperrt. Ausnahmsweise ist eine Anfechtung jedoch nach § 119 BGB möglich, wenn der Erklärungsempfänger die Anfechtbarkeit kannte oder kennen musste.

Es bleibt daher bei einer punktuellen Anwendung der Rechtsgeschäftslehre des BGB auf die Einwilligung. Dies ist vor allem auch dem Ziel der DS-GVO, eine Harmonisierung der Wirksamkeitsvoraussetzungen der Einwilligung zu

bewirken, geschuldet. Gänzlich umgekehrt stellt sich das Regel-Ausnahme-Verhältnis hinsichtlich des Abschlusses eines Vertrages dar, der nach Art. 6 Abs. 1 lit. b DS-GVO die Rechtmäßigkeit der Datenverarbeitung bewirkt. Dem widmet sich der folgende Abschnitt.

III. Vertragsschluss und DS-GVO

Hinsichtlich des Einwilligungsregimes ist ein Rückgriff auf die Rechtsgeschäftslehre des BGB nur vereinzelt möglich. Gänzlich anders stellt sich die Lage beim Vertragsschluss dar, auch wenn der Vertrag nach Art. 6 Abs. 1 lit. b DS-GVO die Rechtmäßigkeit der Datenverarbeitung herbeiführt. Hier ist der Rekurs auf nationales Vertragsrecht grundsätzlich möglich und erforderlich, da die DS-GVO zur Frage des Abschlusses und der Wirksamkeit des Vertrages keine auch nur entfernten Ansatzpunkte beinhaltet. Gemäß Art. 3 Abs. 10 DIDD-Richtlinie überlässt auch diese die Probleme des Abschlusses und der Wirksamkeit eines auf die Bereitstellung digitaler Inhalte oder Dienstleistungen gerichteten Vertrages gänzlich dem nationalen Vertragsrecht;[333] Gleiches gilt für die Warenkauf-Richtlinie nach deren Art. 3 Abs. 6.

Lediglich sekundär können die Wertungen der DS-GVO zum Einwilligungsregime Berücksichtigung finden, um Wertungsinkonsistenzen zu vermeiden. Abgesehen von solchen punktuellen Modifikationen findet das nationale Vertragsrecht jedoch uneingeschränkte Anwendung. Daher ist insbesondere danach zu fragen, wie nicht nur die Verhältnisse zwischen Erstanbieter und Primärnutzer (1.), sondern auch zu Dritten, die im Rahmen der digitalen Wirtschaft und zumal der drei Leitfälle eine entscheidende Rolle spielen, vertraglich gestaltet werden können (2.).

1. Ermöglichungsstrukturen zwischen Erstanbieter und Primärnutzer

Im Rahmen der bilateralen Beziehungen zwischen betroffener Person und datenschutzrechtlich Verantwortlichem herrscht zunächst einmal grundsätzlich gemäß § 311 Abs. 1 BGB Vertragsfreiheit, welche die privatautonome Gestaltung des Verhältnisses durch rechtsgeschäftliche Vereinbarungen ermöglicht.[334] Bekanntlich ist der Grundsatz der Privatautonomie grundrechtlich über Art. 16 GRCh[335] und Art. 2 Abs. 1 GG[336] abgesichert. Den Parteien steht es daher zunächst einmal frei, Vertragsklauseln so zu vereinbaren, wie es ihrem gemeinsamen Interesse entspricht. Dies bedeutet insbesondere, dass eine

[333] Siehe nur *Metzger*, JZ 2019, 577 (583 f.).

[334] Statt vieler *Emmerich*, in: MüKo, BGB, 8. Aufl. 2019, § 311 Rn. 1 f.; *Feldmann*, in: Staudinger, BGB, 2018, § 311 Rn. 1.

[335] EuGH, Urt. v. 18.7.2013 – Rs. C-426/11 (*Alemo-Herron*) – Rn. 32.

[336] *Di Fabio*, in: Maunz/Dürig, GG, 86. EL Januar 2019, Art. 2 Rn. 101.

Einigung auch auf solche Klauseln möglich ist, die eine erweiterte Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO ermöglichen.

Allerdings wird der Grundsatz der Privatautonomie nicht schrankenlos gewährt,[337] sodass auch im bilateralen Verhältnis zwischen Erstanbieter[338] und Primärnutzer die Wirksamkeit der vertraglichen Vereinbarung genau zu prüfen ist (dazu im Einzelnen unten, § 5 C.). Denn nur dann kann sie ihre datenschutzrechtliche Legitimationswirkung im Rahmen von Art. 6 Abs. 1 lit. b DS-GVO entfalten.[339]

2. *Drittbezogene Ermöglichungsstrukturen*

Die Analyse der vorangegangenen Kapitel hat jedoch gezeigt, dass Austauschprozesse im Rahmen der digitalen Wirtschaft in erheblichem Maße durch Drittbezüge gekennzeichnet sind,[340] welche das durch einen grundsätzlich bilateralen Bezugsrahmen und die Relativität der Schuldverhältnisse geprägte Vertragsrecht vor prinzipielle Herausforderungen stellen.[341] Es würde jedoch den Rahmen der Arbeit sprengen, eine Dogmatik der Vertragsnetze[342] oder Verbundverträge[343] für das Internet der Dinge zu entwickeln.[344] Die folgenden Überlegungen konzentrieren sich daher, unter angelegentlicher Einbeziehung auch der Multipolarität von *leistungs*bezogenen Rechtsverbindungen in digitalen Austauschverhältnissen,[345] auf die Wechselwirkungen von Datenschutz-

---

[337] *Emmerich*, in: MüKo, BGB, 8. Aufl. 2019, § 311 Rn. 3 f.; *Di Fabio*, in: Maunz/Dürig, GG, 86. EL Januar 2019, Art. 2 Rn. 104.

[338] Unter dem Erstanbieter wird derjenige Anbieter verstanden, an dessen Leistung der Nutzer primär interessiert ist. Bei einem IoT-Gerät bezeichnet der Primär-/Erstanbieter denjenigen, von dem der Nutzer das Produkt erwirbt und mit dem daher ein Kaufvertrag (oder ein sonstiger Nutzungsvertrag, siehe § 5, Fn. 368) zustande kommt.

[339] Siehe oben, Text bei § 4, Fn. 921.

[340] Siehe insbesondere oben, § 3 A.III.

[341] Siehe nur *Grünberger*, AcP 218 (2018), 213 (245, 288 f.); zur bilateralen Grundkonzeption des (bürgerlich-rechtlichen) Vertragsrechts auch *Oechsler*, Gerechtigkeit im modernen Austauschvertrag, 1997, 386 ff.; *Zwanzger*, Der mehrseitige Vertrag, 2013, 28 ff.

[342] Dazu *Grundmann*, AcP 207 (2007), 718 (733 ff.); aus entscheidungstheoretischer und rechtlicher Sicht nun auch *Grundmann*, in: Grundmann/Hacker (Hrsg.), Theories of Choice. The Social Science and the Law of Decision Making, 2020, (im Erscheinen).

[343] Dazu *Teubner*, Netzwerk als Vertragsverbund, 2004, 101 ff.; *Malzer*, Vertragsverbünde und Vertragssysteme, 2013, 427 ff.

[344] Ansätze hierzu bei *Grünberger*, AcP 218 (2018), 213 (290 ff.); knapp auch bei *Wendehorst*, NJW 2016, 2609 (2610); *Wendehorst*, in: Wendehorst/Zöchling-Jud (Hrsg.), Ein neues Vertragsrecht für den digitalen Binnenmarkt?, 2016, 45 (50).

[345] Dazu ausführlich *Grünberger*, AcP 218 (2018), 213 (280 ff.); *Engert*, AcP 218 (2018) 304 (344 ff.); *Wendehorst*, in: Wendehorst/Zöchling-Jud (Hrsg.), Ein neues Vertragsrecht für den digitalen Binnenmarkt?, 2016, 45 (60 ff.); *Wendehorst*, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, Rechtsgutachten für Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz, 2016, 5 f., 72 ff. (mit der grundlegenden Unterscheidung von Einheits-, Agentur- und Garantiemodellen sowie dem Vorschlag einer – vertragsnetzähnlichen – Netzwerkhaftung des Herstellers).

recht und Vertragsrecht im Allgemeinen und hier nun die Multirelationalität von personenbezogenen Daten im Besonderen.

In datenbasierten Austauschverhältnisse, besonders aber im Internet der Dinge, werden personenbezogene (und andere) Daten an Drittanbieter weitergeleitet oder von diesen direkt durch Tracking-Instrumente erhoben; umgekehrt erfassen besonders IoT-Geräte Daten von unbeteiligten Dritten in signifikantem Umfang.[346] Aufgrund der datenschutzrechtlichen Legitimationswirkung nach Art. 6 Abs. 1 lit. b DS-GVO besteht mithin ein erhebliches Interesse der Anbieter dahingehend, auch zu diesen Dritten, bzw. als Drittanbieter zu den Primärnutzern, vertragliche Bande zu knüpfen.[347]

Die Fragestellung lässt sich daher in der Weise zuspitzen, dass jeweils eruiert werden soll, welche Möglichkeiten der Schaffung von vertraglichen Verbindungen zwischen den relevanten Akteuren im Bereich datenbasierter Austauschverhältnisse, besonders des Internets der Dinge, das bestehende Vertragsrecht überhaupt bereithält. Allerdings wird sich erweisen, dass diese schon tatbestandlich nicht in allen drei Leitfällen zu einer vertraglichen Bindung der Dritten (Drittanbieter, dazu unter a); Drittnutzer, dazu unter b)) führen können. Ferner müssen gerade aufgrund der datenschutzrechtlichen Legitimationswirkung die Wertungen der DS-GVO bei der Auslegung der Willenserklärungen berücksichtigt werden. Von den hier behandelten Problemen der Einbeziehung Dritter ist die Frage scharf zu trennen, ob autonome Geräte selbst für den Vertragsschluss, als Stellvertreter, Boten, technische Werkzeuge oder gar Entitäten mit eigener Rechtspersönlichkeit, genutzt werden können,[348] was im weiteren Verlauf der Arbeit noch genauer ausgeführt wird.[349]

a) Einbeziehung von Drittanbietern

Insbesondere Drittanbieter dürften ein gesteigertes Interesse an einer vertraglichen Einbindung haben, da dies zumindest potenziell eine Datenweiterleitung an sie oder eine direkte Datenerhebung durch sie datenschutzrechtlich nach

---

[346] Siehe oben, § 3 A. und § 3 D.I.

[347] Dieses Interesse kann jedoch infolge der dadurch ausgelösten vertraglichen Haftung wiederum reduziert sein, was letztlich eine Frage des Einzelfalls ist. Grundsätzlich dürften jedoch die datenschutzrechtlichen Sanktionen (Art. 82 ff. DS-GVO) mittlerweile gegenüber der vertraglichen Haftung (Streuschäden) das „schärfere Schwert" darstellen, so dass datenschutzrechtliche Compliance – via Vertrag – tendenziell stärker wiegt als die Vermeidung vertraglicher Haftung gegenüber Nutzern.

[348] Dazu etwa *Cornelius*, MMR 2002, 353 (354 f.); *Sester/Nitschke*, CR 2004, 548; *Sorge*, Softwareagenten, 2006, 23 ff.; *Wettig*, Vertragsabschluss mittels elektronischer Agenten, 2010, 161 ff.; *Bräutigam/Klindt*, NJW 2015, 1137 (1137 f.); *Sosnitza*, CR 2016, 764 (766 ff.); *Schirmer*, JZ 2016, 660 (663 f.); *Günther*, Roboter und rechtliche Verantwortung, 2016, 52 ff.; *Keßler*, MMR 2017, 589 (592); *Specht/Herold*, MMR 2018, 40; *Borges*, NJW 2018, 977 (979); *Paulus/Matzke*, ZfPW 2018, 431 (442 ff.); *Heuer-James/Chibanguza/Stücker*, BB 2018, 2818 (2820 ff.); *Specht*, Diktat der Technik, 2019, 44 ff.; *Paulus*, Jus 2019, 960 (964 f.); *Foerster*, ZfPW 2019, 418 (425 ff.).

[349] Siehe unten, § 6 C.I.3.c)aa)(1).

Art. 6 Abs. 1 lit. b DS-GVO legitimieren könnte. Im Rahmen des Internets der Dinge ist insbesondere bereits die vertragliche Einbindung von Erbringern digitaler Zusatzleistungen, die nicht mit dem Verkäufer des Geräts identisch sind,[350] komplex. In der Literatur werden hier verschiedene Lösungsansätze diskutiert,[351] die aber im Kontext dieser Arbeit nicht im Einzelnen verfolgt werden können. Demgegenüber ist bislang das Problem der vertraglichen Einbeziehung von datenschutzrechtlich relevanten Drittanbietern, die etwa lediglich Tracking betreiben oder personalisierte Werbung schalten, soweit ersichtlich nicht systematisch untersucht worden. Dies betrifft jedoch zentral den ersten und zweiten Leitfall. So ist denkbar, dass sich der Nutzer auch gegenüber einem Drittanbieter (zum Beispiel dem Anbieter eines Tracking-Instruments, das in das Produkt des Erstanbieters eingebunden wird) zur Abgabe einer Einwilligung und zur Überlassung von Daten verpflichtet. Dies kann insbesondere dann datenschutzrechtlich relevant sein, wenn eine Einwilligung später widerrufen wird.[352] Ferner kann der Drittanbieter sich verpflichten, bestimmte Dienste (zum Beispiel personalisierte Werbung) zu erbringen, für welche die von ihm gewünschte Datenanalyse erforderlich ist. Für derartige Verknüpfungen kommen ein mehrseitiger Vertrag, ein bilateraler Vertragsschluss unter Verwendung des Erstanbieters als Stellvertreter für den Drittanbieter, ein Vertrag zugunsten Dritter oder auch eine Bedingung zugunsten Dritter in Betracht.

aa) Mehrseitiger Vertrag

Erstanbieter, Drittanbieter und Nutzer können sich im Rahmen der Vertragsfreiheit auf einen mehrseitigen Vertrag einigen, durch den auch Rechte und Pflichten des Nutzers gegenüber dem Drittanbieter geregelt werden.[353] Für eine Legitimationswirkung im Rahmen von Art. 6 Abs. 1 lit. b DS-GVO kom-

[350] Zur Vielzahl dieser Akteure etwa *Grünberger*, AcP 218 (2018), 213 (286), der Veräußerer, Hersteller, die Inhaber von Immaterialgüterrechten, Access-Provider, Anbieter digitaler Dienstleistungen sowie Plattform- oder Cloudanbieter unterscheidet; siehe auch *Wendehorst*, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, Rechtsgutachten für Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz, 2016, 2–4; knapper *Wendehorst*, in: Schulze/Staudenmayer (Hrsg.), Digital Revolution. Challenges for Contract Law in Practice, 2016, 189 (196).

[351] Siehe die Nachweise oben, in § 5, Fn. 345; vgl. ferner zur Bedeutung mehrseitiger Verträge für das Internet der Dinge, infolge der Mehrzahl der Anbieter, die an einem Produkt beteiligt sind, *Heun/Assion*, CR 2015, 812 (815); *Börding et al.*, CR 2017, 134 (136 f.); in der Praxis wird dann regelmäßig der Verkäufer des Geräts als konkludent durch die anderen Anbieter bevollmächtigt angesehen werden müssen, wenn diese am Abschluss des Vertrags ein eigenes Interesse haben; vgl. *Heuer-James/Chibanguza/Stücker*, BB 2018, 2818 (2825); siehe auch *Solmecke/Vondrlik*, MMR 2013, 755 (755 ff.).

[352] Siehe oben, § 4 C.I.2.c)bb)(2).

[353] Zum Abschluss eines mehrseitigen Vertrags ausführlich *Zwanzger*, Der mehrseitige Vertrag, 2013, 133 ff.

men nach hier vertretener Auffassung jedoch Pflichten des Nutzers selbst nicht in Betracht.[354] Vielmehr müsste der Drittanbieter sich zur Erbringung von Leistungen verpflichten, für deren Erfüllung die Weiterleitung von Daten an ihn oder die direkte Erhebung durch ihn erforderlich ist. Dies lässt sich für eine Verpflichtung zur Erbringung personalisierter Dienstleistungen oder Werke, inklusive personalisierter Werbung, durchaus begründen.[355]

(1) Grundsätzlich nur ausdrücklicher Vertragsschluss

Abgesehen von Wirksamkeitsfragen, die später zu behandeln sind (unter § 5 C.), ist hier jedoch zu bemerken, dass ein mehrseitiger Vertrag rein tatbestandlich unter den Bedingungen der digitalen Wirtschaft grundsätzlich nur in ausdrücklicher, nicht in konkludenter Form geschlossen werden kann. Zwar ist die Anwendung der Lehre vom objektiven Empfängerhorizont auf mehrseitige Verträge infolge der Vielzahl der Vertragsparteien nicht trivial.[356] Letztlich muss jedoch schon aufgrund der Zentralität des Datenschutzgrundrechts des Nutzers sowie zur Verringerung der Informationsasymmetrie eine Erkennbarkeit gerade der Parteistellung des Drittanbieters für einen objektiven Beobachter in der Person des Nutzers gewährleistet sein. Dies ist jedoch regelmäßig dann nicht der Fall, wenn, wie es gerade bei Tracking-Instrumenten häufig geschieht,[357] die Datenerhebung durch den Drittanbieter für den durchschnittlichen Nutzer völlig unbemerkt abläuft. Gleiches gilt für eine etwaige Weiterleitung von Daten an Dritte.

Der konkludente Abschluss eines mehrseitigen Vertrages unter Einbeziehung von Drittanbietern dürfte daher, gemessen an den §§ 133, 157 BGB, mit einem angemessenen Interessenausgleich nicht vereinbar sein.[358] Dies hat der Verfasser für die Verpflichtung zur Einwilligung und zur Datenüberlassung im Rahmen bilateraler Verträge zwischen dem Erstanbieter und dem Nutzer an anderer Stelle ausführlich begründet.[359] Im Ergebnis tragen diese Erwägungen auch hinsichtlich des mehrseitigen Vertrages. Zwar hat insbesondere der Drittanbieter wegen der potenziellen datenschutzrechtlichen Legitimationswirkung ein erhebliches Interesse an einer derartigen Gestaltung. Demgegenüber erscheint jedoch das Interesse des Nutzers vorrangig, Vertragsbeziehungen nur mit solchen Parteien einzugehen, mit deren Parteistellung er vernünftigerweise rechnen konnte und die ihm gegenüber ausdrücklich benannt wurden.[360] Dies

[354] Siehe oben, § 4 B.II.2.b)bb)(2).
[355] Siehe oben, § 4 B.II.3.
[356] Ausführlich *Zwanzger*, Der mehrseitige Vertrag, 2013, 183 ff.
[357] Siehe oben, § 2 A.
[358] Zur Maßgeblichkeit der Interessenlage BGH NJW 1973, 2019 (2020); LG Köln NJW-RR 1993, 1424; *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 157 Rn. 7; *Wendtland*, in: BeckOK BGB, 50. Ed. 2019, § 157 Rn. 14 f.
[359] *Hacker*, ZfPW, 2017, 148 (170 ff.).
[360] Vgl. BGH GRUR 2017, 1269 (1272); BGH NJW 2013, 598 (600).

dient mittelbar auch der Rechtssicherheit durch die klare Abgrenzbarkeit von Vertragspartnern[361] und ist insbesondere zur Beurteilung der datenschutzrechtlichen Risiken durch den Nutzer, und damit zur Reduzierung der in § 3 angesprochenen Informationsasymmetrie, unumgänglich.

Ferner muss auch der Ausgang der Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO berücksichtigt werden, da Konsequenz und Zweck einer vertraglichen Bindung gerade die datenschutzrechtliche Legitimationswirkung wäre. Die datenschutzrechtliche Analyse hat jedoch gezeigt, dass typischerweise in den Fällen der Datenweiterleitung an Dritte und der Datenerhebung durch Dritte das Datenschutzgrundrecht des Nutzers im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO überwiegt.[362] Dies spricht entscheidend dafür, auch einen konkludenten mehrseitigen Vertragsschluss abzulehnen, mit dem letztlich die Kautelen sowohl des datenschutzrechtlichen Einwilligungsregimes als auch von Art. 6 Abs. 1 lit. f DS-GVO (z. B. Art. 21 Abs. 1 DS-GVO) umgangen werden könnten. Schließlich steht es Erstanbieter und Drittanbieter frei, durch entsprechende ausdrückliche Gestaltung der Nutzungsbedingungen die Voraussetzungen für einen mehrseitigen Vertrag zu schaffen, sodass ihre Interessen nicht über Gebühr zurückgestellt werden.

(2) Ausnahmsweise konkludenter Vertragsschluss bei salientem Hinweis

Denkbar wäre es jedoch, dass schon die ausdrückliche Benennung des Drittanbieters als Datenverarbeiter im Rahmen der Datenschutzerklärung oder der Cookie-Richtlinie Grundlage für einen mehrseitigen Vertrag ist. Auch hier muss jedoch gelten, dass gerade die Parteistellung, und die Existenz genau definierter Rechte und Pflichten gegenüber dem Drittanbieter, für einen objektiven Nutzer nur dann erkennbar sein wird, wenn diese jeweils ausdrücklich an geeigneter Stelle in den Nutzungsbedingungen festgehalten werden. Soweit ersichtlich, ist dies bei gegenwärtig im Onlinebereich verwendeten Nutzungsbedingungen nicht der Fall.[363] Die bloße Erwähnung der Datenverarbeitung durch einen konkreten Drittanbieter kann demgegenüber für einen mehrseitigen Vertrag noch nicht ausreichend sein. Lediglich dann, wenn der Hinweis auf die Partei- und Pflichtenstellung des Dritten so salient erfolgt, dass mit einer tatsächlichen Kenntnisnahme des objektiven Beobachters in der Person des Nutzers gerechnet werden muss, kann ein konkludenter mehrseitiger Vertragsschluss unter Einbeziehung des Drittanbieters zustande kommen, je nach Erwerbsform etwa durch Bestellung oder Inbetriebnahme des Geräts durch den Primärnutzer.

---

361 Vgl. *Schubert*, in: MüKo, BGB, 8. Aufl. 2018, § 164 Rn. 24.

362 Siehe oben, § 4 C.I.3.a) und b).

363 Zu den im Rahmen des Projekts untersuchten Nutzungsbedingungen genauer *Hacker*, ZfPW, 2017, 148 (163 Fn. 105 und 169 Fn. 146).

bb) Bilateraler Vertrag mit Drittanbieter kraft Stellvertretung

Ganz entsprechend kann auch der Abschluss eines *eigenständigen* Vertrages zwischen dem Drittanbieter und dem Nutzer, bei dem der Erstanbieter als Stellvertreter (oder Bote) des Drittanbieters auftritt,[364] nur angenommen werden, wenn vertragliche Rechte und Pflichten ausdrücklich benannt werden und die Stellvertretung gemäß dem Offenkundigkeitsprinzip (§ 164 Abs. 2 BGB) offengelegt wird.[365] Die Voraussetzungen für die in teleologischer Reduktion von § 164 Abs. 2 BGB anerkannten Ausnahmen vom Offenkundigkeitsprinzip (Geschäft für den, den es angeht[366]) sind schon aufgrund der komplexen datenschutzrechtlichen Implikationen klarerweise nicht erfüllt.[367] Wenn ein derartiger bilateraler Vertrag *neben* einem dem Vertrag zum Erwerb des IoT-Geräts[368] geschlossen wird,[369] so ist die Annahme eines Vertragsnetzes, wie es für die Koordination verschiedener Akteure etwa in der komplexeren Produktion, im koordinierten Absatz[370] oder in dezentralen Systemen diskutiert wird,[371] aufgrund der mangelnden Gleichordnung der Parteien zwar nicht zwingend, kann jedoch bei einzelnen, hier nicht weiter zu vertiefenden Koodinierungsfragen und Wechselwirkungen zwischen den Parteien als Ausgangspunkt der Analyse sehr ergiebig sein.[372]

---

[364] *Wendehorst*, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, Rechtsgutachten für Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz, 2016, 5 (Agenturmodell); siehe ferner oben, § 5, Fn. 345.

[365] Zum Offenkundigkeitsprinzip statt vieler *Schubert*, in: MüKo, BGB, 8. Aufl. 2018, § 164 Rn. 24; *Schilken*, in: Staudinger, BGB, 2014, Vorbem zu §§ 164 ff Rn. 35.

[366] Dazu etwa *Schubert*, in: MüKo, BGB, 8. Aufl. 2018, § 164 Rn. 126 ff.

[367] So kann nicht angenommen werden, dass es dem Betroffenen gleichgültig ist, wer sein Vertragspartner hinsichtlich der Verarbeitung personenbezogener Daten wird, da hier unterschiedliche Risiken bestehen können; dies wäre für ein verdecktes Geschäft für den, den es angeht, jedoch Voraussetzung, siehe BGH NJW 1955, 587 (590); BGH NJW 2016, 1887 (1888); *Schubert*, in: MüKo, BGB, 8. Aufl. 2018, § 164 Rn. 130; *Schäfer*, in: BeckOK BGB, 50. Ed. 2019, § 164 Rn. 27.

[368] Zur Einordnung des Erwerbs des IoT-Geräts selbst als Kaufvertrag *Grünberger*, AcP 218 (2018), 213 (286); nunmehr grundsätzlich auch, für Waren mit funktional notwendigen „digitalen Elementen", Art. 2 Nr. 1 i. V. m. Nr. 5 sowie die Erwägungsgründe 15–17 der Warenkauf-Richtlinie, sowie der 21. Erwägungsgrund der DIDD-Richtlinie; zu allfälligen Differenzierungen und gemischt-typischen Verträgen, siehe die Nachweise in § 4, Fn. 542.

[369] Zur Frage, ob ein einheitlicher Paketvertrag oder einzelne Verträge geschlossen werden, ausführlich *Heuer-James/Chibanguza/Stücker*, BB 2018, 2818 (2824).

[370] Dazu jeweils *Grundmann*, AcP 207 (2007), 718 (721 ff.).

[371] *Börding et al.*, CR 2017, 134 (136).

[372] Siehe nur *Grundmann*, AcP 207 (2007), 718 (740 ff.) unter Betonung von Generalklauseln und § 313 BGB; ferner, für die Rechtsbeziehungen auf Plattformen und im Internet der Dinge, *Grünberger*, AcP 218 (2018), 213 (282 ff.) mit Betonung des Verbundvertrags.

cc) Vertrag zugunsten Dritter

Gewissermaßen als Minus zu einem mehrseitigen Vertrag können Erstanbieter und Nutzer ferner einen Vertrag zugunsten des Drittanbieters nach § 328 BGB schließen. Dies kann grundsätzlich auch konkludent geschehen, § 328 Abs. 2 BGB.[373] Dann würde dem Drittanbieter ein eigenständiges Forderungsrecht i. S. v. § 241 Abs. 1 BGB, etwa hinsichtlich der Abgabe einer Einwilligung und der Überlassung von Daten, eingeräumt, ohne dass dieser am Vertragsabschluss beteiligt ist und Vertragspartei würde.[374] Auch ein solcher Vertrag kann grundsätzlich die Erlaubniswirkung von Art. 6 Abs. 1 lit. b DS-GVO gegenüber dem Drittanbieter auslösen, da dort nach dem eindeutigen Wortlaut nur Voraussetzung ist, dass die betroffene Person, nicht jedoch der Verantwortliche, Vertragspartei sein muss. Ob solch ein Forderungsrecht eines Dritten angenommen werden kann, ist in Ermangelung einer ausdrücklichen Regelung gem. § 328 Abs. 2 BGB aus den Umständen und dem Zweck des Vertrags zu schließen. Dies entspricht der Vertragsauslegung nach §§ 133, 157 BGB.[375]

Hinsichtlich der datenschutzrechtlichen Konsequenzen eines derartigen Vertrags zugunsten des Drittanbieters ist jedoch ferner zu bemerken, dass dieser nach der hier vertretenen Auffassung der Irrelevanz von Nutzerpflichten im Rahmen von Art. 6 Abs. 1 lit. b DS-GVO[376] ohnehin nur eingeschränkte Wirkung entfaltet. Lediglich bei transparenter, salienter Vereinbarung einer Pflicht zur Einwilligung und zur Überlassung entsprechender Daten kann auch nach Widerruf der Einwilligung typischerweise ein Überwiegen der Interessen des Drittanbieters bei der Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO angenommen werden.[377] Schon eine Aufnahme derartiger Pflichten lediglich in die (nicht salienten) Nutzungsbedingungen steht einer derartigen Legitimationswirkung jedoch aus datenschutzrechtlicher Perspektive entgegen.[378]

Daher sind die datenschutzrechtlichen Konsequenzen eines derartigen Vertrags zugunsten des Drittanbieters deutlich weniger weitreichend als jene eines mehrseitigen oder bilateralen Vertrages mit dem Drittanbieter. Nichtsdestoweniger spricht auch hier die Erkennbarkeit des Inhabers eines eigenständigen Forderungsrechts sowie die Vertragsgestaltungsmöglichkeit durch das Zusammenwirken von Erstanbieter und Drittanbieter entscheidend dafür, einen konkludenten Vertrag zugunsten des Drittanbieters regelmäßig abzulehnen. Insofern gilt das soeben zur Vertragsauslegung Gesagte entsprechend. Bei dem

[373] BGH NJW 1991, 2209 (2209); *Janoschek*, in: BeckOK BGB, 50. Ed. 2019, § 328 Rn. 11; *Klumpp*, in: Staudinger, BGB, 2015, § 328 Rn. 84.

[374] BGH NJW 2005, 3778 (3778); *Klumpp*, in: Staudinger, BGB, 2015, Vorbem zu § 328 ff Rn. 4, 8; *Gottwald*, in: MüKo, BGB, 8. Aufl. 2019, § 328 Rn. 1, 25; *Janoschek*, in: BeckOK BGB, 50. Ed. 2019, § 328 Rn. 1, 9.

[375] *Gottwald*, in: MüKo, BGB, 8. Aufl. 2019, § 328 Rn. 33; *Klumpp*, in: Staudinger, BGB, 2015, § 328 Rn. 84.

[376] Siehe oben, § 4 B.II.2.b)bb)(2).

[377] Siehe oben, § 4 C.I.2.c)bb)(2).

[378] Siehe oben, § 4 C.I.2.c)bb)(2).

Vertrag zugunsten Dritter handelt es sich zudem um eine atypische Vertragsgestaltung,[379] mit welcher der Nutzer nicht rechnen muss. Denn der Erstanbieter handelt nicht lediglich im Interesse des Dritten,[380] sondern auch, und für den Nutzer primär erkennbar, im Eigeninteresse. Auch die drittbegünstigende Klausel muss in diesem Fall daher ausdrücklich, unter Benennung der konkreten Rechtsstellung des Drittanbieters, vereinbart werden. Denn anders als etwa bei dem Abschluss eines Sparvertrags zugunsten einer dritten Person[381] liegt für den Versprechenden, den Nutzer, der Drittbezug bei der Datenweiterleitung oder Tracking-Instrumenten gerade nicht auf der Hand. Diese Beschränkung auf eine ausdrückliche Anordnung des drittbegünstigenden Forderungsrechts ist der Rechtsordnung nicht fremd, sie gilt etwa auch bei Unterhaltsverträgen.[382]

dd) Bedingung zugunsten Dritter

Im Rahmen bilateraler Verträge zwischen Erstanbieter und Nutzer, bei denen Daten als Gegenleistung fungieren, ist bei Stillschweigen des Vertrags über eine Verpflichtung zur Einwilligung und zur Datenüberlassung nach hier vertretener Auffassung regelmäßig lediglich eine konkludente Bedingung dahingehend anzunehmen, dass die kontinuierliche Datenüberlassung (und, soweit datenschutzrechtlich erforderlich, auch die Einwilligung) Voraussetzung für die Wirksamkeit der Verpflichtung des Erstanbieters zur Erbringung des nachgefragten Angebots sind. Dies wurde andernorts eingehend ausgeführt.[383] Damit erhebt sich die Frage, ob auch die Datenüberlassung gegenüber dem Drittanbieter (inklusive der Datenerhebung unmittelbar durch den Drittanbieter), und gegebenenfalls eine diesbezügliche Einwilligung, konkludente Bedingung für die Erbringung der Leistung des Erstanbieters sein können. Grundsätzlich steht es den Parteien im Rahmen der Vertragsfreiheit frei, auch Bedingungen zu vereinbaren, die als Potestativbedingungen gegenüber einem Dritten zu erfüllen sind.[384]

(1) Datenschutzrechtliche Irrelevanz der drittbegünstigenden Bedingung

Im konkreten Kontext der digitalen Austauschprozesse kann jedoch eine solche konkludente Bedingung nur angenommen werden, wenn für den Nutzer

379 *Gottwald*, in: MüKo, BGB, 8. Aufl. 2019, § 328 Rn. 20.

380 BGH NJW 1991, 2209 (2209).

381 Zur ausdifferenzierten Rechtsprechung hinsichtlich der Abgrenzung von § 328 BGB von der Stellvertretung einerseits und einem bilateralen Vertrag in eigenem Namen andererseits in diesen Fällen siehe *Grundmann*, in: Staub, HGB, Band 10/1, Bankvertragsrecht, 1. Teil, 5. Aufl. 2016, Rn. 224; *Gottwald*, in: MüKo, BGB, 8. Aufl. 2019, § 328 Rn. 60 f.; OLG Düsseldorf NJW-RR 1992, 625; OLG Zweibrücken NJW 1989, 2546.

382 BGH NJW-RR 1986, 428.

383 *Hacker*, ZfPW 2019, 148 (170 ff.).

384 Vgl. BGH NJW-RR 1996, 1167; *Westermann*, in: MüKo, BGB, 8. Aufl. 2018, § 158 Rn. 19.

bei Abschluss des Vertrages die Datenüberlassung an den Drittanbieter hinreichend erkennbar ist. Diese nutzerseitige Bedingung entfaltet allerdings, ebenso wie Nutzerpflichten, nach hier vertretener Auffassung keine datenschutzrechtliche Legitimationswirkung im Rahmen von Art. 6 Abs. 1 lit. b DS-GVO.[385] Auch für die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO ist sie ohne Belang, da bei Nichterfüllung die Leistungserbringung ohnehin eingestellt werden kann und der Nutzer sich vor allem nicht einmal initial zu einer längerfristigen Datenüberlassung oder Aufrechterhaltung einer Einwilligung verpflichtet hat. Damit ist die Annahme einer derartigen Bedingung in datenschutzrechtlicher Hinsicht letztlich irrelevant.

(2) Folgen für die Vertragsauslegung

Die Auslegung des Vertrags zwischen Erstanbieter und Nutzer muss daher, anders als bei einer echten Verpflichtung des Nutzers,[386] datenschutzrechtliche Konsequenzen nicht berücksichtigen. Demnach ist einerseits zu konstatieren, dass der Erstanbieter ein erhebliches Interesse auch an der Datenüberlassung gegenüber dem Drittanbieter haben kann, da Tracking-Instrumente nur dann vom Erstanbieter in sein Angebot eingebunden werden, wenn dieser davon mittelbar (etwa durch zur Verfügung gestellte Datenanalysen[387] oder auch direkt monetär) profitiert. Auch die Datenüberlassung an Dritte ist daher, ökonomisch betrachtet, Teil der Zahlung mit Daten. Daran haben auch Nutzer mit niedrigen Datenschutzpräferenzen zur Erweiterung ihrer Budgetrestriktionen ein erhebliches Interesse. Andererseits ist die Datenüberlassung an Dritte für Nutzer mit stark ausgeprägten Datenschutzpräferenzen besonders misslich. Zwar können diese regelmäßig nicht legitimerweise erwarten, ohne jegliche Gegenleistung in den Genuss des Angebots zu kommen, weshalb regelmäßig eine konkludente Bedingung hinsichtlich der Überlassung von Daten an den Erstanbieter angenommen werden muss.[388]

Hinsichtlich Drittanbietern jedoch bietet sich als angemessener Interessenausgleich im Rahmen der Vertragsauslegung an, eine konkludente Bedingung nur dann anzunehmen, wenn die Datenüberlassung an diese Dritten transparent zum Zeitpunkt des Vertragsschlusses kommuniziert wird. Dies kann etwa durch Cookie-Banner, welche den Drittbezug offenlegen, oder auch *tracking walls*, welche mit klaren Informationen über die Drittanbieter versehen sind, erfolgen. Wenn jedoch die Weiterleitung an Dritte oder die Erhebung durch diese unbemerkt von den Durchschnittsnutzern erfolgt, so muss auch eine konkludente Bedingung letztlich verneint werden, weil diese zwar keine daten-

[385] Siehe oben, Text bei § 4, Fn. 610.

[386] Zu deren, freilich beschränkter, datenschutzrechtlicher Relevanz siehe oben, § 4 C.I.2.c)bb)(2).

[387] Siehe etwa oben, Text bei § 4, Fn. 287.

[388] Siehe nochmals *Hacker*, ZfPW 2019, 148 (170 ff.).

schutzrechtliche Legitimationswirkung entfaltet, unbemerktes Drittanbieter-Tracking jedoch die informationelle Selbstbestimmung in besonderem Maße gefährdet und die dahingehenden Interessen daher nur sehr vermindert schützenswert sind. Ausreichend dürfte angesichts der mangelnden Legitimationswirkung allerdings noch die konkrete Benennung der Drittanbieter in den Nutzungsbedingungen, der Datenschutzrichtlinie oder der Cookie-Richtlinie sein (vorbehaltlich einer AGB-rechtlichen Wirksamkeitskontrolle[389]), die dann von Informationsintermediären ausgewertet werden können.[390] Durch derartige Gestaltung können die Anbieter ihre Dienste vertraglich an die Überlassung von Daten an Dritte und gegebenenfalls diesbezügliche Einwilligungen koppeln. Die datenschutzrechtliche (Un-)Zulässigkeit dieser Verarbeitungen, auch im Lichte von Art. 7 Abs. 4 DS-GVO,[391] wird dadurch allerdings nicht tangiert. Ob hingegen eine datenschutzrechtliche Unzulässigkeit auf die Wirksamkeit der Klausel oder des Vertrags insgesamt durchschlägt, ist noch eingehend zu untersuchen.[392]

ee) Zusammenfassung zur Einbeziehung von Drittanbietern

Insgesamt ermöglicht das Vertragsrecht daher eine flexible Einbeziehung von Drittanbietern in verschiedenen Formen, sofern diese Einbeziehung hinreichend transparent gemacht wird und bei genuinen vertraglichen Verpflichtungen des Nutzers oder des Drittanbieters eine ausdrückliche Vereinbarung erfolgt.

b) Einbeziehung von Drittnutzern und unbeteiligten Dritten

Auch hinsichtlich des dritten Leitfalls, der Datenerhebung bei Dritten (zum Beispiel bei der Aufzeichnung von Gesprächen mit Unbeteiligten durch ein IoT-Gerät), haben Anbieter ein erhebliches Interesse an einer vertraglichen Bindung, die datenschutzrechtliche Legitimationswirkung entfalten könnte. Umgekehrt kann aber auch der Dritte nach Wegen suchen, von der Vertragsposition des Primärnutzers zu profitieren.

aa) Eigener Vertrag kraft Nutzung

Typischerweise wird ein IoT-Gerät von einem Primärnutzer erworben, der auch einen Erwerbs- und/oder Nutzungsvertrag zumindest mit dem Veräußerer des jeweiligen IoT-Geräts (Erstanbieter[393]), potenziell aber auch, wie gesehen, mit den Anbietern der jeweiligen weiteren Dienste abschließt.[394] Dass auf

[389] Dazu unten, § 5 C.II.1.e)cc).
[390] Siehe oben, § 4 B.I.5.b).
[391] Dazu oben, § 4 B.I.3.a)dd)(5)(b).
[392] Siehe unten, § 5 C.I.
[393] Zum Begriff oben, § 5, Fn. 338.
[394] Siehe bereits § 5, Fn. 368 zur vertragstypologischen Einordnung und § 5, Fn. 351 zur Frage des Verhältnisses dieser Nutzungsverträge untereinander.

beiden Seiten mehrere Akteure auftreten können, mag zu komplexeren, zum Teil mehrseitigen Vertragsverhältnissen führen,[395] spricht jedoch nicht grundsätzlich gegen die Annahme eines Nutzungsvertrags oder mehrerer Nutzungsverträge, die Grundlage für eine vertragserforderliche Datenverarbeitung sind. Besondere Probleme stellen sich jedoch bei der Involvierung Dritter auf Nutzerseite, die nicht Parteien des ursprünglichen Erwerbs- bzw. Nutzungsvertrags waren. Ausgeschlossen ist von vornherein ein Vertrag zulasten dieser Dritten, in dem ihnen Duldungspflichten hinsichtlich der Datenverarbeitung auferlegt werden, da dies nach zutreffender Ansicht mit der negativen Privatautonomie der Dritten nicht vereinbar ist.[396] Allerdings ist denkbar, dass die Dritten einen eigenen Vertrag mit Anbietern digitaler Leistungen (dem oder den datenschutzrechtlich Verantwortlichen) kraft Nutzung des Geräts abschließen. Hier ist zunächst danach zu differenzieren, ob eine bewusste Nutzung des IoT-Geräts bzw. der IoT-Infrastruktur erfolgt oder lediglich Daten von Unbeteiligten verarbeitet werden.

(1) Bewusste Nutzung

Entscheidet sich eine Person für die bewusste Nutzung eines IoT-Geräts, so kann darin, je nach Intensität der Nutzung und Typ des Geräts, potenziell der Abschluss eines Nutzungsvertrags mit dem Anbieter der jeweiligen Dienste liegen.

(a) Angebot des Anbieters

Daran hat der Anbieter jedenfalls dann, wenn das Gerät dem Dritten vom primär Nutzungsberechtigten zur Nutzung überlassen wurde, ein erhebliches Interesse. Zwar entstehen infolge des Vertragsschlusses auch vertragliche Pflichten gegenüber dem Dritten. Es ist jedoch jedenfalls grundsätzlich nicht ersichtlich, dass der oder die Anbieter diese gegenüber Dritten nicht gleichermaßen wie gegenüber dem Primärnutzer erfüllen könnten oder wollten. Lieferengpässe[397] bestehen bei digitalen Gütern üblicherweise nicht. Eine besondere Bonitätsprüfung, wie sie im Falle von monetär zu bezahlenden Angeboten auf einer Webseite oder in einem Schaufenster als Argument für eine bloße *invitatio ad offerendum* des Verkäufers angeführt wird,[398] dürfte regelmäßig aus An-

[395] Siehe die Analyse bei *Solmecke/Vondrlik*, MMR 2013, 755 (755 ff.); *Heuer-James/Chibanguza/Stücker*, BB 2018, 2818 (2823 ff.), sowie oben, § 5 B.III.2.a)aa).

[396] Siehe nur BGH NJW 2014, 1882 (1883); *Martens*, AcP 177 (1977), 113 (139); *Klumpp*, in: Staudinger, BGB, 2015, Vorbem zu § 328 ff Rn. 53; *Emmerich*, in: MüKo, BGB, 8. Aufl. 2019, § 311 Rn. 2; *Gottwald*, in: MüKo, BGB, 8. Aufl. 2019, § 328 Rn. 261; *Janoschek*, in: Beck-OK BGB, 50. Ed. 2019, § 328 Rn. 5.

[397] Zu diesem Argument etwa AG Butzbach, NJW-RR 2003, 54 (54 f.); *Föhlisch/Stariradeff*, NJW 2016, 353 (357); *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 145 Rn. 14.

[398] Siehe etwa AG Butzbach, NJW-RR 2003, 54 (54); *Föhlisch/Stariradeff*, NJW 2016, 353 (357); *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 145 Rn. 14.

bietersicht entbehrlich sein. Denn diese wird, hinsichtlich des Ersterwerbers, typischerweise bereits durch den Verkäufer anlässlich der initialen Erwerbstransaktion durchgeführt. Drittnutzer jedoch zahlen üblicherweise nicht mit Geld, sondern mit ihren Daten, die freilich grundsätzlich verfügbar sind. Der Anbieter kann auf technologischem Wege, etwa durch *tracking walls*,[399] sicherstellen, dass das Gerät auch nur gegen Überlassung von Daten genutzt werden kann. Schließlich führt, wie gesehen, der Vertragsschluss regelmäßig lediglich zu einer konditionalen Verknüpfung.[400] Der Anbieter kann daher die Leistung einstellen, sofern keine oder lediglich fehlerhafte Daten überlassen werden. Sofern einzelne Anbieter abweichend von dieser grundsätzlichen Analyse kein Interesse an einem immediaten Vertragsschluss mit Drittnutzern haben, können sie eine Zugangssperre oder ein Registrierungsmodul in den meisten Fällen unproblematisch auf technischem Wege einbauen. Ferner kann ein Hinweis auf dem Gerät angebracht werden, dass ein Vertragsschluss durch Nutzung abgelehnt wird.[401]

Wenn hingegen die Nutzung durch Dritte ohne Einschränkungen möglich ist (etwa bei einem Musikgerät, das anhand ermittelter musikalischer Präferenzen des Nutzers eine individuelle Playlist zusammenstellt) und auch kein entgegenstehender Hinweis sichtbar angebracht ist, so dürfte in dem Inverkehrbringen des Produkts zugleich gem. § 145 BGB ein Angebot *ad incertas personas* liegen, das Produkt bestimmungsgemäß unter Abschluss eines Nutzungsvertrags zu gebrauchen. Dieser Nutzungsvertrag, der hier nur hinsichtlich seiner datenschutzrechtlichen Relevanz untersucht werden soll, entspricht regelmäßig dem Interesse des Anbieters, da er wiederum Grundlage einer Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO sein kann.[402] Zugleich folgt aus dieser datenschutzrechtlichen Relevanz, sowie den Haftungsrisiken bei Nutzung des Produkts durch Dritte, dass in der Regel ein Angebot gerich-

[399] Dazu oben, Text bei § 4, Fn. 625, auch zur datenschutzrechtlichen Zulässigkeit.

[400] Siehe oben, § 5 B.2.d).

[401] BMW ConnectedDrive macht etwa in den AGB bei Weiterveräußerung eines vernetzten Fahrzeugs die Vertragsübernahme von der Zustimmung durch BMW und der Löschung der Primärnutzerdaten abhängig, dazu *Metzger*, GRUR 2019, 129 (133). Dies kann bei der Frage des konkludenten Angebots eines Nutzungsvertrags berücksichtigt werden, wenn die AGB öffentlich verfügbar sind und im Rahmen des objektivierten Empfängerhorizonts mit einer Kenntnisnahme des Hinweises auf die AGB gerechnet werden kann, vgl. § 305 Abs. 2 BGB. Wenn allerdings eine Nutzung ohne Zustimmung des Anbieters durch Dritte stattfindet, so ist trotz dieser Regelung zu fragen, ob eine vertragliche Bindung zum Drittnutzer (nicht notwendig eine komplette Vertragsübernahme) den Interessen des Anbieters nicht doch eher entspricht als eine Regelung des Verhältnisses rein auf Grundlage gesetzlicher Schuldverhältnisse. Dies ist letztlich eine Frage des Einzelfalls.

[402] Anders kann der Fall etwa zu beurteilen sein, wenn eine datenschutzrechtliche Legitimationswirkung ausscheidet, etwa weil sensitive Daten nach Art. 9 DS-GVO verarbeitet werden, zum Beispiel Gesundheitsdaten durch eine sensorbetriebene Zahnbürste. Dann besteht jedenfalls in datenschutzrechtlicher Hinsicht kein Interesse des Anbieters an einem separaten Nutzungsvertrag.

tet auf eine vertragliche Bindung, und nicht lediglich ein Gefälligkeitsverhältnis,[403] angenommen werden muss.

(b) Annahme durch den Drittnutzer

Problematisch ist dann jedoch typischerweise, inwiefern dieses Angebot durch die bloße Nutzung des Geräts bzw. Inanspruchnahme der Dienstleistung auch angenommen wird.[404] Auf den Zugang der Annahmeerklärung wird der Anbieter regelmäßig nach § 151 S. 1 BGB verzichtet haben.[405] Jedenfalls dann, wenn aus den Umständen ersichtlich ist, dass eine dauerhafte bestimmungsgemäße Nutzung intendiert ist (etwa bei Ersterwerb des Geräts vom Verkäufer oder bei Erwerb des Geräts auf dem Sekundärmarkt), wird man von einer konkludenten Annahme des Vertragsangebots ausgehen dürfen. Dann sind regelmäßig auch hinreichende objektive Anhaltspunkte für einen Rechtsbindungswillen und Indizien für ein Erklärungsbewusstsein vorhanden. Dass diese Konstruktion bei Minderjährigen jedenfalls grundsätzlich nur auf Grundlage einer Zustimmung der gesetzlichen Vertreter gelingen kann,[406] wurde bereits erörtert und ist angesichts der besonderen Relevanz des Datenschutzes gerade bei Minderjährigen auch angemessen.

(aa) Bestimmung der Identität des Anbieters

Problematisch erscheint selbst bei längerfristiger bewusster Nutzung jedoch, dass zu den *essentialia negotii* des Nutzungsvertrags auch die Identität des Anbieters gehören dürfte.[407] Zwar hat der Anbieter, wie gesehen, kein signifikantes Interesse an der Kenntnis der Identität des Drittnutzers. Umgekehrt jedoch

[403] Zu den Abgrenzungskriterien BGH NJW-RR 2017, 1479 Rn. 24; *Schäfer*, in: MüKo, BGB, 7. Aufl. 2017, § 662 Rn. 23 f.; diese werden auch durch die DIDD-Richtlinie nicht berührt, siehe Art. 3 Abs. 10 DIDD-Richtlinie, dazu *Metzger*, JZ 2019, 577 (583 f.); für eine vertragliche Bindung angesichts der Haftungsfragen jedenfalls im bilateralen Verhältnis zum Primärnutzer auch *Heun/Assion*, BB 2018, 579 (580); im Ergebnis ebenfalls *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.1.; ferner auch *Hacker*, ZfPW 2019, 148 (158).

[404] Zur (regelmäßig zu bejahenden) Annahme des Angebots durch den Primärnutzer infolge der Nutzung des Geräts, siehe *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.2.

[405] So auch *Metzger*, AcP 216 (2016), 817 (839). Zwar ist bei der Annahme von § 151 S. 1 BGB Zurückhaltung zu üben, da der Antragende dann über Existenz und Identität des Vertragspartners im Dunklen bleiben kann, siehe *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 151 Rn. 2; *Bork*, in: Staudinger, BGB, 2015, § 151 Rn. 11. Allerdings hat der Antragende, wie gesehen, in den hier beleuchteten Konstellationen ein genuines, datenschutzrechtlich begründetes Interesse an dem Zustandekommen eines Vertragsschlusses auch ohne Zugang der konkludenten Annahmeerklärung; zum Erfordernis der Abgabe der Annahmeerklärung bei § 151 S. 1 BGB ausführlich *Singer*, Selbstbestimmung und Verkehrsschutz im Recht der Willenserklärungen, 1995, 161 ff.

[406] Siehe oben, § 4 B.I.3.b)cc)(2).

[407] BGH GRUR 2017, 1269 (1272).

ist die Kenntnis des jeweiligen Anbieters für den Drittnutzer, wie bereits diskutiert, regelmäßig entscheidend, da es gerade um die Verarbeitung personenbezogener Daten und daher regelmäßig anbieterabhängige datenschutzrechtliche Risiken geht.[408] Sofern der einzubeziehende Anbieter mit dem Hersteller identisch ist, ist von einer hinreichenden Kenntnis regelmäßig auszugehen, da der Hersteller typischerweise auf dem Produkt vermerkt ist. Ist der Anbieter, wie etwa bei *third-party tracking* oder bestimmten digitalen Zusatzleistungen, jedoch vom Hersteller verschieden, so wird er nur dann für den Drittnutzer hinreichend bestimmbar sein, wenn er separat auf dem Gerät vermerkt ist. Denkbar ist schließlich noch ein Hinweis auf dem Gerät selbst auf AGB, welche die Identität des Anbieters enthalten, wobei hier bereits die zumutbare Möglichkeit der Kenntnisnahme nach § 305 Abs. 2 Nr. 2 BGB nicht immer gewährleistet sein wird.[409]

(bb) Erklärungsbewusstsein bei kurzzeitiger Nutzung

Noch schwieriger zu beurteilen sind Fälle, in denen zwar eine bewusste, aber lediglich einmalige oder seltene Drittnutzung, etwa anlässlich eines Besuchs bei dem Eigentümer des Geräts, erfolgt. Hier muss nach dem Gerät bzw. der Umgebung differenziert werden. Ein Nutzungsvertrag ist nach hier vertretener Auffassung jedenfalls dann denkbar, wenn die Nutzung des IoT-Geräts, und sei sie auch kurzzeitig, gerade unter bewusster Verwendung seiner vernetzten Komponenten erfolgt.[410] Problematisch ist hier jedoch, dass das Erklärungsbewusstsein des Nutzers fehlen kann,[411] wenn er z. B. subjektiv lediglich von einer rechtlich unverbindlichen, da probeweisen Nutzung des Geräts ausgeht.

α. Mangelndes Erklärungsbewusstsein bei § 151 S. 1 BGB

Nach herrschender Meinung kann fehlendes Erklärungsbewusstsein jedoch partiell kompensiert werden. Erstens muss der Nutzer, sofern objektive Anhaltspunkte für einen Rechtsbindungswillen vorliegen, das Fehlen subjektiven Erklärungsbewusstseins selbst darlegen und beweisen.[412] Zweitens kann auch bei entsprechendem Vortrag das fehlende Erklärungsbewusstsein grundsätzlich überwunden werden, wenn der Nutzer bei Anwendung der im Verkehr erforderlichen Sorgfalt zumindest hätte erkennen und vermeiden können, dass

[408] Siehe oben, § 5 B.III.2.a)aa).

[409] Beim Ersterwerb kann dieser Hinweis freilich auch anderweitig im Rahmen des Vertragsschlusses über eine Webseite oder einen stationären Händler erfolgen; dies betrifft jedoch nur Primärnutzer, nicht Drittnutzer.

[410] Dies ist etwa abzulehnen, wenn ein Besucher lediglich eine eigene Flasche Wein in einen *smart fridge* einstellt, um sie später gekühlt zu entnehmen.

[411] *Metzger*, GRUR 2019, 129 (134).

[412] BGH NJW-RR 1986, 415 (415).

seine Handlung nach der Verkehrssitte als Willenserklärung aufgefasst werden darf und sie der Empfänger auch tatsächlich so verstanden hat.[413]

Die Erkennbarkeit der vertraglichen Bindungswirkung bei Anwendung ordnungsgemäßer Sorgfalt dürfte regelmäßig bei bewusster Nutzung der Vernetzungs- und Datenverarbeitungsfunktion zu bejahen sein. Das tatsächliche Verständnis des Vertragspartners der Handlung als konkludente Willenserklärung wird bei § 151 S. 1 BGB jedoch zumeist fehlen. Dennoch soll nach Ansicht einer Literaturströmung die Erklärungsfahrlässigkeit in diesem Fall genügen, wenn ein objektiver, unbeteiligter Beobachter, auf den es für den Vertragsschluss ohnehin ankommt,[414] das Verhalten als Willenserklärung verstanden hätte.[415] So ließe sich auch die zweideutige Rechtsprechung des BGH verstehen,[416] die bei genauem Hinsehen jedoch ein Erklärungsbewusstsein bei § 151 S. 1 BGB positiv fordert.[417]

Postuliert man hingegen eine Überwindbarkeit fehlenden Erklärungsbewusstseins, bleibt bei § 151 S. 1 BGB unklar, worin genau der Vertrauenstatbestand liegen soll, der die Überwindung des Mangels des Erklärungsbewusstseins rechtfertigt.[418] Nicht umsonst wird im Rahmen der allgemeinen Rechtsscheinshaftung eine Kenntnis des Rechtsscheins durch den Begünstigten gefordert.[419] Zwar erwächst auch dann, wenn der Anbieter die Drittnutzung nicht erkennen kann, ein Interesse des Anbieters an vertraglicher Bindung aus der datenschutzrechtlichen Relevanz des Vorgangs. Allerdings dürfte das rein abstrakte Interesse des Anbieters nicht genügen, um den für die Erklärungsfahrlässigkeit nach der Rechtsprechung erforderlichen Vertrauenstatbestand zu erfüllen, der immerhin der Überwindung der negativen Privat-

---

413 Siehe die Nachweise oben, in § 5, Fn. 270.

414 Infolge der mangelnden Empfangsbedürftigkeit der Annahme nach § 151 S. 1 BGB ist statt auf den objektiven Empfängerhorizont auf das Verständnis eines unbeteiligten, objektiven Dritten abzustellen, siehe BGH NJW 2004, 3699; *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 151 Rn. 9; *Eckert*, in: BeckOK BGB, 50. Ed. 2019, § 151 Rn. 3; *Bork*, in: Staudinger, BGB, 2015, § 151 Rn. 15; *Singer*, in: Staudinger, BGB, 2017, Vorbem §§ 116 ff Rn. 47.

415 *Singer*, in: Staudinger, BGB, 2017, Vorbem §§ 116 ff Rn. 47; *Bork*, in: Staudinger, BGB, 2015 § 151 Rn. 16; *Repgen*, AcP 200 (2000), 533 (553 f.); *Schönfelder*, NJW 2001, 492 (494); im Ergebnis auch *Flume*, AT II, 4. Aufl. 1992, 656.

416 Zu dieser Zweideutigkeit, hinsichtlich der Notwendigkeit des Vorliegens von Erklärungsbewusstsein im Fall von § 151 S. 1 BGB, *Frings*, BB 1996, 809 (809 f.); *Eckhardt*, BB 1996, 1945 (1947).

417 BGH NJW-RR 1986, 415 (415 unter 2.a)bb)); so auch *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 151 Rn. 10; *Scheffer*, NJW 1995, 3166 (3168); *Kleinschmidt*, NJW 2002, 346 (347); kritisch *Singer*, Selbstbestimmung und Verkehrsschutz im Recht der Willenserklärungen, 1995, 166–168; eine Differenzierung zwischen objektiven Anzeichen für einen Rechtsbindungswillen („Annahmewillen") und Erklärungsbewusstsein bei § 151 S. 1 BGB aber ablehnend *Eckhardt*, BB 1996, 1945 (1950).

418 Ähnlich *Eckhardt*, BB 1996, 1945 (1948); *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 151 Rn. 10.

419 Siehe nur *Canaris*, Handelsrecht, 24. Aufl. 2006, § 6 VII; *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, 1971, 507 ff.

autonomie geschuldet ist. Die immer verbleibende Anfechtungsmöglichkeit[420] kann dies nicht gänzlich kompensieren, zumal die Frist („unverzüglich", § 121 Abs. 1 BGB) leicht versäumt werden kann.[421]

β. Besonderheiten im Rahmen digitaler Austauschprozesse

Der Verkehrsschutz erfordert jedoch nach hier vertretener Auffassung dann eine Zurechnung der objektiven Erklärung zum Nutzer, wenn der Anbieter aufgrund der übermittelten Daten erkennen kann, dass nicht der Primärnutzer agiert.[422] In dieser Möglichkeit liegt die Besonderheit der Anwendung von § 151 S. 1 BGB auf digitale Austauschprozesse. Das Wissen von digitalen Verarbeitungsagenten wird dem Anbieter dabei grundsätzlich, sofern es extrahierbar ist, analog § 166 Abs. 1 BGB zugerechnet.[423]

Allerdings ist in einem zweiten Schritt zu fragen, ob die im Rahmen der Einwilligung getroffene Wertung, dass ein mangelndes Einwilligungsbewusstsein nicht durch Verkehrsschutzbelange überwunden werden kann,[424] nicht auf das rechtsgeschäftliche Erklärungsbewusstsein insoweit übertragen werden muss, als es um Verträge im Rahmen von Art. 6 Abs. 1 lit. b DS-GVO geht. Im Rahmen solcher Verträge dürfte jedoch der Verkehrsschutz in stärkerem Maße zu berücksichtigen sein als im Rahmen der datenschutzrechtlichen Einwilligung. Denn erstens wird das Datenschutzgrundrecht hier nur indirekt, durch die Reflexwirkung des Art. 6 Abs. 1 lit. b DS-GVO, tangiert. Zweitens erscheint die Beeinträchtigung des Datenschutzgrundrechts deutlich reduziert, wenn der Nutzer, wie hier vorausgesetzt, bewusst die Vernetzungs- und Datenverarbeitungskomponenten eines IoT-Geräts nutzt. Er mag dann zwar kein subjektives rechtliches Erklärungsbewusstsein haben, muss aber regelmäßig erkennen, dass zur bestimmungsgemäßen Nutzung des Geräts Daten faktisch verarbeitet werden müssen. Daher besteht in diesem Fall kein schutzwürdiges Interesse des Drittnutzers, einer vertragserforderlichen Datenverarbeitung die Rechtmäßigkeit auf Grundlage von Art. 6 Abs. 1 lit. b DS-GVO zu versagen. Dies gilt, wie im nächsten Abschnitt (cc) noch zu erörtern ist, jedoch nur dann, wenn die Handlung *unmissverständlich* auf die Vernetzungs- und Datenverarbeitungskomponente des Geräts bezogen ist.

Daher muss im Ergebnis der Anbieter, sofern das mangelnde Erklärungsbewusstsein anhand von Indizien durch den Nutzer belegt wird, einen konkreten, beispielsweise auf datengetriebener Erkenntnis der Drittnutzung, ba-

---

[420] BGH NJW 1984, 2279.

[421] Insoweit zutreffend *Canaris*, NJW 1984, 2281 (2281 f.).

[422] Für eine völlige Irrelevanz des Verkehrsschutzes bei § 151 S. 1 BGB plädieren hingegen *Eckhardt*, BB 1996, 1945 (1948); *Scheffer*, NJW 1995, 3166 (3168); *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 151 Rn. 10, allerdings ohne Berücksichtigung der datengetriebenen Zuordnungsmöglichkeit.

[423] Dazu genauer *Hacker*, RW 9 (2018), 243 (270 ff.).

[424] Siehe oben, § 5 B.II.2.b).

sierenden Vertrauenstatbestand nachweisen können. Dies ist etwa möglich bei dem Transport eines Drittnutzers mit einem vernetzten und (partiell) autonomen Fahrzeug, bei dem der Insasse Sprachbefehle erteilt und mittels Sprachanalyse die Dritteigenschaft festgestellt wird. Nach dem Gesagten wird man hier von einer Erfüllung des Tatbestands der Annahme ausgehen können, sofern der Vertragspartner für den Nutzer bestimmbar ist.

Nur zur Klarstellung ist schließlich festzuhalten: Werden hierbei Informationspflichten nach Art. 6 Abs. 1 der Verbraucherrechterichtlinie (VRRL[425]) verletzt,[426] so hindert dies den Vertragsschluss nicht,[427] sondern führt allenfalls zu einer Verlängerung der Widerrufsfrist[428] oder der mangelnden Ersatzfähigkeit bestimmter Kosten.[429] Um die Komplexität der Prozesse abzubilden, wird der Anbieter regelmäßig ohnehin versuchen, AGB über informatorische Hinweise in den Vertrag einzubeziehen[430] und auf diese Weise auch die Informationspflichten zu erfüllen.

(cc) Unmissverständlichkeit der Annahme bei nicht primär nutzungsorientierter Handlung

Einen gesondert zu beurteilenden Fall stellt es schließlich dar, wenn die Berührungspunkte mit dem IoT-Gerät oder der vernetzten Umgebung lediglich anlässlich einer mit anderer Zielrichtung als der Nutzung der IoT-Infrastruktur verfolgten, insgesamt daher mehrdeutigen Handlung erfolgen. Dies ist insbesondere dann der Fall, wenn vernetzte Infrastruktur genutzt wird. So wird man in dem kurzzeitigen Gastaufenthalt in einer Smart City keine konkludente Annahme eines möglicherweise angebotenen Nutzungsvertrags mit den datenschutzrechtlich Verantwortlichen sehen können. Denn hier bestehen bereits keine hinreichenden objektiven Anhaltspunkte für einen Rechtsbindungswillen, wenn die Nutzung eigentlich zu anderen Zwecken (etwa den Besuch von Freunden, die in der Smart City wohnen) erfolgt.[431] Die Fälle unterscheiden sich erheblich von jenen der Nutzung frei zugänglicher öffentlicher Verkehrsmittel, in denen ein konkludenter Beförderungsvertrag durch die Nutzung des Verkehrsmittels angenommen wird.[432] Denn dort hat der Beförderte regelmäßig kein schutzwürdiges Interesse daran, die angebotene Leistung ohne Entrichtung eines vertraglichen monetären Entgelts zu nutzen. Zwar ließe sich

[425] Richtlinie 2011/83/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 über die Rechte der Verbraucher, ABl. 2011 L 304/64.

[426] Siehe dazu etwa *de Franceschi*, in: Schmidt-Kessel/Kramme (Hrsg.), Geschäftsmodelle in der digitalen Welt, 2017, 113 (126 ff.); *Mischau*, ZEuP 2020, 335 (354 ff.).

[427] Siehe nur *Wendehorst*, in: MüKo, BGB, 8. Aufl. 2019, § 312d Rn. 145–147.

[428] Siehe Art. 10 Abs. 1 VRRL, § 356 Abs. 3 BGB.

[429] Art. 6 Abs. 6 VRRL, § 312e, 357 Abs. 6–8 BGB.

[430] Vgl. *Heun/Assion*, CR 2015, 812 (815).

[431] Vgl. *Singer*, Selbstbestimmung und Verkehrsschutz im Recht der Willenserklärungen, 1995, 146 f., 151 f.

[432] Vgl. AG Mühlheim, NJW-RR 1989, 175 (176); *Harder*, NJW 1990, 857 (858).

in ähnlicher Weise argumentieren, dass auch die Annehmlichkeiten einer Smart City nur gegen Zahlung durch Daten nutzbar sein sollten. Den Anbietern steht es jedoch vertragsrechtlich frei, bestimmte Dienste nur bei Überlassung von Daten freizuschalten. Letztlich überwiegt hier das Interesse des Nutzers, einen Zugriff auf seine grundrechtlich geschützten Daten nicht über den Umweg eines Nutzungsvertrags freigeben zu müssen. Dem Anbieter bleibt immerhin der Rückgriff auf Art. 6 Abs. 1 lit. f DS-GVO. Gegen die Annahme eines Vertragsschlusses in dieser Konstellation spricht auch der Abgleich mit dem Einwilligungsregime der DS-GVO. Aufgrund der legitimierenden Wirkung des Vertrags stellt dieser immerhin ein Einwilligungssubstitut dar. Dann liegt es jedoch nahe, wie bei der Einwilligung,[433] eine objektiv unmissverständliche Willenserklärung des Nutzers zu fordern. Dies führt letztlich zu einem schonenden Ausgleich der negativen Privatautonomie und des Datenschutzgrundrechts der betroffenen Person einerseits mit den Verkehrsschutzinteressen des Verantwortlichen andererseits. Auch aus ökonomischer Perspektive wird dadurch einer Verschärfung der in § 3 angesprochenen Informationsasymmetrie durch hochgradig uninformierte, weil so vom Nutzer nicht intendierte, Vertragsschlüsse Einhalt geboten. Wie gesehen, kann im Rahmen einer vertraglichen Beziehung ein subjektiv fehlendes Erklärungsbewusstsein zwar grundsätzlich durch Verkehrsschutzinteressen, anders als bei der Einwilligung, überwunden werden. Die Interessen der betroffenen Person müssen jedoch nur dann zurücktreten, wenn der Wille zur Nutzung der Datenverarbeitungskapazitäten objektiv unmissverständlich vorliegt. Ist dies nicht der Fall, so erscheint das Verkehrsschutzinteresse deutlich gemindert, da aus der Handlung dann nicht objektiv eindeutig auf einen Rechtsbindungswillen geschlossen werden kann. Ferner steht dem Verantwortlichen der Weg über Art. 6 Abs. 1 lit. f DS-GVO grundsätzlich offen. Die Wertung von Art. 4 Nr. 11 DS-GVO (Unmissverständlichkeitsgebot) und des 32. Erwägungsgrunds der DS-GVO stützt diese Ansicht.

Der objektiv bestimmbare Rechtsbindungswille muss also besonders klar zutage treten. Diese Wertung deckt sich auch mit den auch in der allgemeinen Rechtsgeschäftslehre vertretenen strengen Anforderungen an den objektiven Erklärungstatbestand bei konkludenten Willenserklärungen.[434] Ein unmissverständlicher Rechtsbindungswille kann jedoch regelmäßig in einer mit anderer Zielsetzung erfolgten Handlung, wie auch bei der Einwilligung,[435] nicht erblickt werden. Dass die DS-GVO selbst kein Kriterium der Unmissverständlichkeit bei Art. 6 Abs. 1 lit. b DS-GVO enthält, spricht auch nicht gegen dessen Annahme im nationalen Vertragsrecht. Denn der Vertragsschluss selbst fällt in

[433] Dazu oben, § 4 B.I.3.a)aa).

[434] *von Savigny*, System des heutigen Römischen Rechts, Band III, § 131, S. 245 („sicherer Schluß […] von der vorgenommenen Handlung auf das Daseyn des Willens"); *Singer*, Selbstbestimmung und Verkehrsschutz im Recht der Willenserklärungen, 1995, 146 f., 151.

[435] Dazu oben, § 4 B.I.3.a)aa)(1)(a)(bb).

einen von der DS-GVO überhaupt nicht geregelten Bereich, sodass eine direkte Kollision nicht vorliegt. Schon aufgrund der Wertungsparallele mit Art. 4 Nr. 11 DS-GVO muss jedoch auch eine indirekte Kollision durch die Forderung einer unmissverständlichen Handlung nach dem nationalen Vertragsrecht verneint werden. Umgekehrt gilt vielmehr, dass die Voraussetzungen der Einwilligung nicht durch eine lose Handhabung der Voraussetzungen für einwilligungssubstitutierende Verträge im nationalen Recht unterlaufen werden dürfen.

Nach den gleichen Maßstäben dürfte hinsichtlich eines Gastaufenthalts in einem Smart Home zu entscheiden sein, das etwa zu Zwecken einer Abendeinladung besucht wird. Auch hier lässt sich in dem reinen Besuch des Hauses keine eindeutige Annahme eines etwaigen Angebots eines Nutzungsvertrags sehen. Wiederum ist der Verantwortliche auf eine separate Einwilligungserklärung oder die Interessenabwägungsklausel verwiesen.

(c) Lösungsmöglichkeiten

Diese Analyse zeigt, dass dem Abschluss eines Nutzungsvertrags zwischen Anbietern und Drittnutzern eine Reihe von rechtlichen Hindernissen im Weg stehen (mangelnde Identifizierbarkeit des Anbieters; mangelndes Erklärungsbewusstsein des Nutzers; mangelnde Unmissverständlichkeit der Annahmehandlung), sodass ein solcher Vertrag letztlich wohl nur selten wirksam zustande kommen wird. Für Anbieter, die zugleich datenschutzrechtlich Verantwortliche sind, bieten sich hier drei mögliche Auswege an.

Erstens können sie versuchen, eine vertragliche Bindung durch klare Hinweise auf dem Gerät zu bewirken, die sowohl ihre eigene Identität als auch den Vertragsschluss durch Nutzung offenlegen.[436] Jedenfalls die mangelnde Identifizierbarkeit des Anbieters und das mangelnde Erklärungsbewusstsein lassen sich dadurch überwinden; bei der Nutzung vernetzter Infrastruktur dürften derartige einseitige Hinweise jedoch nicht reichen, um eine hinreichend unmissverständliche Annahmehandlung zur Entstehung zu bringen.[437] Ferner

[436] Vgl. BGH NJW-RR 1986, 415 (415 f.).

[437] Anders lässt sich allerdings BGH NJW-RR 1986, 415 (415 f.) deuten, wenn eine klare Bedingung der Akzeptanz der Nutzungsbedingungen an den Zutritt gekoppelt ist; kritisch allerdings *Frings*, BB 1996, 809 (810 f.); *Eckhardt*, BB 1996, 1945 (1948). Jedenfalls eine nach außen erkennbar hervortretende Ablehnung des Nutzungsvertrags reicht jedoch dann auch nach der Rechtsprechung aus, um einen objektiven Rechtsbindungswillen zu verneinen, siehe BGH NJW 1990, 1655 (1656); anders noch BGH NJW 1956, 1475. Hier taucht das aus § 242 BGB bekannte Problem der *protestatio facto contraria* wieder auf (siehe etwa BGH NJW 1965, 387 [388]; *Wolf/Neuner*, BGB AT, 11. Aufl. 2016, § 37 Rn. 47; *Medicus/Petersen*, BGB AT, 11. Aufl. 2016, Rn. 249 ff.), freilich mit dem entscheidenden Unterschied zu den sonst diskutierten Fällen, dass es nicht um die Ersparnis der Kosten öffentlichen Nahverkehrs oder mangelnden Beitrag zur Daseinsvorsorge, sondern – faktisch – um die Einwilligung in einen Grundrechtseingriff hinsichtlich des Datengrundrechts geht und, siehe BGH NJW-RR 1986, 1496 (1497), eine andere Deutung der Handlung daher durchaus möglich ist. Daher ist jedenfalls eine *protestatio* als valide anzusehen.

können derartige Hinweise das Gerät weniger benutzerfreundlich erscheinen lassen und die ästhetische Erscheinung beeinträchtigen. Dies dürfte der primäre Grund dafür sein, dass derartige Hinweise gegenwärtig, soweit ersichtlich, wenig verbreitet sind.

Zweitens können die Anbieter auf eine vertragliche Bindung verzichten und statt auf Art. 6 Abs. 1 lit. b DS-GVO auf eine datenschutzrechtliche Erlaubnis nach Art. 6 Abs. 1 lit. f DS-GVO setzen. Bei einer bewussten Nutzung wird hinsichtlich der Daten, die zur bestimmungsgemäßen Nutzung des Geräts erforderlich sind, die Interessenabwägung regelmäßig zu Gunsten des Verantwortlichen ausfallen. Im Einzelfall kann jedoch schwer zu bestimmen sein, welche Datenverarbeitungen noch technisch zur Nutzung der Infrastruktur notwendig sind,[438] etwa im Rahmen einer Smart City. Datenweiterleitung zu Zwecken personalisierter Werbung und *third-party tracking* ist auf diesem Weg jedoch grundsätzlich nicht zu rechtfertigen.[439]

Schließlich mögen im Einzelfall nicht personenbezogene Daten vorliegen. Dies ist etwa denkbar, wenn ein IoT-Gerät (etwa eine sensorgetriebene Zahnbürste) einmalig von einem bisher für den oder die Anbieter unbekannten Nutzer verwendet wird. Mit zunehmender Vernetzung verschiedener Alltagsgegenstände und Integration der diesbezüglichen Datenbanken wird jedoch ein Personenbezug auch bei kurzfristiger Exposition dem Gerät oder der Applikation gegenüber immer wahrscheinlicher.[440]

(2) Erhebung bei Unbeteiligten

Schon grundsätzlich kommt die Annahme eines Angebots auf Abschluss eines Nutzungsvertrags nicht in Betracht, wenn bei einer unbeteiligten Person Daten erhoben werden, bei der für einen objektiven Beobachter ersichtlich ist,[441] dass keine eigene Nutzung des Geräts intendiert ist. Dies betrifft etwa Sprachmitschnitte von Wohnungsbesuchern durch IoT-Geräte im häuslichen Kontext oder auch die Erfassung von Personen außerhalb eines vernetzten und (partiell) autonomen Fahrzeugs.

(3) Zusammenfassung zum eigenen Vertrag mit Drittnutzern

Damit gelingt eine Abmilderung der datenschutzrechtlichen Problematik der Datenerhebung bei Drittennutzern über die Annahme eines konkludenten Nutzungsvertrags allenfalls dann, wenn objektiv ersichtlich ist, dass die betreffende Person das Gerät bewusst bestimmungsgemäß unter Verwendung der Vernetzungseigenschaften nutzt. Auch diese Lösung versagt jedoch bei Minderjährigen sowie bei sensitiven Daten im Sinne von Art. 9 DS-GVO. Dies ist

438 *Engeler/Felber*, ZD 2017, 251 (255); *Engeler*, ZD 2018, 55 (61).
439 Siehe oben, § 4 C.I.3.a) und b).
440 Siehe oben, § 4 A.II.2.a)aa)(3).
441 Siehe § 5, Fn. 414.

allerdings aufgrund der klaren gesetzlichen Wertung hinzunehmen und letztlich auch gerechtfertigt.

bb) Vertrag zugunsten Dritter

In umgekehrter Interessenrichtung lässt sich fragen, welche Instrumente zur Verfügung stehen, um unbeteiligten Dritten, zusätzlich zu dem datenschutzrechtlichen Schutzregime, vertragliche Ansprüche gegen die datenschutzrechtlich Verantwortlichen zu sichern. In Ermangelung einer ausdrücklichen Abrede ist hier wiederum gem. § 328 Abs. 2 BGB aus den Umständen und dem Zweck des Vertrags zu entnehmen, ob eigene Nutzungsrechte der Dritten intendiert sind. Dies kann etwa relevant sein, wenn dem Dritten aus einer Fehlfunktion des Geräts ein Schaden entsteht und er Schadensersatz verlangen möchte.[442]

Die Annahme eines eigenen Forderungsrechts des Dritten gerichtet auf Nutzung des Geräts und der damit verbundenen Dienste ist jedoch allenfalls in den Fällen zu bejahen, in denen der Dritte klar definiert ist (zum Beispiel Ehegatte oder Lebenspartner) und dessen Nutzungsinteresse auch bei Vertragsschluss dem Anbieter gegenüber offengelegt wird. Hinsichtlich noch unbestimmter und auch nicht bestimmbarer Dritter kann kein Vertrag zugunsten Dritter abgeschlossen werden.[443] Zwar genügt für die Bestimmbarkeit, dass der Leistungsanspruch dem *jeweiligen* Nutzer zustehen soll.[444] Hier bietet jedoch der eigenständige Vertrag, der konkludent gegebenenfalls durch die Nutzung des Geräts abgeschlossen wird, den Vorteil, dass der Anbieter jeweils durch Registrierungsmaßnahmen einzelfallbezogen entscheiden kann, ob er einen Vertrag eingehen möchte oder nicht. Ferner können im Rahmen dieses Vertrags Gegenleistungspflichten des Nutzers, anders als beim isolierten drittbegünstigenden Forderungsrecht,[445] berücksichtigt werden. Daher wird man ein eigenständiges Nutzungsrecht einer aus einem zum Zeitpunkt des Vertragsschlusses noch unbestimmten Personenkreis stammenden Person gem. § 328 Abs. 2 BGB grundsätzlich verneinen müssen und auch bei bereits bestimmten Dritten nur sehr zurückhaltend bejahen können.

cc) Vertrag mit Schutzwirkung zugunsten Dritter

Ferner kann der Dritte nach den Grundsätzen des Vertrags mit Schutzwirkung zugunsten Dritter so in das Schuldverhältnis zwischen dem Anbieter und dem Primärnutzer einbezogen sein, dass die dem Primärnutzer gegenüber beste-

[442] Dem Dritten stehen eigene schadensersatzrechtliche Sekundäransprüche beim Vertrag zugunsten Dritter zu, siehe nur *Janoschek*, in: BeckOK BGB, 50. Ed. 2019, § 328 Rn. 20.

[443] BGH NJW NJW-RR 2008, 683 Rn. 10; *Gottwald*, in: MüKo, BGB, 8. Aufl. 2019, § 328 Rn. 24.

[444] Vgl. BGH NJW 1979, 2036 (2036).

[445] BGH NJW 2005, 3778 (3778).

henden Pflichten gemäß § 241 Abs. 2 BGB auch gegenüber dem Dritten zu beachten sind.[446]

(1) Tatbestandliche Voraussetzungen

Voraussetzung ist nach den hergebrachten Kriterien der Rechtsprechung zunächst, dass der Dritte mit der Leistung bestimmungsgemäß wie der Vertragspartner in Berührung kommt (Leistungsnähe).[447] Dieses Kriterium dürfte typischerweise erfüllt sein, wenn das IoT-Gerät dem Dritten gegenüber ähnliche Analysewirkung entfaltet, etwa ähnliche Daten erhebt, und der Dritte sich mit Willen des Primärnutzers im Erhebungsbereich des Geräts aufhält.[448] Denn dann treffen ihn etwaige datenschutzrechtliche Implikationen ebenso wie den Primärnutzer.[449] Zweitens muss der Dritte dem Gläubiger der Schutzpflichten hinreichend nahestehen oder der Gläubiger zumindest ein berechtigtes Interesse an der Einbeziehung des Dritten haben.[450] Dies ist insbesondere bei Kindern des Primärnutzers oder sonstigen Rechtsverhältnissen mit personenrechtlichem Einschlag regelmäßig zu bejahen.[451] Bei Gästen eines Smart Home wird man ein schutzwürdiges Interesse des Primärgläubigers ebenfalls bejahen können, da sich die Gäste in seine Obhut begeben und der Zweck des Nutzungsvertrags eines Smart Home typischerweise auch den Schutz von Gästen, zumindest implizit im Wege ergänzender Vertragsauslegung, berücksichtigen wird.[452]

Drittens muss der Einbezug des Dritten für den Anbieter erkennbar sein,[453] was bei gegenüber Dritten nicht weiter abgeschirmten IoT-Geräten jedoch typischerweise der Fall sein wird. Allerdings wird, um eine übergebührliche Ausweitung der vertraglichen Haftung unter Überspielung der Grenzen des Deliktsrechts zu verhindern, einschränkend gefordert, dass der Personenkreis abgegrenzt sein muss.[454] Daher wurde eine Einbeziehung des nicht weiter spezifizierten Endverbrauchers in den Vertrag zwischen Hersteller und Abnehmer eines Produkts abgelehnt.[455] In der Tat würden damit die Voraussetzungen

[446] Vgl. *Klumpp*, in: Staudinger, BGB, 2015, § 328 Rn. 89.
[447] BGH NJW 2001, 3115 (3116); *Klumpp*, in: Staudinger, BGB, 2015, § 328 Rn. 111.
[448] Vgl. *Gottwald*, in: MüKo, BGB, 8. Aufl. 2019, § 328 Rn. 184.
[449] Vgl. BGH NJW 2001, 3115 (3116); *Janoschek*, in: BeckOK BGB, 50. Ed. 2019, § 328 Rn. 53.
[450] BGH NJW 1996, 2927 (2928); BGH NJW 2001, 3115 (3116); *Klumpp*, in: Staudinger, BGB, 2015, § 328 Rn. 117.
[451] BGH NJW 2001, 3115 (3116).
[452] Zu dieser ergänzenden Vertragsauslegung allgemein BGH NJW 2001, 3115 (3116).
[453] BGH NJW 2014, 2577.
[454] BGH NJW 1977, 2073 (2074); *Gottwald*, in: MüKo, BGB, 8. Aufl. 2019, § 328 Rn. 190; *Klumpp*, in: Staudinger, BGB, 2015, § 328 Rn. 121.
[455] BGH NJW 1969, 269 (272), wenngleich mit anderer Begründung (Verneinung der Gläubigernähe auf Grundlage der engeren Voraussetzungen der älteren Rechtsprechung); zustimmend infolge mangelnder Erkennbarkeit der geschützten Personen *Gottwald*, in: MüKo, BGB, 8. Aufl. 2019, § 328 Rn. 190; *Klumpp*, in: Staudinger, BGB, 2015, § 328 Rn. 280.

der Produkthaftung unterminiert.[456] Andererseits wurde der Kreis der Teilnehmer einer Veranstaltung bei einer Saalnutzung noch für ausreichend abgegrenzt gehalten.[457] Letztlich ist entscheidend, ob der Personenkreis für den Schuldner kalkulierbar und das Risiko damit angemessen versicherbar ist.[458] Dies ist jedenfalls für Familienmitglieder zu bejahen. Hinsichtlich der Gäste eines Smart Home dürfte ebenfalls noch keine nur unangemessen versicherbare Anzahl von Personen erreicht sein. Anders verhält es sich bei den Besuchern einer Smart City oder den Passanten außerhalb eines autonomen Fahrzeugs.

Besonders zu hinterfragen ist viertens die Schutzbedürftigkeit des Dritten. Darunter wird grundsätzlich das Fehlen eines vertraglichen, gleichwertigen Anspruchs gegen den Schuldner oder eine sonstige Person verstanden.[459] Regelmäßig hat der Dritte zwar datenschutzrechtliche Ansprüche gegen den Anbieter. Diese umfassen jedoch keinen Schutz vor Schäden, die aus einer nicht datenschutzrelevanten Fehlfunktion des Geräts resultieren. Jedenfalls insoweit ist die Schutzbedürftigkeit daher zu bejahen.[460]

(2) Vereinbarkeit mit Unionsrecht

Auch der Anwendungsvorrang des Unionsrechts steht einer Einbeziehung Dritter nach diesen Kriterien nicht im Wege, obgleich eine zivilrechtliche Haftung des Verantwortlichen in Art. 82 DS-GVO sowie auch in Art. 11 ff. DIDD-Richtlinie und Art. 10 der Warenkauf-Richtlinie geregelt ist. Zunächst ist zu bemerken, dass nicht ersichtlich ist, dass die über den Vertrag mit Schutzwirkung zugunsten Dritter begründete Schadensersatzhaftung für nicht unmittelbar datenschutzrelevante Fehlfunktionen die mit der DS-GVO, der DIDD- und der Warenkauf-Richtlinie und den darin enthaltenen Haftungsnormen verfolgten Ziele konterkarieren könnte, da eine Wirksamkeitseinbuße des Unionsrechts aufgrund der gänzlich unterschiedlich gelagerten Sachverhalte nicht zu befürchten steht. Bei datenschutzrechtsrelevanten Fehlfunktionen hingegen ist Art. 82 DS-GVO *lex specialis*,[461] was angesichts der dort (Art. 82 Abs. 3 DS-

[456] Für den Vorschlag einer Direkthaftung des Hersteller gegenüber dem *Primär*nutzer, ausgestaltet als Netzwerkhaftung, siehe aber *Wendehorst*, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, Rechtsgutachten für Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz, 2016, 78 f.

[457] AG Wermelskirchen MDR 1988, 407.

[458] So bereits BGH NJW 1969, 269 (272); ferner AG Wermelskirchen MDR 1988, 407; *Gottwald*, in: MüKo, BGB, 8. Aufl. 2019, § 328 Rn. 190; *Janoschek*, in: BeckOK BGB, 50. Ed. 2019, § 328 Rn. 55.

[459] BGH NJW 2014, 2577 (2578 f.); *Klumpp*, in: Staudinger, BGB, 2015, § 328 Rn. 124; kritisch *Schwarze*, AcP 203 (2003), 348.

[460] Allerdings muss in diesen Fällen genau geprüft werden, ob eine hinreichende Leistungs- und Gläubigernähe vorliegt; diese kann dann zumindest nicht mit der gleichartigen Berührung durch Tracking begründet werden; zur Verletzung datenschutzbezogener Schutzpflichten i. S. v. § 241 Abs. 2 BGB im Übrigen noch unten, § 5 C.III.2.a).

[461] Siehe ausführlich unten, § 5 C.III.2.c).

GVO) vorgesehenen Haftungserleichterungen aber auch nicht Schutzlücken gegenüber der Verschuldensvermutung des § 280 Abs. 1 S. 2 BGB führt.

Wollte man dies anders sehen, so muss – zur Vermeidung einer indirekten Kollision nach der oben entwickelten zweistufigen Prüfung[462] – durch die nationale Norm erstens ein spezifisches, unionsrechtlich nicht adressiertes Risiko geregelt werden, das zweitens sachgerecht und mit den Zielen der unionsrechtlichen Regelung kompatibel ist. Das Risiko einer nicht unmittelbar datenschutzrechtlich relevanten Fehlfunktion eines IoT-Geräts wird jedoch weder in der DS-GVO noch in der DIDD- oder der Warenkauf-Richtlinie adressiert: Erstere beschäftigt sich nur mit datenschutzrelevanten Risiken, letztere regeln beide jeweils Fehlfunktionen, aber unter Ausblendung des Schadensersatzrechts. Daher ist das erste Kriterium der zweistufigen Prüfung erfüllt. Die Zubilligung eines vertragsrechtlichen Schadensersatzanspruches stellt sich aber auch auf der zweiten Stufe als sachgerecht dar, da die bekannten Schwächen des deutschen Deliktsrechts so überwunden werden können[463] und eine Kompensation Dritter in für den Anbieter vorhersehbaren und daher auch versicherbaren Fällen erfolgen kann. Sie ist daher mit den Zielen der unionalen Regelungen vereinbar.

dd) Drittschadensliquidation

Eher fernliegend erscheint demgegenüber, dass Schäden, die bei Dritten eintreten, im Wege der Drittschadensliquidation durch den Primärnutzer geltend gemacht werden können. Denn es fehlt üblicherweise bereits an einer ungerechtfertigten Schadensverlagerung vom Vertragspartner auf den Dritten.[464] Stattdessen tritt das Risiko für den Dritten zu dem für den Primärnutzer hinzu, was eine Drittschadensliquidation grundsätzlich ausschließt.[465] Damit ist nicht gesagt, dass in Sonderkonstellationen, in denen das IoT-Gerät selbst Gegenstand einer schuldrechtlichen, schadensverlagernden Abrede ist, die Drittschadensliquidation nicht zur Geltung kommen könnte.[466] Dies dürfte jedoch nur selten der Fall sein.

3. Zusammenfassung zu Vertragsschluss und DS-GVO

Eine Einbeziehung von Drittanbietern in die Vertragsbeziehung zwischen Erstanbieter und Nutzer gelingt vor allem über eine Bedingung und auch dies

[462] Siehe oben, § 5 A.I.2.b).

[463] *Gottwald*, in: MüKo, BGB, 8. Aufl. 2019, § 328 Rn. 166; *Klumpp*, in: Staudinger, BGB, 2015, § 328 Rn. 91.

[464] Zu diesen Kriterium BGH NJW 2016, 1089 Rn. 27; BGH NJW 2008, 2245 Rn. 35; *Oetker*, in: MüKo, BGB, 8. Aufl. 2019, § 249 Rn. 289 ff.; *Gottwald*, in: MüKo, BGB, 8. Aufl. 2019, § 328 Rn. 194; *Janoschek*, in: BeckOK BGB, 50. Ed. 2019, § 328 Rn. 51; kritisch, für eine Aufgabe der Rechtsfigur, *Stamm*, AcP 217 (2017), 165.

[465] BGH NJW 1969, 269 (272); *Oetker*, in: MüKo, BGB, 8. Aufl. 2019, § 249 Rn. 292; *Janoschek*, in: BeckOK BGB, 50. Ed. 2019, § 328 Rn. 51.

[466] Vgl. BGH NJW 2016, 1089 Rn. 27.

nur dann, wenn der Drittbezug hinreichend kenntlich gemacht wurde (konditionale Verknüpfung). Dies befördert auch informierte Vertragsschlüsse und reduziert damit die in § 3 angesprochene Informationsasymmetrie. Bei hinreichender Transparenz der Klausel jedoch kann die Wirksamkeit des Vertrags zivilrechtlich von einer Datenüberlassung an Dritte oder einer dahingehenden Einwilligung abhängig gemacht werden. Die datenschutzrechtliche (Un-)Zulässigkeit dieser Koppelung wird dadurch jedoch nicht berührt. Eine genuine Verpflichtung des Nutzers, Daten an Dritte zu überlassen und eine dahingehende Einwilligung zu erklären, kann nur dann angenommen werden, wenn sie ausdrücklich vereinbart wurde. Dafür streitet neben ökonomischen Erwägungen zur Reduzierung von Informationsasymmetrie auch der Abgleich mit Art. 6 Abs. 1 lit. f DS-GVO. Bei ausdrücklicher Vereinbarung sind ferner sowohl ein mehrseitiger Vertrag, ein bilateraler Vertrag unter Nutzung des Erstanbieters als Stellvertreter oder auch ein Vertrag zugunsten Dritter möglich.

Hinsichtlich der vertraglichen Bewältigung der Datenerhebung bei Dritten ist hingegen zu differenzieren. Wenn die Nutzung durch den Dritten erkennbar bewusst erfolgt, kann ein eigenständiger Nutzungsvertrag anzunehmen sein. Dies gilt jedoch nur, wenn ein Bewusstsein gerade hinsichtlich der Nutzung der Vernetzungskomponente besteht und, jedenfalls grundsätzlich, Erklärungsbewusstsein vorliegt. Anders als im Rahmen der Einwilligung kann mangelndes Erklärungsbewusstsein jedoch ausnahmsweise durch Verkehrsschutzbelange überwunden werden, wenn die Handlung objektiv unmissverständlich auf einen Rechtsbindungswillen schließen lässt und ein konkreter Vertrauenstatbestand des Verantwortlichen vorliegt. In Übertragung der Wertung des Unmissverständlichkeitsgebots der Einwilligung auf den datenschutzrechtlich relevanten konkludenten Vertragsschluss muss dieser jedoch verneint werden, wenn mit der Handlung primär andere Ziele (Besuch von Freunden in einem Smart Home/einer Smart City) verfolgt werden. Durch diese Kombination von objektiver Unmissverständlichkeit und potenzieller Überwindung subjektiv mangelnden Erklärungsbewusstseins wird dem Widerstreit von Verkehrsschutzbelangen einerseits und der negativen Privatautonomie sowie dem Datenschutzgrundrecht andererseits in spezifischer Weise Rechnung getragen.

Werden schließlich Daten von Unbeteiligten erhoben, die keine erkennbare Nutzungsintention haben, so scheidet ein konkludenter Nutzungsvertrag klar aus. Diese können dann jedoch über den Vertrag mit Schutzwirkung zugunsten Dritter zusätzlich geschützt sein. Dem Anbieter verbleibt dann in datenschutzrechtlicher Hinsicht letztlich der Rekurs auf eine wirksame Einwilligung oder auf die Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f DS-GVO.

C. Regulatorische Strukturen im allgemeinen Privatrecht

Das Zivilrecht hält jedoch seit jeher nicht nur Ermöglichungs-, sondern auch Ordnungsstrukturen vor, welche der privatautonomen Rechtsgestaltung Grenzen ziehen. Wenn die Rechtmäßigkeit der Datenverarbeitung auf eine Einwilligung oder einen Vertrag gestützt wird, so ergibt sich jeweils die Frage, inwiefern die klassischen Wirksamkeitsvoraussetzungen und Einwendungen des Zivilrechts hinsichtlich dieser Instrumente neben der DS-GVO Bestand haben können. Entscheidend ist dies insofern, als gesichert erscheint, dass nur eine wirksame Einwilligung oder ein wirksamer Vertrag die Legitimationswirkung von Art. 6 Abs. 1 lit. a oder b DS-GVO entfalten kann. Die für den Kontext digitaler Austauschverhältnisse bedeutsamsten zivilrechtlichen Grenzen der Privatautonomie und der gesetzlichen Ausgestaltung von marktförmigen Rechtsverhältnissen werden daher in diesem Abschnitt untersucht.

Eine im datenschutzrechtlichen Kontext besonders wichtige Wirksamkeitsvoraussetzung stellt § 134 BGB dar, da datenschutzrechtliche Vorschriften insofern als Verbotsgesetz verstanden werden können (I.). Ferner begrenzt die Inhaltskontrolle im weiteren Sinne, im AGB-Recht, aber auch in §§ 138, 242 BGB, die privatautonome Gestaltung datenschutzrechtlicher Vorgänge (II.). Sind diese Hürden genommen, so stellt sich weiterhin die Frage, ob eine Erfassung datenschutzrechtlich relevanter Konstellationen durch das deutsche Haftungsrecht grundsätzlich neben dem Schadensersatzregime der DS-GVO statthaben kann (III.).

I. § 134 BGB: Erstreckung der Datenschutzrechtswidrigkeit auf das Rechtsgeschäft?

§ 134 BGB setzt der privatautonomen Gestaltung von Rechtsverhältnissen eine objektiv-rechtliche Grenze. Rechtsgeschäfte sind demnach bei Verstoß gegen ein gesetzliches Verbot nichtig, wenn sich nicht aus dem Verbot etwas anderes ergibt. Dies ist insofern für Rechtsgeschäfte im Bereich der digitalen Wirtschaft bedeutsam, als die DS-GVO selbst als gesetzliches Verbot aufgefasst werden kann. Auf die datenschutzrechtliche Einwilligung als geschäftsähnliche Handlung könnte § 134 BGB zwar grundsätzlich Anwendung finden. Allerdings folgt die Unwirksamkeit der Einwilligung bei Verstoß gegen Verbotsvorschriften der DS-GVO bereits aus der DS-GVO selbst,[467] sodass ein Rückgriff auf § 134 BGB ausgeschlossen ist.[468]

---

[467] Siehe oben, § 5, Fn. 309.

[468] Die Anwendbarkeit von § 134 BGB auf die Einwilligung ist hinsichtlich anderer Verbotsgesetze umstritten, was hier jedoch mangels Bezug zur datenschutzrechtlichen Thematik nicht weiter verfolgt werden muss; dazu ausführlich *Ohly*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, 2002, 397 ff.

Sowohl dogmatisch als auch praktisch äußerst relevant ist jedoch die Frage, inwiefern die Verletzung datenschutzrechtlicher Vorschriften die Wirksamkeit eines Vertrages berührt, der jene Tätigkeiten zum Inhalt hat, die zu einer Datenschutzrechtsverletzung führen.[469] Dabei geht es nicht nur um Datendiebstahl und den illegalen Verkauf von Daten, etwa im Darknet.[470] Vielmehr betreffen diese Konstellation das Herz der gegenwärtigen digitalen Wirtschaft. Wie im Rahmen der datenschutzrechtlichen Analyse (§ 4) aufgezeigt, verstoßen die derzeit am Markt befindlichen Geschäftsmodelle in den drei Leitfällen nach hier vertretener Auffassung regelmäßig gegen datenschutzrechtliche Vorschriften. Gesetz im Sinne des § 134 BGB kann aber auch eine unionsrechtliche Verordnung wie die DS-GVO sein.[471]

Die herrschende Meinung im deutschen und auch internationalen Schrifttum nimmt bislang denn auch eine Unwirksamkeit des Vertrags an, der auf eine datenschutzrechtlich verbotene Tätigkeit gerichtet ist.[472] Auch die Rechtsprechung verfolgt grundsätzlich diese Linie.[473] Wie die folgende Analyse zeigen wird, kann diese Einschätzung jedoch nur für bestimmte Konstellationen überzeugen. Schon im Ausgangspunkt wird man unterscheiden müssen zwischen Verträgen, die mit der betroffenen Person selbst abgeschlossen werden, und Verträgen, die Dritte hinsichtlich der Daten einer betroffenen Person eingehen. Diese Differenzierung wird bislang in Rechtsprechung und Literatur nicht hinreichend vorgenommen.

1. Verträge mit Betroffenen: Entkopplung von Datenschutzrecht und Vertragsrecht

Besonders bedeutsam im Rahmen der hier verhandelten Leitfälle sind Verträge, bei denen sich die betroffene Person selbst zu Handlungen oder Unterlassungen verpflichtet, die zu einer datenschutzwidrigen Datenverarbeitung führen. Dies betrifft insbesondere die Konstellationen, in denen personenbezogene Daten als Gegenleistung überlassen werden (bzw. deren Erhebung geduldet wird). Ein konkretes Beispiel liefert der vom Bundeskartellamt ent-

---

469 Siehe zur Rechtslage nach dem BDSG aF auch *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012, 172 ff.

470 Dazu etwa *Symantec*, Internet Security Threat Report, Volume 24, 2019, 56 ff.

471 *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 134 Rn. 37; vgl. auch BGH NJW 1994, 858 (858 f.).

472 *Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 Rn. 30; wohl auch *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (220 f.); zum BDSG aF *Specht*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, 2012, 178 f.; siehe auch *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, 2016, 8 (kein Entgelt); ebenso *Lölfing*, Die App-Ökonomie des Schenkens, 2017, 74 f.

473 OLG Frankfurt a. M. BB 2018, 720 (722) (zu § 28 Abs. 3 Satz 1 BDSG aF); *Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 7 Rn. 30.

schiedene Facebook-Fall.[474] Es sei zu Analysezwecken einmal unterstellt, dass erstens in dem zwischen Facebook und seinen Nutzern abgeschlossenen Vertrag eine Verpflichtung[475] der Nutzer zur Überlassung des Klarnamens sowie zur Duldung der Datenerhebung mittels *third-party tracking* (z. B. durch den Like Button) enthalten ist und dass zweitens sowohl die Verarbeitung des Klarnamens als auch der durch die Tracking-Instrumente erhobenen Daten durch Facebook datenschutzrechtswidrig erfolgt. Dies ist keineswegs unrealistisch: Das LG Berlin hat die Verpflichtung zur Überlassung des Klarnamens nach altem Datenschutzrecht als rechtswidrig beurteilt[476] und die Analyse in § 4 hat gezeigt, dass der Einsatz von *third-party tracking* typischerweise datenschutzrechtswidrig ist und auch durch eine Einwilligung im Falle Facebooks wegen Verstoßes gegen das Kopplungsverbot des Art. 7 Abs. 4 DS-GVO jedenfalls grundsätzlich nicht gerechtfertigt werden kann.

Die herrschende Meinung in der Literatur geht in diesem Fall davon aus, dass eine datenbasierte Gegenleistung nicht wirksam vereinbart werden kann.[477] Auch wenn dies nicht immer explizit ausgesprochen wird, muss dies dogmatisch letztlich aus § 134 BGB folgen.[478] Die Wirksamkeit des Vertrages soll daher datenschutzrechtsakzessorisch ausgestaltet sein.[479] Demgegenüber wird hier jedoch dafür plädiert, bei Verträgen mit Betroffenen Datenschutzrecht und Vertragsrecht zu entkoppeln.[480] § 134 BGB sollte also insoweit, trotz Verstößen gegen die DS-GVO, die unmittelbar mit dem Vertrag zusammenhängen, nicht auf den Vertrag angewendet werden. Dafür sprechen eine Reihe von Argumenten.

Man wird die Anwendung von § 134 BGB zwar nicht daran scheitern lassen können, dass weder die Leistungspflicht des Anbieters (z. B. Zugang zu sozialem Netzwerk) noch die des Nutzers (Überlassung von Daten oder Duldung der Erhebung) noch ihre Erfüllung gegen die DS-GVO verstoßen, sondern erst die davon jedenfalls logisch getrennte Verarbeitung der so erlangten Daten durch den Verantwortlichen. Denn nach dem Wortlaut von § 134 BGB genügt es, dass „das Rechtsgeschäft" gegen § 134 BGB verstößt. Bei teleologischer Auslegung sind davon auch Geschäfte erfasst, die in ihren konkreten Leistungspflichten zwar nicht gegen den Buchstaben, aber wohl gegen den Zweck

[474] Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16.

[475] Die Analyse ändert sich im Ergebnis nicht, wenn die Datenüberlassung mit der Leistung des Anbieters lediglich konditional verknüpft ist, vgl. *Westermann*, in: MüKo, BGB, 8. Aufl. 2018, § 158 Rn. 45 f.

[476] LG Berlin MMR 2018, 328 Rn. 62 ff. Die Berufung wurde insoweit zurückgenommen, siehe KG MMR 2020, 239 Rn. 48.

[477] Siehe oben, § 5, Fn. 472.

[478] So explizit OLG Frankfurt a. M. BB 2018, 720 (722) (zu § 28 Abs. 3 Satz 1 BDSG aF).

[479] Für eine datenschutzakzessorische Interpretation des Vertragsrechts insbesondere *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, 2016, 16.

[480] So auch bereits *Hacker*, ZfPW 2019, 148 (160 ff.); *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen).

des Verbotsgesetzes verstoßen.[481] Wäre dies, wie die herrschende Meinung offenbar annimmt, bei datenschutzrechtswidriger Verarbeitung im Anschluss an die vertraglich ausbedungene Überlassung der Daten der Fall, so stünde jedenfalls die isolierte Makellosigkeit der konkreten Leistungspflichten einer Anwendung von § 134 BGB nicht im Wege.

Bedenklich erscheint an dieser Lösung jedoch bereits, dass eine datenschutzrechtsakzessorische Beurteilung der Wirksamkeit des Vertrags erhebliche Rechtsunsicherheit aus dem Datenschutzrecht in das Vertragsrecht transplantieren würde.[482] Wie die datenschutzrechtliche Analyse gezeigt hat, ist die Beurteilung neuer technologischer Phänomene und Geschäftsmodelle in datenschutzrechtlicher Hinsicht regelmäßig mit großer Unsicherheit behaftet.[483] Eine Ausdehnung dieser Unsicherheit auf das Vertragsrecht ist letztlich weder im Interesse der Nutzer noch der Anbieter. Ökonomische und rechtliche Entscheidungen sind deutlich einfacher zu treffen, wenn die rechtlichen Rahmenbedingungen klar sind. Dieses konsequentialistische Argument kann allerdings für sich betrachtet eine Anwendung von § 134 BGB nicht ausschließen, da jede Verbotsnorm letztlich mit Rechtsunsicherheit behaftet sein kann. Auf dogmatischer Ebene sind vielmehr zwei Argumente entscheidend: der Vorrang der datenschutzrechtlichen Abwicklung (a)) und die Gefahr der Umkehrung der Schutzrichtung der DS-GVO (b)). Schließlich ist die Lösung über die Wirksamkeit des Vertrags auch anderen dogmatischen Figuren überlegen; jedoch zeigt sich, dass Einwilligung und Vertrag über § 313 BGB zumindest partiell verknüpft sein könnnen (c)).

a) Vorrang der datenschutzrechtlichen Abwicklung

Es entspricht der herrschenden Meinung, dass § 134 BGB nach der Regel *lex specialis derogat legi generali*[484] verdrängt wird, sofern das Verbotsgesetz selbst ein privatrechtliches Sanktionsinstrumentarium bereithält.[485] Dies ist im unionsrechtlichen Kontext nicht nur bei Art. 101 Abs. 2 AEUV (der freilich sogar unmittelbar die Nichtigkeit anordnet),[486] sondern auch bei der DS-GVO der Fall, so dass sich die Frage des Anwendungsvorrangs des Unionsrechts gar

[481] BGH NJW 1991, 1060 (1061); *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 134 Rn. 15; *Sack/Seibl*, in: Staudinger, BGB, 2017, § 134 Rn. 145 f.

[482] *Hacker*, ZfPW 2019, 148 (161); *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen); aA *Faust*, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, 2016, 16.

[483] Vgl. *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (142).

[484] Dazu bereits oben, Text bei § 5, Fn. 122.

[485] BGH NJW 2003, 3692 (3692); OLG Celle, Urt. v. 10.9.2003, BeckRS 2004, 07985, unter B.III.; *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 134 Rn. 3; *Palzer*, JZ 2013, 691 (692).

[486] Zur Verdrängung von § 134 BGB durch Art. 101 Abs. 2 AEUV *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 134 Rn. 37; *Schmidt*, in: Immenga/Mestmäcker, Wettbewerbs-

nicht stellt.[487] Insbesondere die Betroffenenrechte der Art. 15–20 DS-GVO beinhalten ein eigenes Abwicklungsregime für den Fall datenschutzrechtswidriger Datenverarbeitung. Diese Ansprüche sind, sofern es um Rechtsbeziehungen zwischen Privaten geht, auch zivilrechtlicher Natur und grundsätzlich auf dem Zivilrechtsweg durchzusetzen.[488] So kann die betroffene Person Auskunft über die Datenverwendung nach Art. 15 Abs. 1 DS-GVO, Löschung der rechtswidrig verarbeiteten Daten nach Art. 17 Abs. 1 lit. d DS-GVO sowie Herausgabe nach Art. 20 Abs. 1 DS-GVO verlangen.

Daneben ist eine Anwendung von § 134 BGB schlichtweg nicht erforderlich; auch die in § 3 angesprochenen Typen von Marktversagen werden durch die Aufrechterhaltung des Vertrags in keiner Weise verstärkt. Denn einem etwaigen Leistungsverlangen des Verantwortlichen hinsichtlich der Überlassung von Daten, deren Verarbeitung rechtswidrig wäre, steht, wie gesehen,[489] schon wegen des Löschungsanspruchs in Kombination mit dem Herausgabeanspruch die *dolo agit*-Einrede entgegen. Die Durchsetzung des inkriminierten Leistungsversprechens steht daher auch ohne die Anwendung von § 134 BGB nicht zu erwarten. Ferner erfolgt durch die Aufrechterhaltung der Wirksamkeit des Vertrages auch keine „Legalisierung" der Datenschutzrechtswidrigkeit,[490] da diese von der Beurteilung durch nationales Vertragsrecht schon aufgrund des Anwendungsvorrangs des Unionsrechts unberührt bleibt. Der wirksame Vertrag führt schließlich auch nicht durch die Hintertür zur Rechtmäßigkeit der Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO, da die Auswirkungen dieser Norm bereits bei der Frage, ob überhaupt eine datenschutzrechtswidrige Verarbeitung vorliegt, berücksichtigt werden müssen.[491]

---

recht, 6. Aufl. 2019, Art. 101 Abs. 2 AEUV Rn. 1; *Schmidt*, in: Immenga/Mestmäcker, Wettbewerbsrecht, 6. Aufl. 2019, Anhang 2 VO 1/2003 Rn. 6.

[487] So bereits *Hacker*, ZfPW 2019, 148 (161); *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen); für das BDSG aF auch OLG Celle, Urt. v. 10.9.2003 – 3 U 137/03, BeckRS 2004, 07985, unter B.III.

[488] *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 17 DS-GVO Rn. 88; zur Rechtslage vor Geltung der DS-GVO *Dix*, in: Simitis, BDSG, 7. Aufl. 2011, § 35 Rn. 82. Allenfalls kann eine Zuständigkeit der Arbeitsgerichte bei einem diesbezüglich einschlägigen Sachverhalt gegeben sein; siehe insgesamt auch § 44 BDSG.

[489] Siehe oben, Text bei § 4, Fn. 685.

[490] Eine Legalisierungswirkung befürchtet jedoch *Dix*, ZEuP 2017, 1 (4).

[491] Folgt die Rechtswidrigkeit der Datenverarbeitung aus der Verletzung einer anderen Norm der DS-GVO als Art. 6 Abs. 1 DS-GVO, so wird diese Rechtswidrigkeit durch Art. 6 Abs. 1 lit. b DS-GVO ohnehin nicht berührt. Beruht die Rechtswidrigkeit hingegen darauf, dass keine Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO einschlägig ist, so ändert die Wirksamkeit des Vertrages daran nichts. Denn wäre die Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO rechtmäßig gewesen, so hätte schon kein Verstoß gegen ein Verbotsgesetz vorgelegen und § 134 BGB wäre daher nicht einschlägig.

b) Umkehrung der Schutzrichtung der DS-GVO

Die Anwendung von § 134 BGB wäre aber nicht nur überflüssig, sondern würde den Interessen gerade der betroffenen Person nachgerade aktiv schaden.[492] Es ist jedoch anerkannt, dass § 134 BGB nicht die Nichtigkeitsfolge auslöst, wenn ihre Anwendung der Schutzrichtung des Verbotsgesetzes zuwiderlaufen würde.[493] Denn dann ergibt sich aus der Verbotsnorm „ein anderes".[494] Der BGH hat dazu entschieden, dass die Nichtigkeitsfolge des § 134 BGB nicht greift, wenn der durch das Gesetz Geschützte an dem Vertrag festhalten will und öffentliche Interessen nicht berührt sind.[495] Sofern sich das Verbotsgesetz nur gegen einen Vertragspartner richtet (hier den Verantwortlichen), tritt Nichtigkeit gar „nur ausnahmsweise ein, wenn es nämlich mit Sinn und Zweck des Verbotsgesetzes unvereinbar wäre, die durch das Rechtsgeschäft getroffene rechtliche Regelung hinzunehmen und bestehen zu lassen".[496] Diese Ausnahmebedingung ist im Fall des Verstoßes gegen die DS-GVO nicht erfüllt: Mit Sinn und Zweck bzw. der Schutzrichtung der DS-GVO ist es vielmehr gerade unvereinbar, dem Vertrag die Wirksamkeit zu versagen.

Denn eine Unwirksamkeit des Vertrags würde gerade den Personen Nachteile bringen, die durch die Regeln der DS-GVO eigentlich primär geschützt werden sollen: den datenschutzrechtlich Betroffenen.[497] Für die Verantwortlichen hingegen ist die zivilrechtliche Unwirksamkeit faktisch irrelevant. Neben den Sanktionen des Datenschutzrechts für die Datenschutzrechtsverletzung (Art. 82 ff. DS-GVO, §§ 41 ff. BDSG) fällt die mangelnde vertragliche Bindung nicht ins Gewicht, zumal eine klageweise Durchsetzung der Verpflichtungen der Nutzer zur Überlassung von Daten schon aus Reputationsgründen praktisch nie in Betracht kommen wird[498] und diesem Begehr zudem regelmäßig die *dolo agit*-Einrede entgegensteht.[499] Gänzlich anders stellt sich jedoch die Situation für die Betroffenen dar. Sie werden durch die datenschutzrechtsakzessorische Lösung doppelt gestraft. Nicht nur müssen sie eine datenschutzrechtswidrige Verarbeitung ihrer personenbezogenen Daten gewärtigen, sondern ihnen verbleiben bei Unwirksamkeit des Vertrages zudem keine vertraglichen Primär- und Sekundäransprüche gegen den Anbieter, etwa bei Schlechterfüllung. Aus diesem Grund geht auch die Rechtsprechung bei einem

[492] Siehe bereits *Hacker*, ZfPW 2019, 148 (161); *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen).
[493] *Palzer*, JZ 2013, 691 (692); *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 134 Rn. 119.
[494] *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 134 Rn. 119.
[495] BGH NJW 2012, 3424 Rn. 18.
[496] BGH NJW 1985, 1020 (1020).
[497] Siehe nur den ersten und zweiten Erwägungsgrund der DS-GVO.
[498] *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (290).
[499] Siehe oben, Text bei und Nachweise in § 4, Fn. 685 f.

lediglich einseitigen Verstoß gegen das SchwarzArbG grundsätzlich von der Wirksamkeit des Vertrags aus.[500]

Seit dem Erlass der DIDD-Richtlinie werden diese Bedenken gegen die Unwirksamkeit des Vertrags verschärft. Denn der 48. Erwägungsgrund der Richtlinie spricht ausdrücklich davon, dass die Verletzung datenschutzrechtlicher Pflichten durchaus als Mangel im Sinne der Richtlinie eingeordnet werden kann. Zugleich stellt er jedoch klar, dass die Sekundäransprüche der Richtlinie entfallen, wenn infolge der Datenschutzrechtswidrigkeit der Vertrag nach nationalem Recht unwirksam ist.[501] Diese Konsequenz würde die Schutzrichtung der DS-GVO nachgerade auf den Kopf stellen. Als Folge hätten zudem Unternehmen, die sich datenschutzrechtswidriger Praktiken bedienen, gegenüber ihren rechtstreuen Wettbewerbern hinsichtlich der Gewährleistungsrechte einen wettbewerblichen Vorteil.[502]

Hinzu kommt, dass auch öffentliche Interessen durch die Wirksamkeit des Vertrags nicht berührt sind. Denn die Sanktion der Datenschutzwidrigkeit wird bereits durch das der DS-GVO immanente Sanktionsregime, in Verbindung mit den einschlägigen Normen des BDSG (§§ 41–43 BDSG), in hinreichender Weise gewährleistet.[503] Es ist nicht ersichtlich, dass die vertragliche Unwirksamkeit, gegenüber der Durchsetzungssperre infolge der *dolo agit*-Einrede, einen zusätzlichen Präventionseffekt verspräche. Auch der lauterkeitsrechtliche Unterlassungsanspruch von Mitbewerbern und qualifizierten Einrichtungen ist, sofern man ihn bei Datenschutzrechtsverletzungen anerkennt,[504] von der Wirksamkeit des Vertrags unberührt.[505] Folge der vertraglichen Unwirksamkeit wäre vielmehr eine im Einzelnen kaum sachgerechte bereicherungsrechtliche Rückabwicklung,[506] wie sich gleich zeigen wird.

---

[500] Zuletzt dezidiert OLG Düsseldorf, Hinweisbeschluss v. 5.2.2016, BeckRS 2016, 14031 Rn. 8; früher bereits BGH NJW 1985, 2303 (2304); BGH NJW 1984, 1175 (1176); ferner BGH NJW-RR 2002, 557; siehe auch *Köhler*, JZ 1990, 466 (467 f.).

[501] Siehe auch *Mischau*, ZEuP 2020, 335 (340).

[502] Vgl. nunmehr auch *Mischau*, ZEuP 2020, 335 (341).

[503] Vgl. zur ausreichenden Wirkung des datenschutzrechtlichen Sanktionsinstrumentariums auch BGH NJW 2007, 2106 Rn. 32.

[504] Befürwortend etwa OLG Hamburg, ZD 2019, 33; OLG Naumburg, ZD 2020, 154; *Uebele*, GRUR 2019, 694 (697 f.); ablehnend etwa LG Stuttgart, ZD 2019, 366; *Köhler*, ZD 2019, 285 (285); differenzierend *Ohly*, GRUR 2019, 686 (688 ff.) (keine Aktivlegitimation für Mitbewerber, mögliche Aktivlegitimation für qualifizierte Einrichtungen).

[505] *Köhler*, JZ 2010, 767 (770).

[506] Dieselben Bedenken bestehen, wenn man mit der Rechtsprechung auf den nichtigen Vertrag die Regeln der §§ 677 ff. BGB anwenden wollte, die im Wesentlichen zum gleicher Ergebnis führen, siehe nur BGH NJW 1962, 2010 (2011); dagegen etwa *Canaris*, NJW 1985, 2404 (2405); *Schäfer*, in: MüKo, BGB, 7. Aufl. 2017, § 677 Rn. 88; zu den Bedenken sogleich im folgenden Abschnitt.

c) Überlegenheit gegenüber anderen dogmatischen Figuren

Schließlich ließe sich gegen das Modell der vertraglichen Wirksamkeit einwenden, dass die für die Betroffenen misslichen Folgen der Unwirksamkeit auch dadurch verhindert werden können, dass auf andere dogmatische Figuren zurückgegriffen wird.

aa) Halbseitige Teilnichtigkeit

Zunächst ist daher auf die von *Canaris* zur Bewältigung einseitiger Gesetzesverstöße ins Spiel gebrachte halbseitige Teilnichtigkeit des Vertrages einzugehen.[507] Der BGH selbst hat in einer Entscheidung aus dem Jahr 1962 über einen wegen Verstoßes gegen das damalige RBeratG nichtigen Geschäftsbesorgungsvertrag diese Folge erwogen, die Entscheidung jedoch letztlich offengelassen. Er führte aus:

„Ferner ist, entsprechend dem vom Gesetz verfolgten Zweck, daran zu denken, den Teil der dem Geschäftsherrn erwachsenen Rechte von der Nichtigkeit auszunehmen, der geeignet ist, ihn zu schützen. Der Rechtsbesorger würde dann dem Auftraggeber unmittelbar nach Auftragsrecht (§§ 662 ff. BGB) haften, während er andererseits wegen seiner eigenen Leistungen auf einen Anspruch aus ungerechtfertigter Bereicherung angewiesen wäre."[508]

Canaris hat die halbseitige Teilnichtigkeit dann für den durch den Besteller unerkannten Verstoß gegen das SchwarzArbG sowie die Wucherfälle ventiliert und dabei die Grundidee der Konzeption des BGH übernommen: Der geschützte Teil behält seine vertraglichen Ansprüche, haftet jedoch gegenüber dem inkriminierten Teil nur aus ungerechtfertigter Bereicherung.[509] Dieser Vorschlag hat in Rechtsprechung und Schrifttum eine erhebliche Kontroverse ausgelöst,[510] sich jedoch letztlich nicht durchsetzen können.[511] Insbesondere wurde in der partiellen Aufrechterhaltung des Vertrags ein Widerspruch zur bereicherungsrechtlichen Abwicklung gesehen.[512] Canaris hat dagegen aufzuzeigen versucht, dass der teilnichtige Vertrag jedenfalls keinen bereiche-

[507] *Canaris*, Gesetzliches Verbot und Rechtsgeschäft, 1983, 29 ff., 31; *Canaris*, NJW 1985, 2404 (2404 f.).

[508] BGH NJW 1962, 2010 (2011).

[509] *Canaris*, Gesetzliches Verbot und Rechtsgeschäft, 1983, 29 ff., 31; *Canaris*, NJW 1985, 2404 (2404 f.).

[510] *Canaris* folgend etwa LG Bonn NJW-RR 1991, 180 (181); LG Mainz NJW-RR 1998, 48; *Petersen*, Jura 2003, 532 (534 f.); im Ergebnis auch *Sack/Seibl*, in: Staudinger, BGB, 2017, § 134 Rn. 281.

[511] Ablehnend etwa OLG Düsseldorf, Hinweisbeschluss v. 5.2.2016, BeckRS 2016, 14031 Rn. 7; in der Sache ebenso BGH NJW 1985, 2403 (2404); *Köhler*, JZ 1990, 466 (467); *Cahn*, JZ 1997, 8 (13 f.); *Köhler*, JZ 2010, 767 (769 f.); *H. Roth*, ZHR 153 (1989), 423 (430 f.); *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 134 Rn. 126; *Sack/Seibl*, in: Staudinger, BGB, 2017, § 134 Rn. 112 f.

[512] *Köhler*, JZ 1990, 466 (467); *Cahn*, JZ 1997, 8 (13); *H. Roth*, ZHR 153 (1989), 423 (430 f.); *Sack/Seibl*, in: Staudinger, BGB, 2017, § 134 Rn. 97, 113.

rungsrechtlichen Rechtsgrund für eine unentgeltliche Befriedigung der Leistungsinteressen des geschützten Teils darstellt.[513] Die halbseitige Teilnichtigkeit scheint jedoch aus mehreren Gründen für die Lösung datenschutzrechtlich relevanter Problemfälle ungeeignet.

Die bereicherungsrechtliche Haftung der betroffenen Person versagt einerseits schon im Ansatz, da es nicht um eine Verpflichtung des Nutzers zur Zahlung einer Geldsumme, sondern um die Überlassung von Daten geht. Bereicherungsrechtlich kann der Verantwortliche daher lediglich gemäß §§ 812 Abs. 1 S. 1 F1, 818 Abs. 2 BGB Wertersatz für seine Dienste oder Produkte in Geld verlangen, nicht jedoch die Überlassung von Daten. Insofern hätte die bereicherungsrechtliche Lösung zur Folge, dass die betroffene Person nunmehr, entgegen der eigentlichen vertraglichen Abrede, nicht zur Überlassung von Daten, sondern von Geld verpflichtet wäre. Die halbseitige Teilnichtigkeit würde damit das Geschäftsmodell „Dienst gegen Daten" in den klassischen Austausch von Dienst gegen Geld konvertieren, der jedoch von beiden Beteiligten gerade nicht gewünscht ist. Die primäre Haftung des Nutzers wäre dann gegenüber der vertraglichen gar noch verschärft.[514]

Sofern man andererseits die neuere BGH-Rechtsprechung, wonach aus generalpräventiven Gründen die Kondiktionssperre aus § 817 S. 2 BGB[515] nicht gem. § 242 BGB ihrerseits gesperrt ist,[516] auf die datenschutzrechtswidrige Verarbeitung überträgt,[517] bedarf es der Teilnichtigkeit nicht, da eine Bereicherungshaftung des Nutzers dann ohnehin ausscheidet. Dieses Ergebnis lässt sich jedoch auch auf direktem Wege bei Annahme der Wirksamkeit des Vertrags erreichen. Denn die betroffene Person kann dem Leistungsverlangen des Anbieters die *dolo agit*-Einrede insofern entgegenhalten, als die Überlassung datenschutzrechtswidrig wäre.[518]

---

[513] *Canaris*, Gesetzliches Verbot und Rechtsgeschäft, 1983, 32.

[514] Kritisch aus diesem Grund gegenüber der halbseitigen Teilnichtigkeit auch, wenngleich nicht im hier vorliegenden Kontext, *Cahn*, JZ 1997, 8 (13).

[515] Nach Ansicht des BGH findet § 817 S. 2 BGB auch Anwendung, wenn lediglich der Leistende gegen ein Verbot verstoßen hat, BGH NJW 2014, 1805 (1805), da nicht ersichtlich ist, warum der redliche Empfänger schlechter gestellt werden sollte. Dies entspricht der hier diskutierten Situation des Einsatzes von Daten als Gegenleistung, da regelmäßig der Nutzer selbst nicht gegen die DS-GVO verstößt. Dass nicht die Leistung des Anbieters selbst, sondern erst die im Gegenzug dafür ermöglichte Datenverarbeitung gegen ein Gesetz verstößt, kann wie schon bei § 134 BGB keinen Unterschied machen (siehe oben, Text bei § 5, Fn. 481). Zur Anwendung von § 817 S. 2 BGB im Falle halbseitiger Teilnichtigkeit jedoch kritisch *Köhler*, JZ 1990, 466 (467).

[516] BGH NJW 2014, 1805 (1806); zustimmend insoweit *Mäsch*, JuS 2014, 1123 (1124); *Stadler*, JA 2014, 623 (625); *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 134 Rn. 132.

[517] Gegen eine Übertragung der Rechtsprechung des BGH zum SchwarzArbG auf andere Sachverhalte aber *Heinze*, LMK 2014, 360329; für eine Anwendung von § 817 S. 2 BGB OLG Frankfurt a. M. BB 2018, 720 (723) (zu § 28 Abs. 3 BDSG aF); *Mankowski*, EWiR 2018, 209 (210).

[518] Siehe oben, Text bei § 4, Fn. 685 f.

Allerdings betrifft die Datenschutzrechtswidrigkeit typischerweise lediglich einen Teil der im Rahmen eines Nutzungsvertrags zu überlassenden Daten. Solche Daten, die für die Erfüllung der vertraglichen Pflichten des Anbieters erforderlich sind, kann der Anbieter durchaus weiterhin verlangen, da ihre Verarbeitung durch Art. 6 Abs. 1 lit. b DS-GVO gedeckt ist. Nun mag man einwenden, dass bei dem hier vertretenen subjektiven Erforderlichkeitsmaßstab unter Ausblendung der Nutzerpflichten gerade die für den Anbieter besonders wertvollen Daten bzw. Formen der Datenverarbeitung (Einsatz für personalisierte Werbung) typischerweise von Art. 6 Abs. 1 lit. b DS-GVO nicht erfasst werden und der Nutzer diese Daten daher auch nicht zu überlassen braucht – was den Interessen des Anbieters signifikant zuwiderliefe. Insoweit ist der Anbieter jedoch nicht schutzwürdig, da er es selbst in der Hand hätte, durch Angebot einer datenschonenden Alternative das Kopplungsverbot außer Kraft zu setzen und so die Datenschutzrechtskonformität der Datenverarbeitung durch eine wirksame Einwilligung herzustellen.[519] In der Summe kommt es daher auch bei Aufrechterhaltung der Wirksamkeit des Vertrages nicht zu einer völlig „unentgeltlichen" Nutzung dergestalt, dass der Nutzer keinerlei Daten überlassen müsste.[520]

Einer halbseitigen Teilnichtigkeit bedarf es daher nicht: Die bereicherungsrechtliche Haftung des Nutzers führt entweder zu einer sachwidrigen Haftung auf eine Geldsumme oder aber sie ist nach § 817 S. 2 BGB ausgeschlossen, was über eine *dolo agit*-Einrede im Fall des wirksamen Vertrags ebenso erreicht wird.

bb) Rechtliche Unmöglichkeit, Geschäftsgrundlage und Nichtigkeit nach § 134 BGB

Für die Schwarzarbeitsfälle hat *Köhler* nach der Schuldrechtsreform eine neue Lösung über das Unmöglichkeitsrecht vorgeschlagen.[521] Demzufolge soll die Erbringung der Leistung durch den inkriminierten Teil infolge des Verbotsgesetzes schon anfänglich rechtlich unmöglich sein. Dies berührt zwar gemäß § 311a Abs. 1 BGB nicht die Wirksamkeit des Vertrages. Nach herrschender Meinung setzt jedoch § 311a Abs. 1 BGB voraus, dass das Rechtsgeschäft gerade nicht nach § 134 BGB nichtig ist.[522] Schon aus diesem Grund kann die Lösung über das Unmöglichkeitsrecht nicht gelingen, wenn nicht zugleich § 134 BGB abgelehnt wird.

---

[519] Siehe oben, § 4 B.I.3.a)dd)(3)(b)(bb).

[520] Eine unentgeltliche Nutzung der geschützten Partei wird auch bei einseitigem Gesetzesverstoß typischerweise für unangemessen gehalten, siehe etwa OLG Düsseldorf, Hinweisbeschluss v. 5.2.2016, BeckRS 2016, 14031 Rn. 7; BGH NJW 1985, 2403 (2404).

[521] *Köhler*, JZ 2010, 767 (770); zustimmend *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 134 Rn. 126.

[522] *Ernst*, in: MüKo, BGB, 8. Aufl. 2019, § 311a Rn. 25; *Lorenz*, in: BeckOK, 50. Ed. 2019, § 275 Rn. 32; *Feldmann*, in: Staudinger, BGB, 2018, § 311a Rn. 15, 62; *Windel*, ZGS 2003, 466 (471 f.); *Canaris*, JZ 2001, 499 (506).

Sähe man hingegen (mit *Köhler*) in § 311a Abs. 1 BGB eine die Privatautonomie schonende, die Rechtsfolge des § 134 BGB modifizierende *lex specialis* zu § 134 BGB,[523] so schlösse die rechtliche Unmöglichkeit die Leistungspflicht des Schuldners gemäß § 275 Abs. 1 BGB und die Gegenleistungspflicht des Gläubigers gemäß § 326 Abs. 1 S. 1 BGB aus. Soweit die Gegenleistungspflicht bereits erfüllt wurde, könnte der Gläubiger das Geleistete nach § 326 Abs. 4 BGB zurückverlangen, der Schuldner nach Bereicherungsrecht.[524]

Für den Anspruch auf Datenüberlassung bietet dieses Modell zwar keine tragfähige Alternative zu § 134 BGB (1). Bei einem Anspruch auf Einwilligung hingegen muss diskutiert werden, inwiefern sich der Verstoß gegen datenschutzrechtliche Vorgaben für die Einwilligung auf den Vertrag auswirkt (2).

(1) Anspruch auf Überlassung von Daten

Die Lösung über das Unmöglichkeitsrecht versagt für datenbasierte Modelle, bei denen die Überlassung von Daten geschuldet ist, aus zwei Gründen auch dann, wenn man von einer rechtlichen Unmöglichkeit infolge von § 134 BGB ausgehen wollte. Erstens würde eine bereicherungsrechtliche Haftung des Schuldners (= Nutzers), sofern nicht § 817 S. 2 BGB eingreift, wiederum zu einer Wertersatzpflicht des Nutzers führen und so die datenbasierte in eine monetäre Gegenleistung konvertieren. Zweitens ist jedoch bereits nicht ersichtlich, dass die Erfüllung der gegenseitigen Verpflichtungen in den hier relevanten Konstellationen rechtlich unmöglich wäre. Datenschutzrechtswidrig ist lediglich die Verarbeitung bestimmter Nutzerdaten zu bestimmten Zwecken durch den Verantwortlichen. Diese Verarbeitung ist jedoch durch die betroffene Person gar nicht geschuldet. Sie verpflichtet sich lediglich dazu, Daten selbst zu überlassen oder die Datenerhebung des Verantwortlichen zu dulden. Diese Tätigkeiten selbst stellen jedoch keinen Verstoß gegen die DS-GVO dar, da sie gerade nicht die datenschutzrechtswidrige Verarbeitung *durch den Verantwortlichen* umfassen. Sofern sich umgekehrt der Verantwortliche gegenüber dem Nutzer zu bestimmten Verarbeitungen wirksam verpflichtet haben sollte, ist die darauf bezogene Verarbeitung nicht datenschutzrechtswidrig, da sie von Art. 6 Abs. 1 lit. b DS-GVO gestattet wird. Rechtliche Unmöglichkeit tritt daher nicht ein.[525]

Anders als bei § 134 BGB[526] wird man auch nicht argumentieren können, dass die Überlassung mit der Verarbeitung so eng verknüpft ist, dass sie von § 275 Abs. 1 BGB erfasst werden müsste. Denn es besteht keine Notwendigkeit, § 275 Abs. 1 BGB derart extensiv auszulegen: Das Recht der Unmög-

[523] So in der Sache *Köhler*, JZ 2010, 767 (770).
[524] *Spoerr/Schlösser* WM 2016, 1323 (1330 f.); *Köhler*, JZ 2010, 767 (770); vgl. auch *Ernst*, in: MüKo, BGB, 8. Aufl. 2019, § 275 Rn. 71.
[525] Im Ergebnis ebenso *Metzger*, AcP 216 (2016), 817 (855).
[526] Siehe oben, Text bei § 5, Fn. 481.

lichkeit dient dazu, in klar definierten Fällen die Parteien von ihrer jeweiligen Verpflichtung zu befreien, weil jegliche Erfüllungsanstrengungen bei Unmöglichkeit vergeblich, daher ineffizient und rechtlich ohne Sinn sind.[527] Dies trifft jedoch dann nicht mehr zu, wenn die Erfüllung möglich, nur die damit durch den Gläubiger bezweckte Verwendung nicht möglich ist. Denn der Schuldner kann erfüllen und der Gläubiger wiederum ist nicht gezwungen, seinen Leistungsanspruch überhaupt durchzusetzen. Zudem könnte er die Daten auch anders als vorgesehen, in datenschutzrechtskonformer Weise, verwenden. Seine Interessen werden daher nicht durch § 275 Abs. 1 BGB, sondern allenfalls durch §§ 119 Abs. 2, 313 BGB gewahrt.[528]

(2) Anspruch auf Einwilligung

Etwas komplexer liegt der Fall, wenn sich die betroffene Person verpflichtet haben sollte, eine Einwilligung abzugeben, die Einwilligung unter den gegebenen Umständen jedoch nicht wirksam erteilt werden kann (etwa, weil das Kopplungsverbot aus Art. 7 Abs. 4 DS-GVO verletzt ist).

Vorauszuschicken ist, dass der Verstoß allein gegen die Wirksamkeitsvoraussetzungen der Einwilligung nicht als Verletzung eines Verbotsgesetzes qualifiziert werden kann. Denn diese Wirksamkeitsvoraussetzungen stellen lediglich Ordnungsvorschriften, und keine Verbotsgesetze im Sinne des § 134 BGB, dar, da sie sich nicht gegen die Abgabe einer Einwilligungserklärung an sich, sondern die Umstände der Erklärung wenden.[529] Die Abgabe einer Einwilligung (mithin der Inhalt des verpflichtenden Rechtsgeschäfts in der hier betrachteten Konstellation) ist bei Nichterfüllung einer Wirksamkeitsvoraussetzung nicht als solche rechtswidrig, sondern die Einwilligung lediglich unwirksam. § 134 BGB scheidet mithin auch insoweit aus.

Allerdings ist in diesem Fall, anders als bei der Verpflichtung zur Datenüberlassung, die Erfüllung der Gegenleistungspflicht selbst von der Datenschutzrechtswidrigkeit betroffen. Insofern stellt sich die Frage, wie sich dies auf die Gegenleistungspflicht des Nutzers und die Leistungspflicht des Anbieters auswirkt. Ausgangspunkt der Analyse ist, dass man nach §§ 133, 157 BGB nicht wird annehmen können, dass der Nutzer verpflichtet ist, eine *wirksame* Einwilligung abzugeben.[530] Denn auf eine Reihe von Wirksamkeitsvoraussetzungen hat er selbst keinen Einfluss (zum Beispiel: hinreichende Information, Art. 4 Nr. 11 DS-GVO; keine Verletzung des Kopplungsverbots, Art. 7 Abs. 4

[527] Siehe nur *Ernst*, in: MüKo, BGB, 8. Aufl. 2019, § 275 Rn. 3–5.

[528] *Köhler*, JZ 2010, 767 (770); kritisch zu § 119 Abs. 2 BGB jedoch *Canaris*, JZ 2001, 499 (506); zu § 313 BGB bereits oben, Text bei § 4, Fn. 745.

[529] Vgl. *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 134 Rn. 41 f.

[530] Dies gilt nach hier vertretener Auffassung sowohl in dem Fall, in dem die Wirksamkeit der Einwilligung im Vertrag nicht thematisiert wird, als auch bei ausdrücklicher Verpflichtung zur Abgabe einer wirksamen Einwilligung; aA *Langhanke*, Daten als Leistung, 2018, 124 f. (Erfüllung nur durch wirksame Einwilligung möglich).

DS-GVO). Ihre Erfüllung kann vielmehr allein der Verantwortliche garantieren. Daher ist der Schuldner bei Auslegung nach §§ 133, 157 BGB regelmäßig lediglich verpflichtet, eine Einwilligungserklärung überhaupt abzugeben und alles seinerseits Erforderliche für deren Wirksamkeit zu tun. Er darf sie beispielsweise nicht in einem die Einwilligungsfähigkeit ausschließenden Zustand der Trunkenheit abgeben. Tut er dies doch, so tritt Erfüllung nicht ein und er muss die Erklärung nochmals abgeben, die dann zugleich nach dem oben Gesagten als Genehmigung der bisherigen, auf der nur vermeintlich wirksamen Einwilligung basierenden Datenverarbeitung aufgefasst werden kann.[531]

(a) Partielle Verknüpfung von Einwilligung und Vertrag

Hinsichtlich derjenigen Wirksamkeitsvoraussetzungen für die Einwilligung hingegen, auf welche der Nutzer keinen Einfluss hat, ist es wiederum eine Frage der Vertragsauslegung gemäß §§ 133, 157 BGB, ob das Nichtvorliegen dieser Wirksamkeitsvoraussetzungen in Durchbrechung des zwischen Einwilligung und Vertrag an sich geltenden Abstraktionsprinzips[532] auf die Wirksamkeit des Vertrags durchschlagen soll.[533] Es wird sich zeigen, dass derartige Fälle über das Recht der Geschäftsgrundlage, nicht jedoch über das Unmöglichkeitsrecht, zu lösen sind.

(aa) Wirksame Einwilligung als Geschäftsgrundlage

In Betracht kommen zunächst verschiedene Rechtsfiguren, um eine Verknüpfung zwischen Einwilligung und Vertrag herzustellen: die Geschäftsgrundlage nach § 313 BGB, wie bereits beim Widerruf der Einwilligung;[534] eine Geschäftseinheit nach § 139 BGB[535] sowie eine Gegenwartsbedingung des Vertrags.[536] Eine Gegenwartsbedingung hat gegenüber der Annahme einer Geschäftseinheit nach § 139 BGB den Vorzug, dass die Bedingung klarer auf das Fehlen *bestimmter* Wirksamkeitsvoraussetzungen zugeschnitten werden kann. Die Geschäftsgrundlage wiederum überzeugt im Vergleich mit der Annahme

---

[531] Dazu oben, § 4 B.I.3.a)ee).

[532] Dazu oben, § 4, Fn. 434.

[533] Für eine Aufrechterhaltung der Wirksamkeit des Vertrags hingegen *Langhanke*, Daten als Leistung, 2018, 218, allerdings ohne Diskussion etwaiger Verknüpfungsmöglichkeiten.

[534] Siehe oben, § 4 B.I.3.b)bb)(3)(b)(aa)b.

[535] Zur Geschäftseinheit von Einwilligung und Vertrag *Ohly*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, 2002, 450 f.; *Langhanke*, Daten als Leistung, 2018, 166 f.; *Graf von Westphalen*, VuR 2017, 323 (331); *Kohte*, AcP 185 (1985), 105 (136).

[536] Eine Gegenwartsbedingung ist bei Unsicherheit hinsichtlich der für das Rechtsgeschäft relevanten Rechtslage nicht unüblich, vgl. *Westermann*, in: MüKo, BGB, 8. Aufl. 2018, § 158 Rn. 52. Es handelt sich nicht um eine reine Rechtsbedingung, da es nicht um die rechtlichen Voraussetzungen des bedingten Geschäfts (Vertrag), sondern der Einwilligung geht. Die Gegenwartsbedingung wird entsprechend § 158 ff. BGB behandelt, *Westermann*, in: MüKo, BGB, 8. Aufl. 2018, § 158 Rn. 52.

einer Geschäftseinheit insoweit, als das Trennungsprinzip zwischen Einwilligung und Vertrag[537] dadurch in stärkerem Maße gewahrt bleibt.

Gleiches gilt für den Abgleich zwischen Geschäftsgrundlage und Gegenwartsbedingung. Für den Fall einer konditionalen Verknüpfung von Leistung und Gegenleistung wurde zwar oben der Widerruf der Einwilligung als auflösende Bedingung und nicht als Geschäftsgrundlage eingeordnet.[538] Die Interessenlage unterscheidet sich jedoch von der hier zu untersuchenden Situation in drei Aspekten, sodass die unterschiedliche Behandlung gerechtfertigt erscheint. Erstens ist die Leistungserbringung bei der konditionalen Verknüpfung ohnehin an Bedingungen geknüpft, sodass es naheliegt, eine weitere Bedingung und nicht eine Geschäftsgrundlage hinsichtlich des Widerrufs der Einwilligung anzunehmen.

Zweitens lässt sich typischerweise leicht und rechtssicher entscheiden, ob ein wirksamer Widerruf der Einwilligung erfolgt ist oder nicht. Dies rechtfertigt die automatische Suspension der Leistungspflicht des Anbieters (bei konditionaler Verknüpfung). Hingegen ist es regelmäßig schwierig, rechtssicher festzustellen, ob die Wirksamkeitsvoraussetzungen der Einwilligung vorliegen, etwa Art. 7 Abs. 4 DS-GVO nicht verletzt ist. Die automatische Kopplung dieser Wirksamkeitsvoraussetzungen an die Wirksamkeit des Vertrages hätte eine beständige Unsicherheit zur Folge, welche durch die Geltung des Abstraktionsprinzips zwischen Einwilligung und Vertrag[539] gerade verhindert werden soll. Daher erscheint für diese Fälle die Annahme einer Geschäftsgrundlage sachgerechter.

Zudem ergibt sich, drittens, ein weiterer Vorteil, wenn die Leistungspflicht des Anbieters nicht automatisch entfällt. Dann kann einerseits berücksichtigt werden, ob eine Verarbeitung auf Grundlage eines gesetzlichen Erlaubnistatbestands nach Art. 6 Abs. 1 DS-GVO möglich ist. Andererseits ist es nach § 313 BGB möglich in Rechnung zu stellen, inwieweit die Unwirksamkeit der Einwilligung lediglich der Sphäre des Verantwortlichen zuzurechnen ist und die Leistungspflicht daher erhalten bleiben sollte,[540] etwa bei mangelnder Freiwilligkeit infolge einer bewussten Täuschung der betroffenen Person. Daher stellen diejenigen Wirksamkeitsvoraussetzungen der Einwilligung, auf welche der Nutzer keinen Einfluss nehmen kann, nach hier vertretener Auffassung eine Geschäftsgrundlage des Vertrags (präziser noch: wesentliche Vorstellungen im Sinne des § 313 Abs. 2 BGB[541]) dar, bei der die gesetzliche und vertragliche Risikoverteilung bzw. die bewusste Schaffung des Risikos der Unwirksamkeit (Sphärengedanke) berücksichtigt werden kann und muss.[542]

[537] Dazu oben, § 4, Fn. 434.
[538] Siehe oben, § 4 B.I.3.b)bb)(3)(b)(bb).
[539] Dazu oben, § 4, Fn. 434.
[540] *Finkenauer*, in: MüKo, BGB, 8. Aufl. 2019, § 313 Rn. 284.
[541] Siehe zur Anwendung von § 313 Abs. 2 BGB auf Rechtsirrtümer nur *Finkenauer*, in: MüKo, BGB, 8. Aufl. 2019, § 313 Rn. 284 f.
[542] *Finkenauer*, in: MüKo, BGB, 8. Aufl. 2019, § 313 Rn. 75.

Dies ist insbesondere relevant außerhalb von Dauerschuldverhältnissen, da sich dann aus §313 BGB ein Recht auf Vertragsanpassung oder Rücktritt ergibt. Bei Dauerschuldverhältnissen hingegen kann die Unwirksamkeit der Einwilligung im Rahmen von §314 BGB, oder bei speziellen Kündigungsrechten des besonderen Schuldrechts, berücksichtigt werden, sodass auf den Wegfall der Geschäftsgrundlage nicht mehr zurückgegriffen werden muss.[543] Damit ist auch die Konkordanz mit dem Widerruf der Einwilligung hergestellt, bei dem hinsichtlich des Vertrags auch §313 BGB greifen kann, sofern nicht ein Dauerschuldverhältnis mit Kündigungsmöglichkeit vorliegt.[544]

Sofern keine Loyalitätspflichten durch den Anbieter verletzt wurden, wird jedoch bei Fehlen sonstiger Wirksamkeitsvoraussetzungen der Einwilligung, deren Mangel auch nicht durch den Nutzer behoben werden kann, das Festhalten an der Leistungspflicht für den Anbieter in der Regel unzumutbar im Sinne von §§313 Abs. 3, 314 Abs. 1 S. 2 BGB sein, wenn Daten als Gegenleistung fungieren und kein gesetzlicher Erlaubnistatbestand jenseits der Einwilligung greift. Dies gilt etwa für den Fall der Unwirksamkeit wegen Verstoßes gegen das Kopplungsverbot des Art. 7 Abs. 4 DS-GVO. Denn sonst würde der Nutzer vollkommen kostenfrei in den Genuss der Leistung gelangen. Damit bleibt festzuhalten, dass eine partielle Verknüpfung von Einwilligung und Vertrag über das Recht der Geschäftsgrundlage geleistet wird.

(bb) Keine Verletzung des Effektivitätsgrundsatzes

Bedenken an dieser Auslegung könnten sich allenfalls aus dem Effektivitätsgrundsatz des Unionsrechts ergeben. Wenn der Verantwortliche bei Unwirksamkeit der Einwilligung infolge eines Umstandes, der aus seiner Sphäre entstammt (z. B. Vertragsgestaltung unter Verletzung des Kopplungsverbots), nicht befürchten muss, seine vertragliche Leistung dennoch erbringen zu müssen, reduziert dies womöglich die Abschreckungswirkung hinsichtlich der Unterlassung der Einholung datenschutzrechtswidriger Einwilligungserklärungen. Im Bereich missbräuchlicher Klauseln hat der EuGH nunmehr entschieden, dass zur Verstärkung der Abschreckungswirkung die Interessen des Verwenders einer unangemessenen Klausel an einer Abänderung der Klausel oder auch an einer Ersetzung durch (typischerweise auf einen Interessenausgleich bedachtes) dispositives Gesetzesrecht keinerlei Berücksichtigung finden dürfen.[545] Zwar enthält die DS-GVO, anders als die Klauselrichtlinie in Art. 7 Abs. 1, keine explizite Zielsetzung, der Verwendung von datenschutz-

[543] Zum Vorrang von §314 BGB vor §313 Abs. 3 BGB, siehe nur BGH, BeckRS 9998, 173405, unter II.4. (zur Rechtslage vor der Schuldrechtsreform); zur Möglichkeit der Überschneidung von §§313 und 314 BGB allgemein auch *Gaier*, in: MüKo, BGB, 8. Aufl. 2019, §314 Rn. 22; *Finkenauer*, in: MüKo, BGB, 8. Aufl. 2019, §313 Rn. 169.

[544] Siehe oben, §4 B.I.3.b)bb)(3)(b)(aa)b.

[545] EuGH, Urt. v. 26.3.2019 – verb. Rs. C-70/17 und C-179/17 (*Abanca Corporación Bancaria*) – Rn. 56; Urt. v. 7.8.2018 – verb. Rs. C-96/16 und C-94/17 (*Banco Santander*) –

rechtswidrigen Einwilligungserklärungen ein Ende setzen zu wollen. Allerdings wird die Frage nach der Unwirksamkeit des Vertrags nur dann virulent, wenn die Datenverarbeitung auch auf Grundlage eines gesetzlichen Erlaubnistatbestands nicht rechtmäßig durchgeführt werden kann. Dass der DS-GVO jedoch das Ziel innewohnt, unrechtmäßige Datenverarbeitungen zu verhindern, wird man nicht ernsthaft bestreiten können. Dies muss auch im Rahmen der Abwägung nach § 313 BGB berücksichtigt werden.

Wollte man den Anbieter jedoch an seiner Leistungspflicht festhalten, auch wenn eine datenschutzrechtskonforme Einwilligung nicht erteilt werden kann, so würde dies primär nicht Anreize dafür setzen, die datenschutzrechtswidrige Verarbeitung zu unterlassen, sondern Verträge, bei denen die Gegenleistung in der Abgabe einer Einwilligung bestehen soll, nicht anzubieten, wenn die Datenschutzrechtskonformität der Einwilligung in Zweifel steht. Dies wiederum benachteiligt insbesondere Nutzer mit niedrigen Datenschutzpräferenzen, die ihre Budgetrestriktionen gerne erweitern möchten. Anders als im Fall missbräuchlicher Klauseln, für die keine eigenständigen Sanktionen neben der Unwirksamkeit vorgesehen sind, dürfte ferner die Abschreckungswirkung hinsichtlich der Unterlassung datenschutzrechtswidriger Verarbeitung ganz maßgeblich auf den Sanktionen nach Art. 82 ff. DS-GVO, §§ 41 ff. BDSG aufruhen.[546] Neben einer nach Art. 83 Abs. 5 DS-GVO möglichen Geldbuße in Höhe von 4 % des globalen Jahresumsatzes fällt die mögliche Bindung an einen Vertrag, bei dem typischerweise wegen der digitalen Natur des Produkts praktisch keine Grenzkosten für die Erfüllung anfallen, für den Anbieter in keiner Weise ins Gewicht. Daher wird der unionsrechtliche Effektivitätsgrundsatz nicht verletzt, wenn die schutzwürdigen Interessen des Anbieters, seine Leistungspflicht nur bei wirksamer Einwilligung erbringen zu müssen, im Ramen von § 313 BGB Berücksichtigung finden.

(cc) Rechtsfolgen für den Vertrag

Ist die Einwilligung wegen Verstoßes gegen die DS-GVO unwirksam, so ist hinsichtlich der Rechtsfolgen für den Vertrag daher zu differenzieren. Mangelt es an einer Wirksamkeitsvoraussetzung, deren Erfüllung die betroffene Person selbst bewirken kann, so dürfte regelmäßig keine Unmöglichkeit eintreten. Denn auch bei dauerhafter Einwilligungsunfähigkeit ist eine Erteilung der Einwilligung durch den gesetzlichen Vertreter prinzipiell möglich. Unterbleibt diese, so liegt allenfalls (sofern der Vertrag wirksam abgeschlossen wurde) eine Pflichtverletzung des Nutzers, nicht aber Unmöglichkeit vor. Hinsichtlich sol-

Rn. 74; Urt. v. 21.1.2015 – verb. Rs. C-482/13, C-484/13, C-485/13 und C-487/13 (*Unicaja Banco und Caixabank*) – Rn. 33; siehe dazu unten, § 5 C.II.1.f)bb).

546 Vgl. auch allgemein zum Verhältnis privat-, verwaltungs- und strafrechtlicher Sanktionen *Wagner*, AcP 206 (2006), 352 (355 ff.); *Grundmann*, in: Festschrift Canaris, 2017, 907 (946 f.).

cher Wirksamkeitsvoraussetzungen, auf die der Nutzer keinen Einfluss hat, besteht hingegen schon keine Pflicht des Nutzers, die Wirksamkeit der Einwilligung herzustellen. Auch insofern scheidet Unmöglichkeit daher aus. Vielmehr sind diese Wirksamkeitsvoraussetzungen Teil der Geschäftsgrundlage. Kann eine derartige Wirksamkeitsvoraussetzung nicht erfüllt werden (etwa bei Verstoß der Einwilligung gegen das Kopplungsverbot), so steht dem Anbieter typischerweise ein Vertragslösungsrecht nach § 313 Abs. 3 BGB oder § 314 BGB zu. Insofern deckt sich die Rechtsfolge der Unwirksamkeit der Einwilligung mit jener des Widerrufs der Einwilligung. Unmöglichkeit hinsichtlich der Gegenleistungspflicht des Nutzers jedenfalls tritt bei Unwirksamkeit der Einwilligung regelmäßig nicht ein.

(b) Modifikationen der Rückabwicklung

Sofern ein Leistungsaustausch bereits stattgefunden hat, wäre bei Annahme eines Rücktrittsrechts nach § 313 Abs. 3 S. 1 BGB der Vertrag nach §§ 346 ff. BGB rückabzuwickeln.[547] Wollte man hingegen, anders als hier vertreten, eine Gegenwartsbedingung oder eine Geschäftseinheit annehmen, so hätte die Unwirksamkeit des Vertrags infolge des Ausfalls der Gegenwartsbedingung bzw. der Gesamtnichtigkeit infolge der Geschäftseinheit eine bereicherungsrechtliche Rückabwicklung zur Folge.[548] In beiden Fällen würde dies jedoch wiederum eine Wertersatzpflicht des Nutzers hinsichtlich bereits erbrachter Leistungen des Anbieters gemäß § 346 Abs. 2 Nr. 1 BGB bzw. §§ 812 Abs. 1 S. 1 F1, 818 Abs. 2 BGB bedingen. Sofern nicht wieder § 817 S. 2 BGB analog eingreift,[549] wäre diese Rechtsfolge jedoch mit dem Anwendungsvorrang der DS-GVO (genauer: dem Effektivitätsgrundsatz) nicht zu vereinbaren, da sie deren Durchsetzung übermäßig erschweren würde. Denn in Übertragung der *Quelle*- und *Fülla*-Rechtsprechung des EuGH[550] ist davon auszugehen, dass die Möglichkeit des Wertersatzes den Nutzer davon abhalten kann, die Unwirksamkeit der Einwilligung zu reklamieren und seine aus der Datenschutzrechtswidrigkeit folgenden Rechte (zum Beispiel Art. 17 Abs. 1 lit. d DS-GVO) geltend zu machen.

Die Unwirksamkeit der Einwilligung führt bei Wegfall der Geschäftsgrundlage, aber auch bei Annahme einer Gegenwartsbedingung also lediglich dazu, dass *pro futuro* keine der Parteien Leistungen erbringen muss. Bei Dauer-

[547] *Finkenauer*, in: MüKo, BGB, 8. Aufl. 2019, § 313 Rn. 110.

[548] Zur Gegenwartsbedingung: für die Rückabwicklung des während der Schwebezeit erfolgten Austauschs bei der der auflösenden Bedingung ist dies anerkannt, siehe BGH, Urt. v. 30.4.1959, BeckRS 1959, 104554 Rn. 28; *Westermann*, in: MüKo, BGB, 8. Aufl. 2018, § 158 Rn. 41; *Bork*, in: Staudinger, BGB, 2015, § 151 Rn. 16; kritisch für den Fall des § 159 BGB *Wunner*, AcP 168 (1968), 425 (445 ff.); zur Geschäftseinheit, siehe nur *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 139 Rn. 1.

[549] Dazu oben, Text bei § 5, Fn. 515.

[550] EuGH, Urt. v. 17.4.2008 – Rs. C-404/06 (*Quelle*) – Rn. 34 f.; EuGH, Urt. v. 23.5.2019 – Rs. C-52/18 (*Fülla*) – Rn. 40.

schuldverhältnissen stellt dies für den Fall des Wegfalls der Geschäftsgrundlage § 313 Abs. 3 S. 2 BGB ohnehin klar. Ein Wertersatzanspruch des Verantwortlichen scheidet jedenfalls aus. Ein etwaiger rücktritts- oder bereicherungsrechtlicher[551] Herausgabeanspruch des Nutzers hinsichtlich aktiv überlassener Daten hingegen steht nicht im Konflikt mit den Betroffenenrechten der DS-GVO und tritt daher in Anspruchskonkurrenz zu diesen (insbesondere zu Art. 17 und 20 DS-GVO).[552]

2. Verträge zwischen Dritten: Kopplung von Datenschutzrecht und Vertragsrecht

Damit ist gezeigt, dass die Datenschutzrechtswidrigkeit nicht zu einer Nichtigkeit des Vertrags zwischen einem Verantwortlichen und der betroffenen Person gemäß § 134 BGB führen sollte. Aus den dafür vorgebrachten Argumenten erhellt jedoch zugleich, dass gänzlich anders zu entscheiden ist, wenn ein Verantwortlicher einen Vertrag, dessen Vollzug gegen die DS-GVO verstößt, nicht mit der betroffenen Person, sondern mit einem Dritten abschließt. Hier ist in der Regel Nichtigkeit nach § 134 BGB anzunehmen. Ein Beispiel wäre der Verkauf von Nutzerdaten durch ein soziales Netzwerk an Drittunternehmen, bei dem die Weiterleitung der Daten gegen die DS-GVO verstößt. Dies betrifft mithin zentral Vertragskonstellationen im Rahmen des ersten Leitfalls.

a) Nichtigkeit nach § 134 BGB

§ 134 BGB ist in diesem Fall, anders als beim Vertrag mit der betroffenen Person selbst, nicht durch ein eigenes Abwicklungsregime der DS-GVO verdrängt. Denn die Betroffenenrechte der Art. 12–22 DS-GVO gelten zwar gegenüber jedem Verantwortlichen, aber immer nur in der Beziehung zwischen diesem und Betroffenem. Eigene privatrechtliche Sanktionen sieht die DS-GVO für das Verhältnis zwischen Verantwortlichem und Drittem (oder weiterem Verantwortlichen) nicht vor.[553]

---

[551] Geht man, anders als hier vertreten, von einer Gegenwartsbedingung und damit einer Anwendung des Bereicherungsrechts aus, so ist Folgendes zu berücksichtigen: Bei in Vollzug gesetzten, fehlerhaften Dauerschuldverhältnissen mag ein im Einzelfall über die genannten Ansprüche der DS-GVO hinausgehender bereicherungsrechtlicher Anspruch des Nutzers wegen Unzumutbarkeit einer vollständigen (noch dazu einseitigen) Rückabwicklung beschränkt sein. Dogmatisch lässt sich dies über eine Beschränkung der Unwirksamkeitsfolge analog § 158 Abs. 1 BGB erreichen (Zur Möglichkeit der vertraglichen Modifikation von Folgen des Bedingungseintritts *Rövekamp*, in: BeckOK BGB, 51. Ed. 2019, § 158 Rn. 33).

[552] Vgl. *Specht*, JZ 2017, 763 (768).

[553] Die einzige explizite Regelung der Offenlegung von Daten gegenüber Dritten findet sich in Art. 19 DS-GVO, wonach der Verantwortliche die Dritten über die Ausübung der Betroffenenrechte nach Art. 16–19 DS-GVO im Rahmen der Zumutbarkeit unterrichten und die Dritten gegenüber der betroffenen Person benennen muss. Dies stellt jedoch gerade

Ferner wird durch die Unwirksamkeit des Vertrags die Schutzrichtung der DS-GVO nicht umgekehrt, sondern verstärkt. Umgekehrt würde die Wirksamkeit des Vertrags die Wahrscheinlichkeit der Verwirklichung der in § 3 genannten ökonomischen und sozialen Risiken erhöhen. Denn sie hätte zur Folge, dass die Verpflichtung zur datenschutzrechtswidrigen Datenweiterleitung durchsetzbar wäre. Insbesondere greift die *dolo agit*-Einrede[554] nicht, da der Verkäufer nicht einwenden kann, dass ein Dritter (die betroffene Person) Löschungsansprüche nach Art. 17 Abs. 1 lit. d DS-GVO innehat. Denn ob die betroffene Person diese ausübt, ist alles andere als sicher. Insofern haftet dem Leistungsbegehren des Dritten keine Treuwidrigkeit an. Die Verletzung datenschutzrechtlicher Pflichten verstärkt jedoch das datenschutzrechtliche Risiko für die betroffene Person,[555] sodass der Normzweck des Verbotsgesetzes eine Nichtigkeit des Vertrags in diesem Fall erfordert. Dies hat zur Folge, dass die Vertragsparteien auf eine bereicherungsrechtliche Abwicklung verwiesen sind, wobei allerdings bei Bösgläubigkeit[556] nach Ansicht der Rechtsprechung die Konditionssperre des § 817 S. 2 BGB greift.[557]

b) Einordnung der bisherigen Rechtsprechung

Mit dieser Differenzierung zwischen Verträgen mit der betroffenen Person einerseits und mit Dritten andererseits lässt sich auch die bisherige Rechtsprechung in Einklang bringen. Das OLG Frankfurt a. M. hat noch nach altem Datenschutzrecht geurteilt, dass der Verstoß gegen § 28 Abs. 3 BDSG aF die Unwirksamkeit nach § 134 BGB nach sich zieht.[558] Dies betraf indes gerade nicht einen Vertrag mit der betroffenen Person, sondern den Adresshandel mit Dritten. Der Insolvenzverwalter eines Adresshandelsunternehmens hatte einen Vertrag mit einem Drittunternehmen über den Verkauf von personenbezogenen Daten abgeschlossen, der nach Ansicht des Gerichts gegen § 28 Abs. 3 BDSG aF verstieß.[559] Da diese Norm den Adresshandel ohne Einwilligung der betroffenen Person nach Ansicht des Gerichts gerade unterbinden sollte, folgte aus der Verletzung der datenschutzrechtlichen Vorschrift auch die Unwirksamkeit des Vertrags nach § 134 BGB.[560] Dasselbe Ergebnis wird man nun bei Verstoß gegen die DS-GVO annehmen können, wenn keine Rechtsgrundlage nach Art. 6 Abs. 1 DS-GVO einschlägig ist. Denn auch die DS-GVO verfolgt unstreitig das Ziel, unrechtmäßige Datenverarbeitungen zu verhindern

keine Regelung der privatrechtlichen Rechtsfolgen im Verhältnis zwischen dem Verantwortlichen und den Dritten dar.

554 Siehe oben, Text bei § 4, Fn. 685 f.

555 Siehe oben, § 4 C.I.3.a).

556 Dazu *Schwab*, in: MüKo, BGB, 7. Aufl. 2017, § 817 Rn. 85.

557 OLG Frankfurt a. M. BB 2018, 720 (723).

558 OLG Frankfurt a. M. BB 2018, 720 (722); zustimmend *Schemmel*, BB 2018, 723.

559 OLG Frankfurt a. M. BB 2018, 720 (721 f.).

560 OLG Frankfurt a. M. BB 2018, 720 (722).

und einer Vertiefung der datenschutzrechtlichen Risiken gerade durch den unrechtmäßigen Datenhandel vorzubeugen.

In einer weiteren Entscheidung hat der BGH allerdings von der Nichtigkeitsfolge des § 134 BGB trotz Verstoßes gegen das alte Datenschutzrecht abgesehen.[561] Wieder ging es um eine Drittkonstellation: Im Rahmen einer Forderungsabtretung hatte der Zedent dem Zessionar die Kontaktdaten des Schuldners übermittelt, damit der Zessionar die Forderung gegen den Schuldner durchsetzen könne. Der BGH urteilte, dass selbst bei Verstoß gegen das BDSG aF § 134 BGB nicht einschlägig sei, da andernfalls der ökonomisch legitime Handel mit Forderungen und die vom BGB grundsätzlich als möglich angesehene Abtretung in weiten Bereichen praktisch nicht vollzogen werden könnten.[562] Ferner würde das datenschutzrechtlich fundierte Abtretungsverbot zu einem unerträglichen Wertungswiderspruch führen, da infolge des beschränkten Anwendungsbereichs des Datenschutzrechts nur Abtretungen von Forderungen gegen natürliche Personen, nicht jedoch gegen juristische Personen, diesem unterfielen.[563]

Nach Geltungsbeginn der DS-GVO dürfte dieser Fall jedoch in der Begründung, zum Teil auch im Ergebnis anders zu behandeln sein. Sofern die Vertragsparteien ein berechtigtes Interesse an der Abtretung haben, ist die Übermittlung der Schuldnerinformationen erlaubt gemäß Art. 6 Abs. 1 lit. f DS-GVO. Lediglich bei der rechtsmissbräuchlichen Verlagerung von Prozess- und Insolvenzrisiken zulasten des Schuldners[564] ist von einer Datenschutzrechtswidrigkeit und dann konsequenterweise aber auch einer Nichtigkeit des Vertrags gemäß § 134 BGB auszugehen.[565] Dass dies nur Forderungen gegen natürliche, nicht aber juristische Personen betreffen kann, ist entgegen dem BGH[566] Folge der klaren gesetzlichen Wertung, den Datenschutz im Rahmen der DS-GVO nur hinsichtlich der Daten natürlicher Personen auszugestalten. Da bei diesen das Datenschutzgrundrecht jedenfalls signifikant größere Bedeutung hat als bei juristischen Personen,[567] liegt hierin eine sachliche Rechtfertigung für die unterschiedliche Behandlung der jeweiligen Forderungstypen.

---

[561] BGH NJW 2007, 2106 Rn. 28 ff.

[562] BGH NJW 2007, 2106 Rn. 33.

[563] BGH NJW 2007, 2106 Rn. 31.

[564] Siehe dazu *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 516; vgl. auch BGH NJW 1957, 498 (499).

[565] Der BGH will eine Abwägung im Einzelfall hingegen verhindern, da diese in den nationalen Abtretungsbestimmungen (besonders §§ 354a HGB, 22d Abs. 4 KWG) nicht vorgesehen sei, BGH NJW 2007, 2106 Rn. 33; zustimmend *Stadler*, JA 2007, 896 (898); *Hennrichs/Pferdmenges*, LMK 2007, 233564. Dies ist mit dem Anwendungsvorrang des Unionsrechts jedoch nicht vereinbar. Die DS-GVO fordert, sofern keine andere Rechtsgrundlage einschlägig ist, klar eine Abwägung nach Art. 6 Abs. 1 lit. f DS-GVO. Diese wird jedoch im Regelfall zugunsten der Verarbeitung der für die Abtretung erforderlichen Daten ausgehen, so dass keine signifikante Rechtsunsicherheit zu befürchten ist.

[566] BGH NJW 2007, 2106 Rn. 31.

[567] EuGH, Urt. v. 9.11.2010 – Rs. C-92/09 und C-93/09 (*Schecke*) – Rn. 52 f.; vgl. auch

3. Zusammenfassung

Damit zeigt sich insgesamt, dass hinsichtlich der vertragsrechtlichen Folgen des Verstoßes gegen unionales Datenschutzrecht zu differenzieren ist. Verträge zwischen einem Verantwortlichen und einer betroffenen Person sind nach hier vertretener Auffassung, entgegen der herrschenden Meinung, nicht nach § 134 BGB nichtig, sodass insbesondere die Überlassung der Daten als Gegenleistung wirksam vereinbart werden kann. Dies folgt aus dem eigenständigen zivilrechtlichen Abwicklungsregime der DS-GVO und dem Umstand, dass eine Nichtigkeit des Vertrags die betroffene Person gegenüber einer Wirksamkeit schlechter stellen und damit die Schutzrichtung der DS-GVO ins Gegenteil verkehren würde. Allerdings können Einwilligung und Vertrag, unter bestimmten Bedingungen, über die Figur der Geschäftsgrundlage verknüpft sein.

Die Argumente gegen eine Anwendung von § 134 BGB greifen jedoch nicht bei Verträgen zwischen einem Verantwortlichen und einem Dritten, etwa im Bereich des Datenhandels. Hier führt der Verstoß gegen datenschutzrechtliche Vorschriften in der Tat zur Nichtigkeit gemäß § 134 BGB, da die DS-GVO für dieses Drittverhältnis kein eigenes privatrechtliches Sanktionsregime beinhaltet und der Vollzug des Vertrags die datenschutzrechtlichen Risiken für die betroffene Person noch vertiefen würde.

Im Verhältnis zwischen Verantwortlichem und betroffener Person führt dies mithin zu einer Entkopplung von Datenschutzrecht und Vertragsrecht. Der vordergründige Konflikt zwischen beiden Regimen ist jedoch hinzunehmen, da er gerade auf der Erstreckung datenschutzrechtlicher Wertungen in das Vertragsrecht beruht. Insofern kollidiert dieses Verständnis auch nicht mit dem Anwendungsvorrang des Unionsrechts.

II. Inhaltskontrolle im weiteren Sinne

Eine zweite, im Kontext der digitalen Wirtschaft besonders bedeutsame Wirksamkeitsbarriere stellt die Inhaltskontrolle von Einwilligungen und Vertragsklauseln dar. Eine Inhaltskontrolle ist grundsätzlich immer dann nicht notwendig, wenn die Voraussetzungen für eine informierte und freie Wahrnehmung privatautonomer Gestaltungsmacht durch die Parteien vorliegen.[568] Sie ist demgegenüber angebracht, wenn hinreichende Anhaltspunkte dafür bestehen, dass aufgrund von Marktversagen der private Aushandlungsmechanismus gestört ist.[569] Die viel beschworene Richtigkeitsgewähr[570] bzw. Richtigkeits-

Schneider, in: BeckOK DatenschutzR, 28. Ed. 2019, DS-GVO Grundlagen und bereichsspezifischer Datenschutz, Syst. B. Völker- und unionsrechtliche Grundlagen Rn. 26–28; siehe dazu auch bereits oben, Text bei § 4, Fn. 193.

[568] *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 320 ff.

[569] *Coester-Waltjen*, AcP 190 (1990), 1 (15 f.); *Rittner*, AcP 188 (1988), 101 (123); *Becker*, Der unfaire Vertrag, 2003, 6.

[570] *Schmidt-Rimpler*, AcP 147 (1941) 130 (149 ff.).

wahrscheinlichkeit[571] des Vertrags ist dann nicht mehr hinreichend hoch.[572] Die Analyse der Marktbedingungen digitaler Austauschprozesse im dritten Kapitel der Arbeit hat ergeben, dass in diesem Kontext mit vier verschiedenen Typen von Marktversagen gerechnet werden muss.[573] Daher kommt der Inhaltskontrolle in diesem Bereich eine gegenüber sonstigen Austauschprozessen erhöhte Dringlichkeit zu. Dies wird noch verstärkt durch den hier vertretenen subjektiven Erforderlichkeitsmaßstab bei Art. 6 Abs. 1 lit. b, Art. 7 Abs. 4 DS-GVO, welcher der zivilrechtlichen Wirksamkeitskontrolle eine zentrale Rolle hinsichtlich der datenschutzrechtlichen Zulässigkeit der Datenverarbeitung zuweist.[574] Nichtsdestoweniger ist bei der konkreten Anwendung der Inhaltskontrolle Zurückhaltung angebracht, da häufig nur schwer festzustellen ist, ob die fehlenden Voraussetzungen für die wirksame Ausübung von Privatautonomie tatsächlich kausal für die spezifische Vertragsklausel oder Einwilligung waren.

In dogmatischer Hinsicht vollzieht sich die Inhaltskontrolle nach deutschem Recht vor allem im Rahmen der AGB-Kontrolle nach den §§ 305 ff. BGB (1.). Daneben lassen jedoch auch § 138 BGB (2.) und § 242 BGB (3.) in gewissem Rahmen eine Inhaltskontrolle im Sinne einer rechtlichen Überprüfung des Inhalts von Vertragsbedingungen zu.[575] Dabei ist jeweils zwischen der Kontrolle einer Einwilligungserklärung einerseits und einem Vertrag andererseits zu unterscheiden. Ein Ziel muss insbesondere darin bestehen, datenschutzrechtliche Überraschungseffekte zu vermeiden, mit denen Verantwortlichen gewissermaßen durch die Hintertür von Art. 6 Abs. 1 lit. b DS-GVO ermöglicht wird, Verarbeitungen vorzunehmen, ohne dass die Schutzvorkehrungen des Einwilligungsregimes (besonders Art. 7 Abs. 3 und 4 DS-GVO) greifen.

1. AGB-Kontrolle

In der Rechtsprechung ist bereits seit langem anerkannt, dass nicht nur Vertragsklauseln, sondern auch einseitige Erklärungen wie die Einwilligung an den §§ 305 ff. BGB gemessen werden können.[576] Das LG Berlin hat gar An-

[571] *Schmidt-Rimpler*, in: Festschrift für Ludwig Raiser, 1974, 3 (12); vgl. auch *Wolf*, Rechtsgeschäftliche Entscheidungsfreiheit und vertraglicher Interessenausgleich, 1970, 73 f. („Richtigkeitschance").

[572] Siehe nur *Rittner*, AcP 188 (1988), 101 (128 f.); *Coester-Waltjen*, AcP 190 (1990), 1 (16); *Becker*, Der unfaire Vertrag, 2003, 6; *Grundmann*, in: Grundmann/Micklitz/Renner (Hrsg.), Privatrechtstheorie, Band I, 2015, 875 (879, 883); *Hacker*, Verhaltensökonomik und Normativität, 2017, 505 f.; *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 528.

[573] Siehe § 3 B.II.1.

[574] Siehe oben, Text bei § 4, Fn. 546.

[575] Zur Differenzierung zwischen der Inhaltskontrolle im engeren Sinne (§§ 305 ff., 242 BGB) und im weiteren Sinne (§§ 134, 138, 315 BGB) im Einzelnen *Fastrich*, Richterliche Inhaltskontrolle im Privatrecht, 1992, 5 f. Allerdings führt von den zuletzt genannten Normen, jedenfalls im hier verhandelten Kontext, nur § 138 BGB zu einer inhaltlichen Überprüfung einzelner Vertragsklauseln; § 315 BGB kann bei Rabattklauseln eine Rolle spielen, muss jedoch hier aus Gründen des Umfangs außen vor bleiben.

[576] Siehe sogleich ausführlich unter § 5 C.II.1.b).

fang 2018 weite Teile der von Facebook vorformulierten Einwilligungserklärung für gemäß § 307 Abs. 1 BGB unwirksam erklärt und damit einen Generalangriff auf das datenbasierte Geschäftsmodell gestartet.[577] Das KG hat dieses Urteil Ende 2019 vollumfänglich bestätigt.[578]

Für das Regime unter Geltung der DS-GVO ist nun einerseits zu klären, nach welchen Regeln diese Kontrolle von Einwilligungserklärungen fortan ablaufen kann. Andererseits müssen für Verträge spezifische Wirksamkeitsschranken, die sich aus der AGB-Kontrolle ergeben, erörtert werden, besonders im Kontext solcher Leistungspflichten, die zur Rechtfertigung der Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO führen können. Wie zu Beginn dieses Kapitels gesehen, stellt die Vereinbarung besonders weiter Leistungspflichten eine mögliche Strategie von Verantwortlichen dar, um die engen Vorgaben der DS-GVO teilweise außer Kraft zu setzen.

Dabei ist zunächst die Anwendbarkeit der AGB-Kontrolle neben der DS-GVO und der Grad ihrer Eigenständigkeit (a)) sowie die sachliche Anwendbarkeit insbesondere auf Einwilligungserklärungen zu klären (b)). Auf dieser Grundlage können dann die drei Kontrollebenen des AGB-Rechts, die Einbeziehungskontrolle (c)), die Transparenzkontrolle (d)) sowie die Inhaltskontrolle im engeren Sinne (e)), für datenbasierte Austauschprozesse fruchtbar gemacht werden. Neuere Rechtsprechung des EuGH ist insbesondere bei den AGB-rechtlichen Rechtsfolgen der Nichteinbeziehung oder Unwirksamkeit einer Klausel zu beachten (f)). Aus der Perspektive eines integrierten Marktordnungsrechts für digitale Austauschprozesse muss sich abschließend die Frage stellen, welche Wechselwirkungen zwischen der AGB-Kontrolle und dem unionalen Datenschutzrecht bestehen (g)). Eine Zusammenfassung beschließt den Abschnitt (h)).

a) Anwendbarkeit neben der DS-GVO

Anders als die zuvor in diesem Kapitel behandelten Phänomene im Schnittbereich von Datenschutzrecht und Zivilrecht stellt sich das Verhältnis von DS-GVO und AGB-Kontrolle primär nicht als ein Fall des Anwendungsvorrangs, sondern der Sachintegration dar. Denn die §§ 305 ff. BGB beruhen bekanntermaßen zum größten Teil, jedenfalls für Verbraucherverträge, ihrerseits auf der unionsrechtlichen Klauselrichtlinie. Dies macht eine Neubestimmung des überkommenen Verhältnisses zwischen Datenschutzrecht und AGB-Kontrolle notwendig, weil der BGH die Eigenständigkeit der AGB-Kontrolle gegenüber dem Datenschutzrecht unter Geltung der DSRL explizit verneint hatte. Nach den Entscheidungen in den Rechtssachen *Payback*[579] und *Happy-*

[577] LG Berlin MMR 2018, 328; dazu etwa *Rothmann/Buchner*, DuD 2018, 342; *Heldt*, MMR 2018, 333.

[578] KG MMR 2020, 239; zustimmend insoweit *Spittka*, GRUR-Prax 2020, 139; siehe auch KG BeckRS 2019, 8570 Rn. 66 ff.

[579] BGH NJW 2008, 3055 Rn. 15, 19.

Digits[580] sollte das BDSG den alleinigen Prüfungsmaßstab für die AGB-Kontrolle von Einwilligungserklärungen darstellen.

Diese Ansicht muss jedoch mit dem Geltungsbeginn der DS-GVO grundlegend revidiert werden. Schon nach allgemeinen Kriterien der unionsrechtlichen Sachintegration finden die §§ 305 ff. BGB neben der DS-GVO Anwendung, insoweit sie eigenständige Risiken adressieren, die in der DS-GVO nicht behandelt werden.[581] Dies ist für Verträge evidentermaßen der Fall, da insoweit Regelungen in der DS-GVO zur vertraglichen Wirksamkeit vollständig fehlen.[582] Dieses Ergebnis gilt jedoch letztlich auch für Einwilligungen. Das Regime der AGB-Kontrolle bildet das einzige zivilrechtliche Gebiet, auf dessen Regelungen in der DS-GVO hinsichtlich der Wirksamkeitsvoraussetzungen von Einwilligungen explizit verwiesen wird. Der dritte Satz des 42. Erwägungsgrunds der DS-GVO lautet: „Gemäß der Richtlinie 93/13/EWG des Rates sollte eine vom Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden, und sie sollte keine missbräuchlichen Klauseln beinhalten."

Die Bedeutung dieser ausdrücklichen Bezugnahme auf die Klauselrichtlinie ist jedoch im Einzelnen umstritten. Zum Teil wird angenommen, dass das AGB-Recht damit zu einer *lex specialis* gegenüber der DS-GVO werde.[583] Dies kann jedoch schon deshalb nicht überzeugen, weil der 42. Erwägungsgrund gerade nicht besagt, dass vorformulierte Einwilligungserklärungen hinsichtlich der in der Klauselrichtlinie enthaltenen Kriterien ausschließlich nach dieser zu beurteilen seien. Vielmehr erscheint eine parallele Anwendung von DS-GVO und AGB-Recht sachgerecht.[584] Dies erhellt schon daraus, dass Transparenzgebote in beiden Instrumenten vorhanden sind, die deutlich weniger detaillierten Transparenzpflichten der Klauselrichtlinie jedoch sicherlich nicht die Art. 12 ff. DS-GVO verdrängen sollen. Dies hätte die kontraintuitive Folge, dass im Bereich der vorformulierten Einwilligungserklärungen womöglich geringere Informationsanforderungen bestünden als bei individuell ausgehandelten Einwilligungserklärungen.

Die Regelungen der Klauselrichtlinie, und ihre Umsetzung im nationalen Recht, ergänzen daher richtigerweise die Regelungen der DS-GVO. Bedeutsam ist dieses Komplementärverhältnis insbesondere dort, wo keine eigenständigen Regelungen der DS-GVO existieren. Dies betrifft vor allem den zweiten Halbsatz des zitierten dritten Satzes des 42. Erwägungsgrunds: missbräuch-

---

[580] BGH NJW 2010, 864 Rn. 16.

[581] Siehe dazu ausführlich oben, § 5 A.II.2.b)bb)(2).

[582] *Indenhuck/Britz*, BB 2019, 1091 (1093).

[583] *Svantesson*, 34 Computer Law and Security Review 2018, 25 (31).

[584] So auch: *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (690) („concurrent, but substantively distinct, fairness assessments"); *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (170).

liche Klauseln. Mit Ausnahme des allgemeinen Fairnessgrundsatzes (Art. 5 Abs. 1 lit. a Var. 2 DS-GVO) enthält die Verordnung keinerlei Vorgaben für die Beurteilung von und den Umgang mit missbräuchlichen Einwilligungserklärungen.[585] Die Risiken, welche die Klauselrichtlinie adressiert – insbesondere die rationale Ignoranz von Vertragsklauseln durch Verbraucher[586] und die daraus folgende, nur unzureichend wettbewerblich disziplinierte einseitige Inanspruchnahme rechtsgeschäftlicher Gestaltungsmacht[587] –, spielen zwar grundsätzlich auch im Rahmen der DS-GVO in empirischer Hinsicht eine entscheidende Rolle, haben dort jedoch infolge des individuellen Kontrolldogmas keine eigenständige normative Regelung erfahren.[588] Nach den oben ausgearbeiteten Kriterien der Sachintegration[589] ergibt sich daraus, dass das AGB-Recht eine eigenständige Kontrolle vorformulierter Einwilligungsbedingungen unternehmen kann und dabei nicht an den Maßstab der DS-GVO gebunden ist. Auch eine Einwilligungserklärung, welche die Wirksamkeitsvoraussetzungen der DS-GVO erfüllt, kann daher aufgrund eines Verstoßes gegen AGB-rechtliche Normen unwirksam sein. Nur so lässt sich letztlich auch der Verweis im 42. Erwägungsgrund verstehen: Hätte die Klauselkontrolle neben der DS-GVO keine eigenständige Wirkung, so wäre der Verweis nicht nur überflüssig, sondern gar irreführend. Die Ansicht des BGH, wonach das Datenschutzrecht

[585] Auch Art. 7 Abs. 4 DS-GVO formuliert keinen Missbrauchstatbestand, sondern eine an der Vertragserforderlichkeit ausgerichtete Wirksamkeitsschranke, die zwar eine Form der Inhaltskontrolle von Einwilligungserklärungen ermöglicht, in den Kriterien aber gerade von Art. 307 ff. BGB unabhängig und verschieden ist; siehe oben, § 4 B.3.a)dd)(3) und *Hacker*, ZfPW 2019, 148 (183).

[586] Früh bereits *Adams*, in: Neumann (Hrsg.), Ansprüche, Eigentums- und Verfügungsrechte, 1983, 655 (663); siehe ferner *Wendland*, Vertragsfreiheit und Vertragsgerechtigkeit, 2019, 541 ff.; *Fastrich*, Richterliche Inhaltskontrolle im Privatrecht, 1992, 83, 86; *Beimowski*, Zur ökonomischen Analyse Allgemeiner Geschäftsbedingungen, 1989, 15, 18; *Fornasier*, Freier Markt und zwingendes Vertragsrecht, 2013, 155, 158; *Kötz*, JuS 2003, 209 (211 f.); *Eidenmüller*, JZ 2005, 216 (222); *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, Vor § 305 Rn. 4–6; *Stoffels*, JZ 2001, 843 (847); *Wackerbarth*, AcP 200 (2000), 45 (70); *Canaris*, AcP 200 (2000), 273 (323 f.); *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, 5. Aufl. 2012, 553 f.; *Drygala*, JZ 2012, 983 (984); *Leyens/Schäfer*, AcP 210 (2010), 771 (782 ff.); *Köndgen*, NJW 1989, 943 (946 f.); *Gottschalk*, AcP 206 (2006), 555 (560); *Leuschner*, AcP 207 (2007), 491 (503–505); *Fuchs*, in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016, Vorbemerkungen zur Inhaltskontrolle Rn. 34; *Hellgardt*, Regulierung und Privatrecht, 2016, 94; aA *Canaris*, NJW 1987, 609 (613).

[587] Die einseitige Inanspruchnahme vertraglicher Gestaltungsmacht stellt die hergebrachte Begründung der AGB-Kontrolle dar, siehe nur BT-Drucks. 7/3919, 15 f.; BGH NJW 1989, 222 (223); BGH NJW 1999, 3558 (3559); *Bieder*, AcP 216 (2016), 911 (912); *Fuchs*, in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016, Vorbemerkungen zur Inhaltskontrolle Rn. 26 f.; *Langhanke*, Daten als Leistung, 2018, 184. Diese Begründung weicht jedoch zunehmend der ökonomisch begründeten Verhinderung von Marktversagen, siehe § 5, Fn. 586; Kombination beider Elemente bei *Leuschner*, AcP 207 (2007), 491 (502–505).

[588] Allenfalls Art. 7 Abs. 4 DS-GVO könnte man hier anführen, der jedoch erkennbar andere Kriterien als die unangemessene Benachteiligung bzw. Missbräuchlichkeit bemüht.

[589] Siehe oben, § 5 A.II., dort besonders 2.b)bb)(2).

den alleinigen Maßstab für die Klauselkontrolle abgibt, muss daher aufgegeben werden.[590]

b) Sachliche Anwendbarkeit: Vertragsbedingungen

In sachlicher Hinsicht ist die AGB-Kontrolle nur anwendbar, wenn gemäß § 305 Abs. 1 S. 1 BGB für eine Vielzahl von Verträgen vorformulierte Vertragsbedingungen vorliegen, die eine Vertragspartei (Verwender) der anderen Vertragspartei bei Abschluss eines Vertrags stellt. Unter die Vertragsbedingungen fallen unproblematisch Klauseln schuldrechtlicher Verträge, die den Vertragsinhalt gestalten.[591] Aber auch einseitige Erklärungen des Verbrauchers wie die Einwilligung sind vom Begriff der Vertragsbedingung umfasst,[592] wenn sie im Zusammenhang mit einem Vertragsverhältnis oder einer rechtlichen Sonderverbindung stehen.[593] Denn auch darin liegt letztlich eine einseitige Inanspruchnahme vertraglicher Gestaltungsmacht durch den Verwender,[594] die infolge der rationalen Ignoranz der Vertragsbedingungen durch die Verbraucher nur unzureichend durch den Markt für Vertragskonditionen diszipliniert wird. Allerdings liegt keine Vertragsbedingung mehr vor, wenn ein bloßer Hinweis auf die Rechtslage oder eine reine Beschreibung von Tätigkeiten ohne eigenständigen rechtlichen Regelungsgehalt erfolgt, was sich jeweils aus Sicht des objektiven Durchschnittsempfängers beurteilt.[595] Dies impliziert, dass Datenschutzerklärungen, soweit sie, wie in der Praxis häufig, lediglich deskriptiv die Datenverarbeitung umschreiben, keine Vertragsbedingungen darstellen.[596] Sofern sie jedoch nach dem objektiven Empfängerhorizont Bedingungen für die Inanspruchnahme der Dienstleistung darstellen, muss wiederum von einer Vertragsbedingung gesprochen werden. Dabei ist es unerheblich, ob die Erklärung als bloße „Richtlinie" bezeichnet wird.[597] Letztlich ist damit jede datenschutzrechtliche Einwilligungserklärung, die über Deskription hinausgeht und vom Verwender gestellt wird, vom sachlichen Anwendungsbereich der AGB-Kontrolle nach § 305 Abs. 1 S. 1 BGB umfasst.

---

[590] Ähnlich *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3748 f.); *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (170); siehe auch bereits *Hacker*, ZfPW 2019, 149 (186).

[591] *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 305 Rn. 9.

[592] So bereits ausdrücklich BGH NJW 1986, 46 (47) zur datenschutzrechtlichen Einwilligung zuletzt BGH GRUR 2020, 891 Rn. 43.

[593] BGH NJW 2008, 3055 Rn. 18; BGH NJW 2010, 864 Rn. 15; BGH NJW 2013, 2683 Rn. 20; LG Berlin MMR 2018, 328 Rn. 57; *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 305 Rn. 9; *Nietsch*, CR 2014, 272 (276); *Langhanke*, Daten als Leistung, 2018, 203.

[594] Vgl. BGH NJW 1989, 222 (223); BGH NJW 2008, 3055 Rn. 18.

[595] BGH NJW 2014, 2269 Rn. 24; KG MMR 2020, 239 Rn. 61; *Nietsch*, CR 2014, 272 (275).

[596] *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3748).

[597] BGH NJW 2014, 2269 Rn. 29; aA LG Berlin, Urt. v. 16.1.2018, BeckRS 2018, 1060 Rn. 78.

c) Einbeziehungskontrolle

Die Einbeziehungskontrolle stellt strenge Voraussetzungen an die Vereinbarung von AGB. Sie ist der Transparenzkontrolle und der Inhaltskontrolle im engeren Sinne vorgeschaltet[598] und bedingt vornehmlich, dass der Vertragspartner des Verwenders eine zumutbare Möglichkeit der Kenntnisnahme der AGB vor Vertragsschluss haben muss (§ 305 Abs. 2 Nr. 2 BGB) und überraschende Klauseln nicht Vertragsinhalt werden (§ 305c Abs. 1 BGB). Beide Ausprägungen, die positive und die negative Einbeziehungskontrolle,[599] sind im Rahmen digitaler Austauschverhältnisse und der hier im Fokus stehenden drei Leitfälle relevant.

aa) Zumutbare Möglichkeit der Kenntnisnahme, § 305 Abs. 2 Nr. 2 BGB

Nach § 305 Abs. 2 BGB werden AGB nur Vertragsbestandteil, wenn auf sie bei Vertragsschluss ausdrücklich hingewiesen wurde (Nr. 1) und eine zumutbare Möglichkeit der Kenntnisnahme besteht (Nr. 2). Die Regelung basiert jedenfalls teilweise auf dem 20. Erwägungsgrund der Klauselrichtlinie, nach dem die Vertragspartei die tatsächliche Möglichkeit der Kenntnisnahme der Vertragsbedingungen haben muss.

Hinsichtlich der Einwilligung enthält hier jedoch bereits die DS-GVO Vorgaben zu Informiertheit, Bestimmtheit und Separierung (vor allem Art. 4 Nr. 11, 7 Abs. 2 S. 1 DS-GVO), neben denen weitere Kriterien keinen Platz haben. Denn die Risiken mangelnder Information über Existenz und Inhalt der Einwilligung werden damit abschließend adressiert. Inhaltlich jedoch gleichen sich die Regelungen insoweit, als wie gesehen im Rahmen der Informiertheit der Einwilligung ebenfalls die zumutbare Kenntnisnahmemöglichkeit genügt.[600]

Die genannten Vorschriften der DS-GVO beziehen sich jedoch nur auf die Einwilligung. Wie bereits mehrfach erwähnt, enthält die DS-GVO keine Kriterien für den Abschluss und die Wirksamkeit von Verträgen, auf deren Grundlage eine Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO erfolgen soll. Daher wiederholt sich hier, wenngleich im Rahmen von § 305 Abs. 2 Nr. 2 BGB anstelle von Art. 4 Nr. 11 DS-GVO, die Problematik, gegenüber Dritten eine hinreichende Kenntnisnahmemöglichkeit zu gewährleisten. Dies ist vor allem im dritten Leitfall relevant, wenn etwa IoT-Geräte Daten von Nicht-Primärnutzern erheben. Sofern hier überhaupt ein Vertrag angenommen wer-

598 *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 57; *Schumacher*, MDR 2002, 973 (977).

599 Begriffe bei *Schmidt*, NJW 2011, 1633 (1635 f.); *Schmidt*, in: BeckOK BGB, 51. Ed. 2019, § 305c Rn. 9; teilweise wird auch nur § 305 Abs. 2 BGB als Einbeziehungskontrolle bezeichnet (*Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 305c Rn. 4), was hier jedoch nicht weiter vertieft werden muss.

600 Siehe oben, § 4 B.I.3.a)cc)(2).

den kann, dürfte die Einbeziehung von AGB häufig an § 305 Abs. 2 Nr. 2 BGB scheitern, da die Dritten vor Nutzung des Geräts typischerweise nicht in zumutbarer Weise auf die Nutzungsbedingungen zugreifen können. Insofern gilt das zur Möglichkeit der Kenntnisnahme der einwilligungsbezogenen Informationen Gesagte entsprechend.[601]

bb) Überraschende Klauseln, § 305c Abs. 1 BGB

Auch bei zumutbarer Möglichkeit der Kenntnisnahme werden gemäß § 305c Abs. 1 BGB solche Klauseln nicht Vertragsbestandteil, die einen für den Vertragspartner des Verwenders überraschenden Inhalt haben. Dies beurteilt sich nach dem Gesetz danach, ob „nach den Umständen, insbesondere nach dem äußeren Erscheinungsbild des Vertrags, [die Bestimmungen] so ungewöhnlich sind, dass der Vertragspartner des Verwenders mit ihnen nicht zu rechnen braucht." Der BGH nimmt dies an, „wenn die Regelung von seinen berechtigten Erwartungen, wie sie sich nach den allgemeinen und individuellen Begleitumständen des Vertragsschlusses ergeben, deutlich abweicht."[602]

Auf die Einwilligung passt § 305c Abs. 1 BGB allerdings insofern seinem Wortlaut nach nicht, als diese, wie gesehen, vom Vertrag streng zu trennen ist und gerade nicht Vertragsbestandteil werden soll. Sofern die Einwilligung in einzelnen Vertragsklauseln versteckt ist, wird man annehmen müssen, dass Art. 7 Abs. 2 S. 1 DS-GVO abschließend ist.[603] Man könnte § 305c Abs. 1 BGB in diesem Kontext allenfalls dergestalt analog anwenden, dass einzelne Klauseln einer aus mehreren Klauseln bestehenden Einwilligung bei überraschendem Inhalt nicht Teil der Einwilligung werden.

Auch dies ist jedoch entbehrlich. Ein Verbot überraschender Klauseln ergibt sich für die Einwilligung zwar nicht ausdrücklich aus der DS-GVO. Nach ihrem 47. Erwägungsgrund sind die vernünftigen Erwartungen der betroffenen Person nur bei der Interessenabwägungsklausel nach Art. 6 Abs. 1 lit. f DS-GVO zu berücksichtigen. Allerdings dürfte insofern gelten, dass eine Klausel, die innerhalb einer Einwilligung an einer Stelle verortet wird, an welcher der Nutzer mit ihr nicht rechnen muss, gegen das Transparenzgebot aus Art. 12 Abs. 1 DS-GVO und damit die Informiertheit der Einwilligung verstößt.[604] Für eine analoge Anwendung von § 305c Abs. 1 BGB auf die Einwilligungserklärung fehlt es insoweit an der Regelungslücke.[605] Daher ist auch das Ver-

---

[601] Siehe oben, § 4 B.I.3.a)cc)(3)(c).

[602] BGH NJW 2002, 2710 (2711); siehe auch *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 305c Rn. 6–10.

[603] Vgl. zu § 4a Abs. 1 S. 4 BDSG aF insoweit *Langhanke*, Daten als Leistung, 2018, 205.

[604] Vgl. *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 1, 2018, 8 Rn. 10.

[605] *Becker* JZ 2017, 170 (173) möchte hingegen möchte „unklare oder pauschale Formulierungen" in Einwilligungen wegen der „sehr weiten Deutungsmöglichkeiten" an § 305c Abs. 1 BGB scheitern lassen.

bot überraschender Klauseln nach § 305c Abs. 1 BGB nur für Vertragsklauseln relevant.

(1) Datenschutzrechtlicher Überraschungseffekt?

Grundsätzlich bestehen dabei keine Besonderheiten gegenüber solchen Vertragsklauseln, die nicht Grundlage einer Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO sind. Allerdings lässt sich fragen, ob die datenschutzrechtliche Legitimierungswirkung selbst ein hinreichendes Überraschungsmoment nach § 305c Abs. 1 BGB begründen kann.[606] Denn dem durchschnittlichen Nutzer wird nicht unbedingt bewusst sein, dass eine Klausel, in der sich der Anbieter zu personalisierter Werbung verpflichtet, zugleich den Effekt haben kann, die dafür erforderliche Verarbeitung personenbezogener Daten zulässig zu machen. Insofern hilft auch die Information nach Art. 13 Abs. 1 lit. c DS-GVO dahingehend, dass eine Verarbeitung auf vertraglicher Grundlage erfolgt, nur sehr eingeschränkt, da diese Information typischerweise nicht in direktem Zusammenhang mit der Vertragsklausel erteilt wird, sondern in einem von den Nutzungsbedingungen separaten Dokument (etwa der Datenschutzrichtlinie).

Daher muss die Klausel, welche eine Datenverarbeitung ermöglicht, erstens salient innerhalb der AGB platziert sein. Dies folgt aus ihrer durch die Legitimierungswirkung verstärkten Bedeutung. Der Nutzer muss nicht damit rechnen, dass derartige Klauseln an wenig prominenter Stelle innerhalb der AGB, beispielsweise zwischen Haftungsbeschränkungen, Platz finden. Zweitens ist zu erwägen, ob unter bestimmten Umständen expliziert werden muss, dass die jeweilige Leistungspflicht impliziert, dass die dafür erforderlichen personenbezogenen Daten nach Art. 6 Abs. 1 lit. b DS-GVO verarbeitet werden dürfen. Wenn etwa eine atypische, weite Leistungspflicht vereinbart wird, die nicht Teil der vom Nutzer typischerweise erwarteten Hauptleistungspflicht ist, aber Datenverarbeitungen legitimiert, mit deren Verarbeitung gerade auf *vertraglicher* Grundlage der durchschnittliche Nutzer nicht zu rechnen braucht, könnte ein erklärender Zusatz innerhalb der AGB, im unmittelbaren Anschluss an die Klausel, vonnöten sein.

So sehr dies zu begrüßen wäre, so wenig ist dies jedoch mit Blick auf die Rechtsfolgen mit dem Schutz des Vertragspartners des Verwenders zu vereinbaren. Denn unterbliebe ein gesetzlich erforderlicher Hinweis, so würde die Klausel nicht Vertragsbestandteil. Dies könnte allerdings zur Folge haben, dass für den Kunden eigentlich positive Leistungspflichten des Anbieters ausgeschlossen werden. Gerechtfertigt ist dies jedoch nur dann, wenn die Klausel, unter Berücksichtigung der datenschutzrechtlichen Legitimierungswirkung, insgesamt eine unangemessene Benachteiligung des Nutzers darstellt.

606 So bereits *Hacker*, ZfPW 2019, 148 (190).

Dies wiederum ist eine Frage der Inhaltskontrolle, nicht der Einbeziehungskontrolle.[607] Auch lässt sich nicht argumentieren, dass die Leistungspflicht bestehen bleiben, der Klausel hingegen isoliert die datenschutzrechtliche Legitimierungswirkung genommen werden soll. Denn damit wäre nichts gewonnen, weil die Leistungspflicht gerade nur durch die Verarbeitung personenbezogener Daten überhaupt erfüllt werden kann. Nur insoweit gilt ja Art. 6 Abs. 1 lit. b DS-GVO. Insgesamt dürfte daher alleine der Überraschungseffekt hinsichtlich der Legitimierungswirkung nicht genügen, um eine Klausel an § 305c Abs. 1 BGB scheitern zu lassen.

(2) Einbeziehung Dritter

Anders ist die rechtliche Situation hingegen zu beurteilen, wenn Anbieter versuchen, Drittanbieter im Wege von AGB als Vertragspartner zu etablieren.[608] So könnte etwa eine Webseite in den Nutzungsbedingungen festhalten, dass durch die Akzeptanz der Nutzungsbedingungen (im Wege der Stellvertretung) ein separater Vertrag zwischen dem Nutzer und dem Anbieter von Drittanbietercookies zustande kommt, um insofern die Legitimierungswirkung von Art. 6 Abs. 1 lit. b DS-GVO auszulösen. Sofern jedoch der Drittbezug für den Nutzer im Rahmen des bestimmungsgemäßen Umgangs mit dem jeweiligen Produkt des Erstanbieters vor Akzeptanz der Nutzungsbedingungen nicht erkennbar ist, liegt in der Einbeziehung Dritter als Vertragspartner ein hinreichender Überraschungseffekt, der die Folge des § 305c Abs. 1 BGB auslöst. Denn der Nutzer muss regelmäßig nicht damit rechnen, dass ihm unbekannte Dritte in die Vertragsbeziehung zum Erstanbieter einbezogen werden bzw. mit diesen separate Verträge geschlossen werden.[609] Soll daher ein mehrseitiger Vertrag unter Einbeziehung des Dritten oder ein separater Vertrag mit diesem abgeschlossen werden, so müssen dieser Umstand und die Identität des Dritten dem Nutzer gegenüber klar und salient auch außerhalb der Nutzungsbedingungen benannt werden. Die Erstreckung eines Vertrags auf Dritte lediglich im Wege der AGB ist daher wegen der damit verbundenen datenschutzrechtlichen Risiken nicht möglich.

d) Transparenzkontrolle

Ist eine Klausel in einen Vertrag einbezogen bzw. vereinbart, so unterscheidet die AGB-Kontrolle bekanntermaßen mit der Transparenzkontrolle (primär lokalisiert in § 307 Abs. 1 S. 2 BGB) einerseits und der Inhaltskontrolle im engeren Sinne (§§ 307 Abs. 1 und 2, 308 f. BGB) andererseits zwei verschiedene Beur-

[607] Zur Vermengung von Wertungen von § 305c Abs. 1 BGB und § 307 BGB *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 305c Rn. 4.

[608] Siehe zu den vertraglichen Konstruktionsmöglichkeiten oben, § 5 B.III.2.a).

[609] Siehe oben, § 5 B.III.2.a)aa) und bb).

teilungsmechanismen.[610] Für alle der AGB-Kontrolle unterfallenden Vertragsbedingungen gilt gemäß § 307 Abs. 1 S. 2 BGB das Transparenzgebot. Danach müssen die Bestimmungen klar und verständlich sein. Ziel dieser durch die Klauselrichtlinie vorgegebenen Norm ist es, sicherzustellen, dass sich jedenfalls theoretisch der einzelne Verbraucher, oder zumindest eine „informierte Minderheit",[611] über den Vertragsinhalt informieren kann, um darauf bezogen eine Auswahlentscheidung zwischen verschiedenen Anbietern durchzuführen.[612] Dadurch soll Konditionenwettbewerb unterstützt werden.[613] Dies impliziert allerdings, dass „der Vertragsinhalt [dem Vertragspartner des Verwenders] ein vollständiges und wahres Bild vermittelt und ihn so auch zum Marktvergleich befähigt."[614] Genau dies soll das Transparenzgebot sicherstellen.

Wenngleich die rationale Ignoranz von AGB derjenigen von datenschutzrechtlichen Einwilligungserklärungen in empirischer Hinsicht in nichts nachsteht,[615] so reproduziert die Rechtsprechung in dogmatischer Hinsicht bei Prüfung von Einwilligungserklärungen im Rahmen des Transparenzgebots nichtsdestoweniger mit bemerkenswerter Akribie die aus dem Datenschutzrecht bekannten Informationspflichten. Einwilligungserklärungen scheitern in der Praxis, im Rahmen der AGB-Kontrolle, häufig am Transparenzgebot, hinsichtlich dessen auf die Anforderungen für eine informierte Einwilligung nach dem Datenschutzrecht verwiesen wird.[616] Sind die Informationspflichten nach dem Datenschutzrecht verletzt, so wird ohne Umschweife auf eine Verletzung des AGB-rechtlichen Transparenzgebots und damit die Unwirksamkeit der Einwilligung geschlossen. Dies ist insofern misslich, als eine erhöhte Transparenz an dem eigentlichen AGB-relevanten Marktversagen, rationaler Ignoranz wegen prohibitiver Informationskosten, nichts ändert,[617] sodass letztend-

[610] *Gottschalk*, AcP 206 (2006), 555 (560 ff.); *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 23.

[611] Zur Verhinderung von informationellem Marktversagen durch eine informierte Minderheit grundlegend aus theoretischer Perspektive *Schwartz/Wilde*, 127 University of Pennsylvania Law Review 1979, 630; siehe auch *Gottschalk*, AcP 206 (2006), 555 (564); *Beimowski*, Zur ökonomischen Analyse Allgemeiner Geschäftsbedingungen, 1989, 108 f.; zur empirischen Unhaltbarkeit dieser These jedenfalls für AGB von Endnutzerverträgen *Bakos/Marotta-Wurgler/Trossen*, 43 The Journal of Legal Studies 2014, 1; ferner allgemeiner *Wagner/Eidenmüller*, 86 University of Chicago Law Review 2019, 581 (607); siehe auch *Hacker*, Verhaltensökonomik und Normativität, 2017, 657.

[612] *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 56.

[613] *Gottschalk*, AcP 206 (2006), 555 (563); *Köndgen*, NJW 1989, 943 (947).

[614] BGH NJW-RR 2008, 251 (253).

[615] Dazu unten, § 4 B.II.4.

[616] Siehe etwa LG Berlin, MMR 2018, 328 Rn. 65, 68; KG ZD 2018, 118 Rn. 84 f.; LG Berlin MMR 2014, 563 (565); LG Berlin NJW 2013, 2605 (2606); ÖOGH, Urt. v. 13.9.2001, 6 Ob 16/01y, Klausel 9; siehe auch, zu weiteren Entscheidungen des ÖOGH, *Langhanke*, Daten als Leistung, 2018, 212 ff.; siehe ferner auch KG BeckRS 2019, 8570 Rn. 84 zu einem wegen Überkomplexität insgesamt unwirksamen Regelwerk zur Datenerhebung und -verwendung.

[617] *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 58; aA *Köndgen*, NJW 1989, 943 (947); *Bieder*, AcP 216 (2016), 911 (927), allerdings ohne Würdigung der empirischen Forschung zu rationaler Ignoranz, die auch durch erhöhte Transparenz nicht überwindbar ist,

lich, wenn die Klausel mit dem Transparenzgebot in Einklang gebracht wurde, doch über die Vereinbarkeit mit den Vorgaben der Inhaltskontrolle im engeren Sinn zu entscheiden ist.[618]

In dogmatischer Hinsicht ist dazu anzumerken, dass die Informationspflichten nach dem Datenschutzrecht mit denjenigen des AGB-Rechts in der Tat im Wesentlichen deckungsgleich sind.[619] Nach § 307 Abs. 1 S. 2 BGB muss eine Bestimmung in AGB „klar und verständlich" sein. Der EuGH hat dazu entschieden, dass dies impliziert, dass die Klausel „nicht nur in grammatikalischer Hinsicht für den Verbraucher nachvollziehbar sein muss", sondern dass der Verbraucher in der Lage sein muss, „die sich für ihn daraus ergebenden wirtschaftlichen Folgen auf der Grundlage genauer und nachvollziehbarer Kriterien einzuschätzen."[620] In ähnlicher Weise formuliert Art. 12 Abs. 1 DS-GVO, dass alle verarbeitungsbezogenen Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" übermittelt werden müssen.

Damit muss es jedoch auch sein Bewenden haben. Mit Art. 12–14 DS-GVO, und dem in Art. 16 Abs. 2 AEUV, Art. 16 GRCh verankerten freien Datenverkehr, ist es nach hier vertretener Auffassung nicht mehr vereinbar, die Intransparenz des „Datenpreises" an einem mangelnden Wertmaßstab für personenbezogene Daten festmachen[621] und über diesen Weg die AGB-rechtliche Unwirksamkeit etwaiger datenbasierter Preisabreden herbeiführen zu wollen.[622] Denn die Möglichkeit, Daten im Rahmen monetär kostenloser Vertragsverhältnisse zu überlassen, wurde von der DS-GVO klar gesehen und nicht grundsätzlich in Frage gestellt.[623] Daher ist auch die Anwendbarkeit der Preisangabenverordnung auf den Datenpreis, wenn man sie überhaupt tatbestandlich für einschlägig hält, durch den Anwendungsvorrang des Unionsrechts bzw., hinsichtlich ihrer unionsrechtlichen Komponenten,[624] durch den sach-

---

siehe etwa *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S41; ferner auch *Adams*, in: Neumann (Hrsg.), Ansprüche, Eigentums- und Verfügungsrechte, 1983, 655 (664 f., 670 ff.).

618 Siehe nur die Abfolge der Urteile BGH NJW 2001, 2012 (2013) und BGH NJW 2005, 3559 (3565).

619 Die von *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (689) ausgemachten Unterschiede erscheinen rein sprachlicher Natur und ändern nach hiesiger Auffassung nichts an der sachlichen Kongruenz. Insbesondere muss auch nach dem 20. Erwägungsgrund der Klauselrichtlinie der Verbraucher die tatsächliche Möglichkeit der Kenntnisnahme haben, was in § 305 Abs. 2 Nr. 2 BGB festgehalten ist. Insofern ist die leichte Zugänglichkeit, die Art. 12 Abs. 1 DS-GVO stipuliert, kein Alleinstellungsmerkmal der DS-GVO.

620 EuGH, Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 75.

621 Zur Bewertung personenbezogener Daten ausführlich *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen); *Malgieri/Custers*, 34 Computer Law & Security Review 2018, 289 (294 ff.).

622 Siehe aber, unter Verweis auf Art. 119 f. AEUV, *Schwintowksi*, NJOZ 2018, 841 (847).

623 Siehe nur den 6. und 7. Erwägungsgrund; siehe auch § 4, Fn. 679.

624 Zu diesen *Ernst*, in: MüKo, Lauterkeitsrecht, 2. Aufl. 2014, PAngV, Einleitung Rn. 8.

integrativen Vorrang der DS-GVO gesperrt.[625] Somit lässt sich festhalten, dass typischerweise bei der Verletzung der Kriterien der informierten Einwilligung auch eine Verletzung des Transparenzgebots im Rahmen der AGB-Kontrolle angenommen werden kann. Umgekehrt impliziert bei der Einwilligungserklärung eine Wahrung der ungleich detaillierteren Transparenzvorgaben der DS-GVO auch eine Einhaltung des AGB-rechtlichen Transparenzgebots.

Allerdings ist damit auch dogmatisch in der Sache letztlich nichts gewonnen. Denn eine Einwilligung, die nach datenschutzrechtlichen Maßstäben nicht informiert erfolgt, ist bereits wegen Verstoßes gegen die DS-GVO unwirksam. Dies hindert zwar eine Unwirksamkeit auch gemäß § 307 Abs. 1 BGB nicht.[626] Dass ein Rechtsgeschäft (und damit auch eine geschäftsähnliche Handlung) aus mehreren Gründen nichtig sein kann,[627] ist gerade der dogmatische Ertrag der Diskussion um die Lehre von der Doppelwirkung im Recht.[628] Weder das Datenschutzrecht noch das AGB-Recht ist zeitlich oder logisch prioritär. Jedoch sind die datenschutzrechtlichen Informationsvorgaben, wie gesehen, deutlich detaillierter.[629] Das AGB-Recht reproduziert damit lediglich das datenschutzrechtliche Verdikt, ohne dass ihm eine eigenständige Bedeutung zukäme. Denn auch die Klagebefugnis von Verbraucherverbänden und anderen qualifizierten Einrichtungen (§ 3 UKlaG), die früher lediglich bei Verstößen gegen die §§ 305 ff. BGB bestand (§ 1 UKlaG), ist mittlerweile durch § 2 Abs. 1 S. 1 i. V. m. Abs. 2 S. 1 Nr. 11 UKlaG auf datenschutzrechtliche Verstöße im geschäftlichen Bereich ausgedehnt worden.[630] Damit ist die zusätzliche AGB-rechtliche Transparenzkontrolle bei Einwilligungen neben den Anforderungen der DS-GVO nur noch von akademischem Interesse.

Lediglich bei Vertragsklauseln erfüllt sie einen eigenständigen Zweck, da die DS-GVO insofern kein Transparenzgebot enthält. Art. 12–14 DS-GVO beziehen sich nur auf Informationen zur Datenverarbeitung selbst, nicht aber auf die Formulierung der Vertragsklauseln, welche eine Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO ermöglichen. Hier ergeben sich jedoch gegenüber der üblichen vertragsrechtlichen Transparenzkontrolle keine Besonderheiten. Denn der Umstand, dass die Vertragsklauseln Grundlage einer Datenverarbeitung sind, muss bereits nach Art. 13 Abs. 1 lit. c DS-GVO der betroffenen Person mitgeteilt werden und begründet, wie gesehen, auch keinen Überraschungs-

---

625 Für eine Kontrolle am Maßstab der PAngV aber *Schwintowksi*, NJOZ 2018, 841 (847 f.), allerdings ohne Problematisierung eines Anwendungsvorrangs.

626 So ausdrücklich zur Nichtigkeit nach § 307 Abs. 1 BGB und § 125 S. 1 BGB BGH NJW-RR 2017, 114 Rn. 21 f.

627 BGH NJW 1986, 46 (47) zur Unwirksamkeit nach BDSG aF und AGB-Recht; BGH NJW-RR 2017, 114 Rn. 22 zu § 125 S. 1 BGB und AGB-Recht; *Schreiber*, AcP 211 (2011), 35 (40); *Herbert*, JZ 2011, 503 (506); *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 142 Rn. 12.

628 Dazu bereits oben, § 5 B.II.2.e)aa)(2).

629 *Helberger/Zuiderveen Borgesius/Reyna*, 54 Common Market Law Review 2017, 1427 (1438).

630 Dazu etwa *Ritter/Schwichtenberg*, VuR 2016, 95.

effekt nach § 305c Abs. 1 BGB. Letztlich dienen diese Transparenzvorgaben, wie auch bei der Einwilligung, bei empirischer Betrachtung lediglich Informationsintermediären.[631]

e) Inhaltskontrolle

Dieses Bild ändert sich, wenn man die Inhaltskontrolle im engeren Sinne (§§ 307 Abs. 1 und 2, 308 f. BGB) in den Blick nimmt. Es wird sich zeigen, dass hier Raum für eine eigenständige Bewertung von Einwilligungserklärungen und Vertragsklauseln besteht, die über einen reinen Nachvollzug des Datenschutzrechts hinauszugehen vermag. Dafür muss jedoch zunächst geklärt werden, inwiefern derartige Erklärungen kontrollfähig gemäß § 307 Abs. 3 S. 1 BGB sind (aa)). Erst dann können Grundsätze der Unangemessenheit für Klauseln, die zumindest teilweise die Hauptleistungspflichten eines Vertrags konturieren, entwickelt (bb)) und auf die drei Leitfälle angewendet werden (cc)).

aa) Kontrollfähigkeit, § 307 Abs. 3 S. 1 BGB

Die Kontrollfähigkeit von Klauseln und Einwilligungserklärungen, die digitale Austauschprozesse gestalten, ist besonders begründungsbedürftig, wenn sie nicht nur im ökonomischen, sondern auch im rechtlichen Sinne Teil der Hauptleistung des Vertrags sind. Dies betrifft vor allem das Geschäftsmodell, bei dem Daten als Gegenleistung eingesetzt werden.

(1) Grundsatz: Mangelnde Kontrollfähigkeit des Hauptgegenstands des Vertrags und des Preis-/Leistungsverhältnisses

Die Inhaltskontrolle im engeren Sinne findet gemäß § 307 Abs. 3 S. 1 BGB nur Anwendung auf AGB, „durch die von Rechtsvorschriften abweichende oder diese ergänzende Regelungen vereinbart werden." Diese Bestimmung ist jedoch richtlinienkonform auszulegen, da sie Art. 4 Abs. 2 der Klauselrichtlinie umsetzt.[632] Danach gilt:

„Die Beurteilung der Mißbräuchlichkeit der Klauseln betrifft weder den Hauptgegenstand des Vertrages noch die Angemessenheit zwischen dem Preis bzw. dem Entgelt und den Dienstleistungen bzw. den Gütern, die die Gegenleistung darstellen, sofern diese Klauseln klar und verständlich abgefaßt sind."

Zwar enthält die Klauselrichtlinie lediglich eine Mindestharmonisierung, sodass die Mitgliedstaaten frei sind, auch die Hauptleistungspflichten und das Preis-/Leistungsverhältnis der Klauselkontrolle zu unterwerfen (Art. 8 der Klauselrichtlinie). In Deutschland hingegen ist dies mit § 307 Abs. 3 S. 1 BGB nicht geschehen, da jedenfalls grundsätzlich gerade keine dispositiven Regeln

631 *Helberger/Zuiderveen Borgesius/Reyna*, 54 Common Market Law Review 2017, 1427 (1442); siehe auch oben, § 4 B.I.5.b).

632 Siehe nur *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 4.

hinsichtlich der Ausgestaltung des vertraglichen Hauptgegenstands und des Preis-/Leistungsverhältnisses existieren.[633] Vielmehr sollen der Preis und die (primären) Leistungsangebote kontrollfrei bleiben.[634] Damit wird die Kontrolle von AGB problematisch, in denen, schuldrechtlich gesehen, Hauptleistungspflichten vereinbart werden. Wie erörtert, betrifft dies im Rahmen des Geschäftsmodells von Daten als Gegenleistung zwei mögliche Gegenleistungspflichten (bzw. -bedingungen[635]): die Pflicht zur Abgabe einer Einwilligung und die Pflicht zur Überlassung von Daten.[636]

Die EuGH-Rechtsprechung zu Art. 4 Abs. 2 der Klauselrichtlinie ist für die richtlinienkonforme Auslegung von § 307 Abs. 3 S. 1 BGB unmittelbar relevant. Der EuGH hat in den Rechtssachen *Kásler* und *Matei* festgestellt, dass der Hauptgegenstand des Vertrags nur Klauseln umfasst, welche die Hauptleistungspflichten des Vertrags festlegen und den Vertrag als solche charakterisieren, nicht hingegen akzessorische Klauseln.[637] Auch die Ausnahme des Preis-/Leistungsverhältnisses habe lediglich eine „eingeschränkte Tragweite".[638] Sie setze zudem weiter voraus, dass für die jeweilige Preiskomponente durch den Unternehmer eine spezifische Leistung erbracht wird.[639]

Diese interpretatorischen Maßstäbe des EuGH deuten zugleich an, dass der Begriff des Hauptgegenstands des Vertrags der Klauselrichtlinie nicht notwendig mit dem Begriff der Gegenleistung nach deutschem Recht identisch sein muss.[640] Dies folgt nicht nur daraus, dass der Richtlinienbegriff ohnehin autonom auszulegen ist,[641] sondern vor allem aus der spezifischen Funktion der beiden Begriffe im digitalen Kontext. Der Begriff des Hauptgegenstands des Vertrags ist nach dem EuGH als Ausnahmebestimmung eng auszulegen.[642] Der Begriff der Gegenleistung hingegen dürfte, jedenfalls in digitalen Aus-

---

633 Siehe nur BGH NJW 1989, 222 (223); BGH NJW 1992, 688 (689); *Fornasier*, Freier Markt und zwingendes Vertragsrecht, 2013, 197.

634 So ausdrücklich die Gesetzesbegründung des AGB-Gesetzes, BT-Drucks. 7/3919, 22.

635 Bei funktionaler Auslegung kann es für die AGB-Kontrolle keinen Unterschied machen, ob eine synallagmatische oder eine konditionale Verknüpfung von Leistung und Gegenleistung vorliegt.

636 Siehe oben, Text bei § 4, Fn. 670.

637 EuGH, Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 49 f.; Urt. v. 26.2.2015 – Rs. C-143/13 (*Matei*) – Rn. 54.

638 EuGH, Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 54; Urt. v. 26.2.2015 – Rs. C-143/13 (*Matei*) – Rn. 55.

639 Urt. v. 26.2.2015 – Rs. C-143/13 (*Matei*) – Rn. 70; siehe auch bereits EuGH, Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 68.

640 *Hacker*, ZfPW 2019, 148 (187).

641 EuGH, Urt. v. 1.12.2016 – Rs. C-395/15 (*Daouidi*) – Rn. 50; EuGH, Urt. v. 1.10.2019 – Rs. C-673/17 (*Planet49*) – Rn. 47; *Kaufmann*, in: Dauses/Ludwigs (Hrsg.), Handbuch des EU-Wirtschaftsrechts, 48. EL 2019, P. II. Vorabentscheidungsverfahren Rn. 60; *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 475 ff.

642 EuGH, Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 42; Urt. v. 26.2.2015 – Rs. C-143/13 (*Matei*) – Rn. 49.

tauschverhältnissen, im deutschen Schuldrecht tendenziell weit zu verstehen sein, um dem Schuldner, der ökonomisch betrachtet eine Gegenleistung erbringt, auch die Vorteile eines rechtlich entgeltlichen Vertrags (wie etwa die Vermeidung von Haftungsprivilegierungen des Gläubigers) zu sichern.[643]

Die deutsche Rechtsprechung hat die Vorgaben des EuGH hinsichtlich der preislichen Gegenleistung bekanntlich durch die Unterscheidung zwischen Preishaupt- und Preisnebenabreden verfeinert.[644] Danach sind Preishauptabreden der Inhaltskontrolle entzogen, nicht jedoch Preisnebenabreden. Preishauptabreden legen Art oder Umfang des Preises für eine rechtsgeschäftlich erbrachte Leistung unmittelbar fest;[645] Preisnebenabreden umfassen dagegen „alle auf Preise bezogene Abreden, die zwar mittelbare Auswirkungen auf Preis und Leistung haben, an deren Stelle aber, wenn eine wirksame vertragliche Regelung fehlt, dispositives Gesetzesrecht"[646] oder eine ergänzende Regelung nach §§ 157, 242 BGB treten kann.[647] Sie betreffen mithin z. B. die Modalitäten der Zahlung oder eine Modifizierung des ursprünglich vereinbarten Preises.[648] Dieser Unterscheidung ist jedenfalls grundsätzlich zuzustimmen: Bestimmte Preisnebenabreden müssen kontrollfähig sein, da sonst § 309 Nr. 1 BGB keinen Sinn ergäbe.[649] Ihre eigentliche Rechtfertigung erlangt die Kontrollfähigkeit nur mittelbar preiswirksamer Abreden jedoch dadurch, dass diese typischerweise, ebenso wie sonstige Vertragsnebenbedingungen, rational übergangen werden.[650]

Mit Blick auf datenschutzrechtlich relevante AGB hat der BGH jedoch in den Rechtssachen *Payback* und *HappyDigits* eine Sonderrechtsprechung entwickelt. Danach prüft der BGH im Rahmen von § 307 Abs. 3 S. 1 BGB, ob die datenschutzrechtlichen Vorschriften eingehalten wurden.[651] Ist dies nicht der Fall, so steht damit für den BGH zugleich fest, dass von einer gesetzlichen Regelung abgewichen wurde, die Klausel mithin kontrollfähig ist. Dies impliziert weiter, auf Grundlage der Prämisse, dass das Datenschutzrecht den alleinigen Prüfungsmaßstab abgibt, die Unangemessenheit der Klausel.[652] Wurden die datenschutzrechtlichen Vorschriften jedoch eingehalten, so muss nach dem

---

[643] Siehe im Einzelnen *Hacker*, ZfPW 2019, 148 (158 ff.); aA numehr KG BeckRS 2019, 8570 Rn. 42–45; dagegen bereits oben, § 5 B.II.

[644] Siehe nur BGH NJW 1989, 222 (223); BGH NJW 1998, 383; BGH NJW 2011, 2640 Rn. 19; *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 17.

[645] BGH NJW 1989, 222 (223); BGH NJW 1992, 688 (689); BGH NJW 2011, 2640 Rn. 19; *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 17. Der Preis für „allgemeine Betriebskosten, Aufwand zur Erfüllung eigener Pflichten oder für Tätigkeiten, die im eigenen Interesse liegen" ist daher kontrollfähig, BGH NJW 2011, 2640 Rn. 19.

[646] BGH NJW 1992, 688 (689); zuvor bereits BGH NJW 1989, 222 (223).

[647] BGH NJW 1985, 3013.

[648] BGH NJW 1985, 3013 (3014); *Fuchs* in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016, § 307 BGB Rn. 76.

[649] *Thomas*, AcP 209 (2009), 84 (91).

[650] *Köndgen*, NJW 1989, 943 (948).

[651] BGH NJW 2008, 3055 Rn. 15, 19; BGH NJW 2010, 864 Rn. 16.

[652] Vgl. BGH NJW 2008, 3055 Rn. 26; LG Berlin MMR 2018, 328 Rn. 65–67.

BGH bereits mangels Kontrollfähigkeit eine AGB-rechtliche Unwirksamkeit verneint werden.[653]

Dieser Rechtsprechung kann jedoch in mehrfacher Hinsicht unter Geltung der DS-GVO nicht gefolgt werden. Dass das Datenschutzrecht nicht den alleinigen Prüfungsmaßstab für datenschutzrechtlich relevante Klauseln abgeben kann, wurde bereits ausgeführt.[654] Es ist jedoch weiterhin keineswegs ausgemacht, wie gleich noch im Einzelnen zu zeigen ist, dass bei Einhaltung datenschutzrechtlicher Vorschriften die Kontrollfähigkeit entfällt. Denn auch in diesem Fall kann eine gesetzliche Regelung ergänzt werden. Vor allem jedoch hilft der Blick auf das Datenschutzrecht lediglich für die Einwilligung, nicht jedoch für Vertragsklauseln, da die DS-GVO für deren Wirksamkeit gar keine Regelungen enthält. Für diese Klauseln muss es daher, sofern sie in schuldrechtlicher Hinsicht zu den Hauptleistungspflichten zählen, zunächst bei der tradierten Abgrenzung von Hauptabreden und Nebenabreden bleiben. Es wird sich jedoch zeigen, dass auch hinsichtlich der Hauptabreden dort, wo die Überlassung von Daten in Rede steht, von einer Kontrollfähigkeit ausgegangen werden kann.

Letztlich sind daher verschiedene Konstellationen in digitalen Austauschprozessen zu unterscheiden. Zunächst stellt sich die Frage nach der Kontrollfähigkeit der Einwilligung selbst, wenn die Pflicht zur Einwilligung eine vertragliche Hauptleistung darstellt. Sodann muss die Kontrollfähigkeit der (von der Einwilligung streng zu trennenden) Vertragsklauseln untersucht werden.

(2) Zur Kontrollfähigkeit der Einwilligung

Die Abgabe einer datenschutzrechtlichen Einwilligung kann, wie bereits mehrfach bemerkt, in Erfüllung einer vertraglichen Pflicht oder Bedingung hinsichtlich der Abgabe erfolgen, die wiederum Gegenleistung für eine Leistung des Anbieters ist. Damit wird die Einwilligung selbst jedoch nicht zum Hauptgegenstand des Vertrags im Sinne von Art. 4 Abs. 2 der Klauselrichtlinie. Denn der Hauptgegenstand wird nach der Rechtsprechung des EuGH durch jene *Vertragsklauseln* gebildet, welche die Hauptleistungspflichten festlegen.[655] Diese müssen jedoch, wie bereits erörtert,[656] von der Einwilligung selbst streng getrennt werden. Die richtlinienkonforme Auslegung von § 307 Abs. 3 S. 1 BGB streitet daher bereits eindeutig für die Kontrollfähigkeit von Einwilligungserklärungen schlechthin.[657]

Diese Auslegung ist allerdings auch mit dem Wortlaut von § 307 Abs. 3 S. 1 BGB, in der Interpretation der Rechtsprechung des BGH, durchaus vereinbar.

---

653 BGH NJW 2008, 3055 Rn. 19, 41; BGH NJW 2010, 864 Rn. 16.

654 Siehe oben, § 5 C.II.1.a).

655 EuGH, Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 49 f.; Urt. v. 26.2.2015 – Rs. C-143/13 (*Matei*) – Rn. 54.

656 Siehe oben, § 4 B.I.2.

657 So im Ergebnis auch *Langhanke*, Daten als Leistung, 2018, 223.

Bereits früh hat der BGH zu der identischen Vorgängerregelung im AGBG entschieden: „Auch eine AGB-Klausel, die nur einen vom Gesetz ausdrücklich eröffneten Gestaltungsspielraum nutzt, ‚ergänzt' die gesetzliche Regelung im Sinne von [nunmehr § 307 Abs. 3 S. 1 BGB]."[658] Genau dies ist bei der Einwilligung der Fall: Die DS-GVO eröffnet mit Art. 6 Abs. 1 lit. a DS-GVO einen Gestaltungsspielraum dahingehend, dass durch die Einwilligung die Erlaubnis zur Datenverarbeitung herbeigeführt werden kann. Dadurch wird unmittelbar die Rechtslage umgestaltet, da infolge der Einwilligung die Datenverarbeitung (sofern kein anderer Erlaubnistatbestand einschlägig ist) nicht mehr verboten, sondern nunmehr erlaubt ist. Daher wurde bereits unter dem Regime des BDSG vertreten, dass die Einwilligung infolge ihrer rechtsgestaltenden Wirkung immer kontrollfähig sein müsse.[659] Dieses Argument wird unter der DS-GVO, in Verbindung mit der richtlinienkonformen Auslegung, nachgerade zwingend.[660] Die in *Payback* und *HappyDigits* begründete Sonderrechtsprechung des BGH kann auch insoweit nicht aufrechterhalten werden. Daher sind Einwilligungserklärungen, unabhängig davon, ob sie in Erfüllung einer Hauptleistungspflicht abgegeben werden oder nicht, stets kontrollfähig.

(3) Zur Kontrollfähigkeit von Vertragsklauseln

Von der Kontrollfähigkeit der Einwilligung ist die Frage der Kontrollfähigkeit von Vertragsklauseln, auch wenn diese auf Abgabe einer Einwilligung gerichtet sind, streng zu trennen. Hier müssen drei unterschiedliche Ansatzpunkte für eine Klauselkontrolle unterschieden werden: erstens die Kontrolle einer datenbasierten Gegenleistungspflicht (die Höhe des „Datenpreises"); zweitens die Kontrolle der Angemessenheit des Verhältnisses von Datenpreis und Leistung des Anbieters; und drittens die Kontrolle von Leistungspflichten des Anbieters.

(a) Kontrollfähigkeit der Verpflichtung zur Datenüberlassung oder Einwilligung

Wie schon mehrfach betont, kann im Rahmen des Geschäftsmodells, in dem Daten als Gegenleistung Verwendung finden, eine Gegenleistung sowohl in einer Verpflichtung zur Überlassung von Daten oder auch zur Abgabe einer Einwilligung (bzw. in einer dahingehenden Bedingung) gesehen werden.[661] Schon auf Grundlage der bisherigen Rechtsprechung des BGH kann darin je-

[658] BGH NJW 1989, 222 (223); siehe auch *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 306.

[659] *Nord/Manz*el, NJW 2010, 3756 (3756 f.); *Hanloser*, MMR 2010, 140 (141); *Langhanke*, Daten als Leistung, 2018, 209; siehe auch *Stoffels*, JZ 2001, 843 (847); im Ergebnis auch implizit *Helberger/Zuiderveen Borgesius/Reyna*, 54 Common Market Law Review 2017, 1427 (1451).

[660] So im Ergebnis auch bereits *Hacker*, ZfPW 2019, 148 (186).

[661] Siehe § 5 B.I.

doch nicht zugleich in jedem Fall eine Preishauptabrede erblickt werden. Vielmehr muss zwischen den einzelnen Geschäftsmodellen differenziert werden.[662]

(aa) Monetäres Grundmodell: Preisnebenabreden

Beim data on top-Modell wie auch beim Rabattmodell liegt in der Klausel, die eine Überlassung von Daten oder die Abgabe einer Einwilligung zum Inhalt hat, lediglich eine Preisnebenabrede.[663] Denn bei diesem monetären Geschäftsmodell steht die Zahlung einer Gegenleistung in Geld im Vordergrund. Sie wird durch die datenbasierte Leistung des Nutzers, sofern darin überhaupt eine Gegenleistung im schuldrechtlichen Sinne erblickt werden kann,[664] lediglich modifiziert: implizit beim data on top-Modell, bei dem die datenbasierte Zahlung zu der monetären hinzutritt; explizit beim Rabattmodell, bei dem auf den ursprünglichen Preis ein Nachlass gewährt wird. Preisanpassungsklauseln sind jedoch nach der Rechtsprechung sowohl des EuGH[665] als auch des BGH[666] grundsätzlich kontrollfähig. Die dieser Wertung zugrunde liegende Prämisse, dass die Verbraucher Anpassungsklauseln nicht mit derselben Aufmerksamkeit belegen und aufgrund ihrer Komplexität nur eingeschränkt nachvollziehen,[667] lässt sich jedoch nicht nur für das monetäre, sondern auch das datenbasierte Grundmodell fruchtbar machen.

(bb) Datenbasiertes Grundmodell:
Preishauptabreden und teleologische Reduktion

Dogmatisch sind die entsprechenden Klauseln im Rahmen datenbasierter Geschäftsmodelle wie dem vollkommen datenfinanzierten Modell oder dem Freemium-Modell jedoch zunächst anders zu bewerten. Hier steht die datenbasierte Leistung des Nutzers ganz im Vordergrund; es fließt kein oder jedenfalls kein signifikantes monetäres Entgelt. Ökonomisch-funktional, aber auch rechtlich gesehen handelt es sich daher um eine echte Gegenleistung,[668] von der man wird sagen müssen, dass sie den Hauptgegenstand der Leistungspflicht des Nutzers ausmacht. Daher wird in der Literatur in der Tat bisweilen vertreten, die den „Datenpreis" bestimmenden Klauseln seien nicht kon-

662 Zu diesen oben, § 3 A.II.2.

663 Siehe bereits *Hacker*, ZfPW 2019, 148 (187).

664 Dazu *Rudkowski*, ZVersWiss 2017, 453 (486); *Specht*, JZ 2017, 763/764); *Hacker*, ZfPW 2019, 148 (163 f.).

665 EuGH, Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 56; Urt. v. 21.3.2013 – Rs. C-92/11 (*RWE*) – Rn. 47; Urt. v. 26.4.2012 – C-472/10 (*Invitel*) – Rn. 23; siehe auch *Rott*, in: Twigg-Flesner (Hrsg.), Research Handbook on EU Consumer and Contract Law, 287 (294).

666 BGH NJW 2003, 507 (508); BGH NJW 2009, 2662 Rn. 18; *Thomas*, AcP 209 (2009), 84 (90 ff.).

667 *Brömmelmeyer* r + s 2017, 225 (231); *Hacker*, ZfPW 2019, 148 (187).

668 Siehe oben, Text bei § 4, Fn. 671 ff.

trollfähig.[669] Demgegenüber wird man zunächst präzisieren müssen, dass auch hier reine Modalitäten der Überlassung von Daten und der Abgabe der Einwilligung als Nebenabreden kontrollfähig bleiben.[670] Echte Preishauptabreden sind nur insoweit zu gewärtigen, als es um die Existenz und den Umfang der Pflicht zur Überlassung von Daten oder der Abgabe einer Einwilligung geht. Auch hier muss man jedoch bei einer teleologischen und richtlinienkonformen Auslegung, die insbesondere die ökonomischen Grundlagen der AGB-Kontrolle berücksichtigt, eine Kontrollfähigkeit annehmen.[671]

α. Gründe für fehlende Kontrollfähigkeit
nach Art. 4 Abs. 2 der Klauselrichtlinie

Der EuGH führt als primären Grund für die Ausnahme des Preis-/Leistungsverhältnisses von der Klauselkontrolle an, dass für die Beurteilung der Angemessenheit insoweit keine rechtlichen Maßstäbe verfügbar seien.[672] Ähnliches ließe sich auch für die isolierte Prüfung der Gegenleistungspflicht behaupten, da juristische Kriterien hinsichtlich der Höhe eines monetären Preises grundsätzlich nicht zur Verfügung stehen.[673] Dies betrifft, um eine Präzisierung *Fastrichs* aufzugreifen, die Kontrollfähigkeit im eigentlichen Sinne.[674] Wie sich jedoch gleich zeigen wird, lassen sich aus der Rechtsprechung des EuGH selbst durchaus derartige Maßstäbe ableiten, zumal für datenbasierte Gegenleistungen, die allerdings zurückhaltend angewandt werden müssen.[675]

Bei ökonomischer Betrachtung hingegen stechen zwei Gründe für die Ausnahmebestimmung des Art. 4 Abs. 2 der Klauselrichtlinie hervor. In Abgrenzung zur Kontrollfähigkeit im eigentlichen Sinne ist mit diesen die mangelnde Kontrollbedürftigkeit angesprochen, die sich aus dem grundsätzlich effektiven Funktionieren des Marktmechanismus bezüglich der nach Art. 4 Abs. 2 der Klauselrichtlinie ausgenommenen Bestimmungen ergibt.[676] Erstens kann in der Regel davon ausgegangen werden, dass der Hauptgegenstand des Ver-

---

[669] *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (697) („*de facto* price"); *Sattler*, JZ 2018, 769 (770), allerdings jeweils ohne Differenzierung zwischen den einzelnen Geschäftsmodellen.

[670] *Metzger*, AcP 216 (2016), 817 (841).

[671] Im Ergebnis ebenso *Graf von Westphalen/Wendehorst*, BB 2016, 2179 (2186); *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3749).

[672] EuGH, Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 55; Urt. v. 26.2.2015 – Rs. C-143/13 (*Matei*) – Rn. 55; siehe auch *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 325; *Looschelders/Olzen*, in: Staudinger, BGB, 2015, § 242 Rn. 473; *Billing*, Die Bedeutung von § 307 III 1 BGB im System der AGB-rechtlichen Inhaltskontrolle, 2006, 151.

[673] Zur Debatte um den *iustum praetium* und die *laesio enormis* noch unten, § 5 C.II.2.

[674] *Fastrich*, Richterliche Inhaltskontrolle im Privatrecht, 1992, 252 ff.; dem folgend *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 320 ff.

[675] Das Argument fehlender Kontrollmaßstäbe ablehnend auch *Fornasier*, Freier Markt und zwingendes Vertragsrecht, 2013, 198, mit zutreffendem Verweis auf §§ 138, 313, 315 BGB.

[676] *Fastrich*, Richterliche Inhaltskontrolle im Privatrecht, 1992, 263 ff.; dem in der Sache

trags, im Gegensatz zu in AGB befindlichen Nebenabreden, durch die Vertragsparteien und insbesondere auch den Verbraucher mit hinreichender Aufmerksamkeit belegt wird.[677] Auf den Preis achtet der Käufer, genauso wie darauf, welchen Gegenstand erwirbt. Der BGH geht insoweit davon aus, dass „der Vertragspartner des Verwenders der – einer materiellen Inhaltskontrolle entzogenen – Preisvereinbarung besondere Aufmerksamkeit widmet und insoweit seine Verhandlungsmöglichkeiten und Marktchancen interessengerecht wahrnimmt."[678] Das Postulat rationaler Ignoranz, das die Klauselkontrolle sonst rechtfertigt,[679] greift daher nicht; wer jedoch weiß, worauf er sich einlässt, muss durch die Inhaltskontrolle nicht geschützt werden.

Damit hängt eng das zweite Argument zusammen. Denn wo ein Marktparameter mit Aufmerksamkeit belegt wird, kann der Wettbewerb seine disziplinierende Wirkung entfalten. Das Marktversagen hinsichtlich eines Konditionenwettbewerbs, das die ökonomische Rechtfertigung für die Klauselkontrolle abgibt,[680] betrifft daher grundsätzlich nur Nebenabreden, nicht hingegen den Hauptgegenstand des Vertrags.[681] Dies gilt in besonderer Hinsicht auch für das Preis-/Leistungsverhältnis.[682] Auch dieses findet sich grundsätzlich am effektivsten und effizientesten am Markt.[683] Verantwortlich dafür ist, wie besonders Hayek nicht müde wurde zu betonen, das Preissignal, das die Kräfte von Angebot und Nachfrage dezentral effizienter steuert als jede externe Instanz es vermöchte, inklusive der Gerichte.[684] Die dezentrale Wirkung des Preismechanismus ist daher jedenfalls grundsätzlich einer zentralen Steuerung überlegen.

β. Marktversagen bei der Kontrolle des „Datenpreises"

Auf Klauseln, die durch die Überlassung von Daten oder die Abgabe einer Einwilligung einen „Datenpreis"[685] festlegen, lassen sich diese Erwägungen jedoch

folgend *Fornasier*, Freier Markt und zwingendes Vertragsrecht, 2013, 198 f.; ähnlich *Becker*, Der unfaire Vertrag, 2003, 48.

[677] *Fastrich*, Richterliche Inhaltskontrolle im Privatrecht, 1992, 264; *Fornasier*, Freier Markt und zwingendes Vertragsrecht, 2013, 155, 157, 199; *Wackerbarth*, AcP 200 (2000), 45 (78); *Stoffels*, JZ 2001, 843 (847); *Köndgen*, NJW 1989, 943 (948); *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 13, 56; *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 321; *Rott*, in: Twigg-Flesner (Hrsg.), Research Handbook on EU Consumer and Contract Law, 287 (293).

[678] BGH NJW-RR 2008, 251 (253).

[679] Siehe oben, § 5, Fn. 586.

[680] Siehe oben, § 5, Fn. 586.

[681] Vgl. *Fuchs* in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016, § 307 BGB Rn. 14; *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 320 f.

[682] *Köndgen*, NJW 1989, 943 (948); *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 324.

[683] *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 1; *Canaris*, NJW 1987, 609 (613).

[684] *Hayek*, 35 American Economic Review 1945, 519 (525–527); *Stigler*, The Theory of Price, 4. Aufl. 1987, 11–16; *Stigler*, 69 Journal of Political Economy 1961, 213 (214 ff.); *Varian*, Intermediate Micro-Economics, 8. Aufl., 2010, 3, 78; siehe auch *Fornasier*, Freier Markt und zwingendes Vertragsrecht, 2013, 31.

[685] Zum Begriff bereits oben, Text bei § 3, Fn. 122.

gerade nicht übertragen. Selbst bei rationalen Akteuren gehen die Annahmen, die aus ökonomischer Perspektive für die Ausnahme von der Kontrollfähigkeit verantwortlich sind, fehl.[686]

Wie bereits im Einzelnen dargelegt wurde, strafen die Nutzer Vertragsbestimmungen, mit denen eine Datenüberlassung oder eine Einwilligung gefordert wird, mit rationaler Ignoranz.[687] Daher stellt sich die Situation im Rahmen digitaler Austauschprozesse, bei denen Daten eine Gegenleistung übernehmen, wie bei (Preis-)Nebenbedingungen in traditionellen Verträgen dar.[688] Dort ist jedoch rationale Ignoranz gerade der Grund für die Inhaltskontrolle.[689]

Aber auch die zweite Voraussetzung, die effektive Steuerung von Angebot und Nachfrage durch einen klaren Datenpreis, trifft auf datenbasierte Austauschprozesse nur äußerst eingeschränkt zu. Nutzer haben ohnehin aufgrund vielfältiger verhaltensökonomischer Effekte erhebliche Schwierigkeiten, den Wert ihrer Daten rational einzuschätzen.[690] Dasselbe Problem besteht jedoch auch für stark rationale Parteien. Denn immer dann, wenn der Preis in einer Datenüberlassung oder einer Einwilligung besteht, ist das Preissignal intrinsisch hochgradig unbestimmt und kann gerade nicht auf eine kardinale Indexzahl reduziert werden.[691] Zwar existieren verschiedene ökonometrische Methoden, um den Wert personenbezogener Daten zu bestimmen.[692] Dabei handelt es sich jedoch lediglich um grobe Abschätzungen, die den einzelnen Nutzern darüber hinaus im Rahmen ihrer Entscheidungsfindung nicht zur Verfügung stehen.[693] Wie Hayek im Einzelnen dargelegt hat, muss das Preissignal aber klar erkennbar sein, gerade auch hinsichtlich kleiner Abweichungen, damit sich das dezentrale „marvel of the market" entfalten kann.[694] Diese Prämisse ist bei den komplexen, über verschiedene Dokumente verstreuten Bedingungen der Datenverarbeitung typischerweise nicht erfüllt. Dies führt dazu, dass Nachfrager von Diensten und Waren, die mit ihren Daten bezahlen, gerade nicht in effizienter Weise den „preiswertesten" Anbieter auswählen können. Angebotsstrategien, die sich über den Datenpreis differenzieren, sind daher schon aus diesem Grund nur in sehr verminderter Form zu erwarten.

---

686 *Hacker*, ZfPW 2019, 148 (188).

687 Siehe oben, § 3 B.II.1.a).

688 Zur Ignoranz von Preisnebenabreden und der daraus folgenden Kontrollfähigkeit *Köndgen*, NJW 1989, 943 (948).

689 Siehe oben, § 5, Fn. 586.

690 Siehe oben, § 3 B.II.1.b).

691 Siehe oben, § 3 B.II.1.d).

692 Überblick bei *OECD*, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, 2013; *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen).

693 *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen).

694 *Hayek*, 35 American Economic Review 1945, 519 (525–527).

Dies hat unmittelbare Auswirkungen auf die Auslegung von Art. 4 Abs. 2 der Klauselrichtlinie und damit auf die richtlinienkonforme Auslegung von § 307 Abs. 3 S. 1 BGB. Nach der Rechtsprechung des EuGH ist, über den Wortlaut einer Vorschrift hinaus, ihr Sinn und ihr Kontext bei der Auslegung maßgeblich zu berücksichtigen.[695] Es besteht jedoch bei datenbasierten Preisstrategien eine hinreichende Wahrscheinlichkeit genau jenes Marktversagens, das die AGB-Kontrolle beheben soll:[696] geschwächter Wettbewerb wegen Unaufmerksamkeit hinsichtlich des Klauselinhalts und wegen unbestimmten Preissignals. Daher muss Art. 4 Abs. 2 der Klauselrichtlinie, und in der Folge auch § 307 Abs. 3 S. 1 BGB,[697] in diesen Fällen teleologisch reduziert werden.[698] In der Konsequenz kann Klauseln, die auf die Überlassung von Daten und die Abgabe einer Einwilligung gerichtet sind, die Kontrollfähigkeit nicht abgesprochen werden.[699]

(b) Kontrollfähigkeit des Preis-/Leistungsverhältnisses

Ganz parallel lässt sich in ökonomischer Hinsicht, wie bereits angedeutet, hinsichtlich des Preis-/Leistungsverhältnisses argumentieren. Wegen der mangelnden Klarheit des Preissignals droht auch hier ein Marktversagen bezüglich der effizienten Ausbalancierung des Verhältnisses von Leistung und Gegenleistung, sodass der Sinn und Zweck der Ausnahme von der Inhaltskontrolle nicht erfüllt ist. Anders als bei der isolierten Betrachtung der Gegenleistungspflicht existiert jedoch für das Preis-/Leistungsverhältnis nach deutschem Verständnis bereits ein rechtlicher Kontrollmechanismus mit der Fallgruppe des wucherähnlichen Geschäfts im Rahmen von § 138 Abs. 1 BGB.[700] Dort hat die Rechtsprechung bereits Kriterien für den Abgleich von Leistung und Gegenleistung entwickelt und ist die Frage nach der Angemessenheit des Verhältnisses von Preis und Leistung systematisch besser verortet.[701] Daher ist eine teleologische Reduktion von § 307 Abs. 3 S. 1 BGB insoweit nicht notwendig.

---

[695] EuGH, Urt. v. 1.4.2008 – verb. Rs. C-14/06 und C-295/06 (*Parlament/Kommission*) – Rn. 67.

[696] Siehe *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, Vor § 305 Rn. 4–6; *Stoffels*, JZ 2001, 843 (847).

[697] Zur teleologischen Reduktion aus Gründen der Herstellung von Gemeinschaftsrechtskonformität allgemein *Herresthal*, Rechtsfortbildung im europarechtlichen Bezugsrahmen, 2006, 241 ff.

[698] Siehe bereits *Hacker*, ZfPW 2019, 149 (188); *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen); so wohl auch *Schweitzer*, in: Körber/Kühling (Hrsg.), Regulierung-Wettbewerb-Innovation, 2017, 269 (277).

[699] Im Ergebnis ebenso *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3748); *Loos/Luzak*, 39 Journal of Consumer Policy 2016, 63 (67); wohl auch *Helberger/Zuiderveen Borgesius/Reyna*, 54 Common Market Law Review 2017, 1427 (1450 f.).

[700] Dazu sogleich, unter § 5 C.II.2.; für eine Kontrolle lediglich am Maßstab von § 242 BGB allerdings, wenngleich nicht mit Blick auf digitale Angebote, *Becker*, Der unfaire Vertrag, 2003, 48 f.

[701] *Hacker*, ZfPW 2019, 149 (188).

Man könnte allenfalls annehmen, dass eine Prüfung auch der Angemessenheit des Verhältnisses von Preis und Leistung im Rahmen der §§ 305 ff. BGB in richtlinienkonformer Auslegung der AGB-Kontrolle insofern zwingend sei, als eine teleologische Reduktion von Art. 4 Abs. 2 der Klauselrichtlinie zur Folge hat, dass das Preis-/Leistungsverhältnis im Rahmen datenbasierter Austauschprozesse Teil des harmonisierten Bereichs der Klauselrichtlinie ist. Allerdings ist richtigerweise anzunehmen, dass insoweit eine richtlinienkonforme Auslegung von § 138 Abs. 1 BGB ausreichend ist.[702]

(c) Kontrollfähigkeit von Leistungsbeschreibungen

Klauseln, welche die Hauptleistung des Anbieters beschreiben, sind als sogenannte Leistungsbeschreibungen grundsätzlich ebenfalls nicht kontrollfähig.[703] Wie jedoch das vierte Kapitel dieser Arbeit gezeigt hat, könnten weite Leistungspflichten als Vehikel genutzt werden, um eine Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO zu legitimieren.[704] Ein Beispiel wäre die Verpflichtung seitens eines Anbieters eines sozialen Netzwerks, personalisierte Werbung zu erbringen. Bei unterstellter Wirksamkeit dieser Verpflichtung wäre die dafür erforderliche Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO zulässig.

Die Vereinbarung solcher Leistungspflichten sollte jedoch in Abweichung vom allgemeinen Grundsatz ebenfalls kontrollfähig sein, wenn die Überlassung von personenbezogenen Daten oder die Abgabe einer Einwilligung die Gegenleistung des Vertrags darstellt.[705] Dies folgt auf Grundlage der bisherigen Rechtsprechung zumeist bereits daraus, dass es sich bei den entsprechenden Leistungspflichten des Anbieters regelmäßig lediglich um Nebenabreden handelt, die gerade nicht den Hauptgegenstand des Vertrags betreffen.[706] So verhält es sich etwa, wenn die Hauptleistungspflicht des Anbieters in der Gewährung des Zugangs zu einem sozialen Netzwerk liegt; die Pflicht, persona-

---

[702] Siehe dazu unten, Text bei § 5, Fn. 879.

[703] BGH NJW 1985, 3013 (3014).

[704] So auch *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3747); ähnlich *Graf von Westphalen/Wendehorst*, BB 2016, 2179 (2185); aA *Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder*, Bericht vom 15. Mai 2017, 2017, 217–219, die derartige Klauseln offenbar nach §§ 133, 157 BGB so auslegen will, dass eine Leistung des Anbieters nicht geschuldet ist. Dem ist jedoch entgegenzuhalten, dass eine solche Auslegung bei ausdrücklicher Formulierung der Pflicht des Anbieters jeder Grundlage entbehrt. Allein der Umstand, dass diese Pflicht für eine Partei – die betroffene Person – (bei hohen Datenschutzpräferenzen) auch negative Folgen hat, kann nicht dazu führen, die Existenz der Pflicht in Abrede zu stellen (so aber ebd., 218 f.). Andernfalls wäre für Verbraucher unangemessenen Klauseln immer im Wege der Auslegung beizukommen, was die Klauselkontrolle entbehrlich machen würde.

[705] Ebenso *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3749); siehe auch bereits *Hacker*, ZfPW 2019, 149 (188 f.).

[706] So auch *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3749); vgl. auch BGH NJW 1995, 2637 (2638).

lisierte Werbung zu schalten, ist demgegenüber als Nebenabrede zu qualifizieren, die – um das Kriterium des EuGH zu bemühen[707] – den Charakter des Vertrags nicht prägt.[708]

Aber auch dann, wenn man in einem Einzelfall von einer Zugehörigkeit zum Hauptgegenstand des Vertrags ausgehen wollte, dürfte aus zwei Gründen wiederum in teleologischer Reduktion von Art. 4 Abs. 2 der Klauselrichtlinie und § 307 Abs. 3 S. 1 BGB eine derartige Vereinbarung kontrollfähig sein. Denn erstens ist das Zusammenspiel mit Art. 6 Abs. 1 lit. b. DS-GVO typischerweise gerade der Aufmerksamkeit auch sophistizierter Kunden entzogen.[709] Dass darauf nach Art. 13 Abs. 1 lit. c DS-GVO hingewiesen werden muss, ist angesichts überwältigender rationaler Ignoranz der Pflichtinformationen unerheblich. Wiederum kann daher in Bezug auf die Datenverarbeitung kein wirksamer Konditionenwettbewerb entstehen. Daher liegt auch insofern ein Marktversagen nahe, welches die AGB-Kontrolle rechtfertigt. Zweitens kann ganz parallel wie bei der Einwilligung argumentiert werden, dass eine derartige Klausel insoweit, als sie nach Art. 6 Abs. 1 lit. b DS-GVO die Datenverarbeitung ermöglicht, ebenfalls die Rechtslage umgestaltet und daher, in Übereinstimmung mit der Auslegung des Begriffs der Ergänzung durch den BGH,[710] die bestehende Rechtslage durch Inanspruchnahme eines rechtlichen Gestaltungsspielraums ergänzt.

(4) Ergebnis

Als Ergebnis lässt sich damit Folgendes festhalten: Die Einwilligung ist als rechtsgestaltende Erklärung in jedem Fall vollumfänglich kontrollfähig. Klauseln, die durch eine Pflicht oder Bedingung hinsichtlich der Überlassung von Daten oder auch der Abgabe einer Einwilligung den Datenpreis bestimmen, müssen, sofern sie nicht ohnehin Nebenabreden darstellen, in teleologischer Reduktion von Art. 4 Abs. 2 der Klauselrichtlinie und § 307 Abs. 3 S. 1 BGB ebenfalls kontrollfähig gestellt werden. Dasselbe gilt für Leistungsbeschreibungen insoweit, als sie Grundlage für eine Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO sind. Denn die beiden Hauptargumente für eine Ausnahme von Kontrollfähigkeit (hinreichende Aufmerksamkeit der Verbraucher; effizientes Funktionieren des marktbasierten Preismechanismus) treffen in diesen Fällen schlichtweg nicht zu. Lediglich das Verhältnis von Preis und Leistung muss systematisch vorrangig bei § 138 Abs. 1 BGB, nicht im Rahmen der AGB-Kon-

[707] EuGH, Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 49 f.; Urt. v. 26.2.2015 – Rs. C-143/13 (*Matei*) – Rn. 54.

[708] Vgl. KG ZD 2014, 412 (417): Lizenzerteilung durch Nutzer als Nebenabrede bei Vertrag über Zugang zu sozialem Netzwerk.

[709] Vgl. *Obar/Oehldorf-Hilsch*, 21 Information, Communication & Society 2018, 1; *Bakos/Marotta-Wurgler/Trossen*, 43 The Journal of Legal Studies 2014, 1; *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S41.

[710] Siehe oben, § 5, Fn. 658.

trolle, überprüft werden. Insgesamt müssen jedoch, um eine freie und letztlich unzulässige Billigkeitskontrolle im Leistungsbereich zu vermeiden,[711] Maßstäbe gefunden werden, anhand derer die genannten Klauseln überprüft werden können.

bb) Grundsätze der unangemessenen Benachteiligung

Die besondere Herausforderung der AGB-Kontrolle von datenschutzrechtlich relevanten Klauseln besteht darin, Maßstäbe für die unangemessene Benachteiligung zu entwickeln, besonders wenn es sich um in Deutschland üblicherweise von der Kontrolle ausgenommene Hauptleistungspflichten handelt. Jenseits der bei der Nutzung von Diensten gegen Daten bisweilen einschlägigen §§ 308 f. BGB[712] kann dabei, wie auch sonst im Rahmen der AGB-Kontrolle, zunächst auf den konkretisierenden § 307 Abs. 2 BGB zurückgegriffen werden, bevor die Kontrolle nach § 307 Abs. 1 S. 1 BGB in den Blick kommt.

(1) § 307 Abs. 2 Nr. 1 BGB

Einen ersten Maßstab liefert § 307 Abs. 2 Nr. 1 BGB, wonach eine unangemessene Benachteiligung im Zweifel angenommen werden kann, wenn eine Bestimmung mit wesentlichen Grundgedanken der gesetzlichen Regelung, von der abgewichen wird, nicht zu vereinbaren ist. Wie auch schon in der Rechtsprechung zum BDSG aF wird man hier auf die Abweichung vom Datenschutzrecht zurückgreifen können.

(a) Datenschutzrecht allgemein als Maßstab

Der BGH und die Instanzrechtsprechung haben bisher in einem Verstoß gegen datenschutzrechtliche Regelungen zugleich eine Abweichung von wesentlichen Grundgedanken des Datenschutzrechts nach § 307 Abs. 2 Nr. 1 BGB erblickt. Wegen der besonderen Relevanz des Schutzes der Privatsphäre wurde etwa in der *Payback*-Entscheidung des BGH bei einem Verstoß gegen die Umsetzung von Art. 13 ePrivacy-Richtlinie in § 7 Abs. 2 UWG zugleich eine AGB-rechtliche Unangemessenheit angenommen.[713] In gleicher Weise wurden Verstöße gegen das BDSG aF[714] oder datenschutzrechtliche Vorschriften des

[711] Deutlich insofern *Billing*, Die Bedeutung von § 307 III 1 BGB im System der AGB-rechtlichen Inhaltskontrolle, 2006, 153; *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 328.

[712] Siehe etwa LG Berlin, MMR 2018, 328 Rn. 58–60 und KG MMR 2020, 239 Rn. 47 zu einer Bestätigung, bei der Registrierung die Datenrichtlinie gelesen zu haben sowie Rn. 74 zur Bestätigung eines Alters von über 13 Jahren (jeweils § 309 Nr. 12b BGB); LG Berlin MMR 2014, 563 (564 f.) zur Haftungsbeschränkung entgegen § 309 Nr. 7a BGB sowie zur einseitigen Änderung der Dienste und der Nutzungsbedingungen entgegen § 308 Nr. 4 BGB; siehe auch *Langhanke*, Daten als Leistung, 2018, 210; *Zscherpe*, MMR 2004, 723 (725); *Graf von Westphalen*, VuR 2017, 323 (327).

[713] BGH NJW 2008, 3055 Rn. 3 – Payback.

[714] KG ZD 2018, 118 Rn. 86 (unter – methodisch fragwürdigem – direktem Rekurs auf

TMG[715] in Verbindung mit § 307 Abs. 2 Nr. 1 BGB als unangemessene Benachteiligung qualifiziert.

Der Grundsatz, wonach ein Verstoß gegen datenschutzrechtliche Vorschriften zugleich über die Scharniernorm des § 307 Abs. 2 Nr. 1 BGB als unangemessene Benachteiligung zu werten ist,[716] gilt auch bei Verletzung der DS-GVO.[717] In diesem Sinne hat auch bereits das KG geurteilt.[718] Grund für diese Wertung dürfte sein, dass jeder Verstoß gegen das sekundärrechtliche Datenschutzrecht zugleich eine Verkürzung des Schutzes des primärrechtlichen Datenschutzgrundrechts darstellt.[719] Hier wirkt sich die besondere, grundrechtsgeprägte Marktordnung im Bereich des Datenschutzprivatrechts aus. Allerdings ist damit noch keine eigenständige Bedeutung der Inhaltskontrolle erreicht, vielmehr werden, wie im Bereich der Transparenzkontrolle, lediglich die materiellen Vorgaben des Datenschutzrechts AGB-rechtlich nachvollzogen.

(b) Grundsätze der Datenverarbeitung als spezieller Maßstab

Im Rahmen der datenschutzrechtlichen Beurteilung kommen insbesondere die Grundsätze der Datenverarbeitung als gesetzliches Leitbild in Betracht.[720] Dies umfasst Art. 5 Abs. 1 DS-GVO, aber auch weitere Grundsätze, die sich aus der DS-GVO induktiv gewinnen lassen, zum Beispiel *data protection by design* nach Art. 25 Abs. 1 DS-GVO.[721] Sind diese Grundsätze verletzt, so muss nach dem soeben Gesagten jeweils auch eine AGB-rechtliche unangemessene Benachteiligung angenommen werden. Zwar sind reine Auslegungsregeln kein im Rahmen von § 307 Abs. 2 Nr. 1 BGB zu berücksichtigender Maßstab;[722] die

die DSRL); LG Berlin, MMR 2018, 328 Rn. 63 ff.; LG Berlin MMR 2014, 563 (565 ff.); LG Berlin NJW 2013, 2605 (2606 f.); LG Berlin, Urt. v. 29.5.2002 – BeckRS 2002, 11506, unter 3.c)aa); OLG Düsseldorf, NJW-RR 1997, 374 (377); OLG Nürnberg, NJW-RR 1997, 1556 (1557); OLG Karlsruhe, Urt. v. 28.6.1996 – BeckRS 1996, 30978678, unter 2.b); OLG Naumburg, Urt. v. 21.7.1994 – BeckRS 1994, 31214988, unter II.1.d)dd).

[715] BGH GRUR 2020, 891 Rn. 44 ff. – Cookie-Einwilligung II; LG Berlin, MMR 2018, 328 Rn. 63 ff.; LG Berlin MMR 2014, 563 (565 ff.); LG Berlin NJW 2013, 2605 (2607).

[716] *Baetge*, AcP 202 (2002), 972 (984 f.); zu einer diesbezüglich immer noch erforderlichen, von der Rechtssprechung jedoch zumeist unterlassenen Abwägung siehe LG Berlin, Urt. v. 29.5.2002 – BeckRS 2002, 11506, unter 3.c)aa)(a.)(cc.).

[717] Wohl auch *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 71.

[718] KG BeckRS 2019, 8570 Rn. 66; KG MMR 2020, 239 Rn. 49 ff.; siehe auch BGH GRUR 2020, 891 Rn. 63 f. – Cookie-Einwilligung II.

[719] Ob zugleich eine Verletzung des Datenschutzgrundrechts erfolgt, hängt erstens davon ab, ob ihm horizontale Direktwirkung zugesprochen wird, sowie zweitens von der dogmatischen Verknüpfung von Sekundär- und Primärrecht. Dies muss hier nicht im Einzelnen weiterverfolgt werden. Siehe für das BDSG aF auch LG Berlin, Urt. v. 29.5.2002 – BeckRS 2002, 11506, unter 3.c)aa)(a.)(bb.).

[720] So auch *Engeler*, ZD 2018, 55 (60); *Helberger/Zuiderveen Borgesius/Reyna*, 54 Common Market Law Review 2017, 1427 (1451); *Indenhuck/Britz*, BB 2019, 1091 (1094).

[721] Dazu oben, § 4 C.III.1.

[722] BGH GRUR 2012, 1031 Rn. 16 ff. – Honorarbedingungen Freie Journalisten (zu § 31 Abs. 5 UrhG).

Grundsätze der Datenverarbeitung stellen jedoch, wie gesehen, echte Rechtspflichten dar, die nicht dispositiv sind, jedoch verletzt werden können.[723] Der BGH hat anerkannt, dass selbst ungeschriebene Rechtsgrundsätze Maßstab im Rahmen von § 307 Abs. 2 Nr. 1 BGB sein können.[724] Dann muss dies a fortiori für die positiv niedergelegten Grundsätze der Datenverarbeitung nach der DS-GVO gelten.

Allerdings sind diese Grundsätze, wie in der datenschutzrechtlichen Analyse gesehen, in erheblichem Maße ausfüllungsbedürftig und ihre Anwendung auf einzelne Fälle mit signifikanten Unsicherheiten behaftet. So wird es einerseits Fälle geben, welche zum Beispiel den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DS-GVO mit an Sicherheit grenzender Wahrscheinlichkeit nicht verletzen. Andererseits sind Fälle eklatant unverhältnismäßiger Datenverarbeitung (zum Beispiel Weiterleitung ins EU-Ausland zu Zwecken politischer Profilbildung) denkbar, die mit an Sicherheit grenzender Wahrscheinlichkeit einen Verstoß gegen den Grundsatz der Datenminimierung darstellen. Dazwischen liegt eine ausgedehnte Grauzone von Fällen, bei denen man nicht unmittelbar ex ante wird sagen können, ob sie den Grundsatz noch wahren oder nicht.

Nach hier vertretener Auffassung könnte in diesen Fällen nun das AGB-Recht das Zünglein an der Waage sein. Denn auch im sonstigen AGB-Recht kann an § 307 BGB scheitern, was individualvertraglich ohne Weiteres vereinbart werden kann (etwa starre Fristen zur Vornahme von Schönheitsreparaturen der Mietwohnung[725]). Diese Verschärfung ist gerade Folge des auf rationale Ignoranz gegründeten Marktversagens, das im Bereich der Datenverarbeitung, wie gezeigt, besonders virulent ist. Daher ist bereits der Umstand, dass ein Grundsatz der Datenverarbeitung berührt wird, bei der Unangemessenheit nach § 307 Abs. 2 Nr. 1 BGB zu berücksichtigen. Bei Grenzfällen, die unter der DS-GVO gerade noch legal sind, kann dann durch Verwendung von AGB die Schwelle zur Rechtswidrigkeit infolge unangemessener Benachteiligung überschritten werden. Insoweit reicht das AGB-Recht also über das Datenschutzrecht hinaus: Es führt, soweit AGB betroffen sind, zu einer (maßvollen) Verschärfung der Grundsätze der Datenverarbeitung.

---

[723] So wurde eine Lizenzklausel am urheberrechtlichen Grundsatz des § 11 S. 2 UrhR, wonach das Urheberrecht zugleich der Sicherung einer angemessenen Vergütung des Urhebers dient, gemessen und nach § 307 Abs. 2 Nr. 1 BGB für unangemessen erklärt in KG ZD 2014, 412 (417); siehe auch BGH GRUR 2012, 1031 Rn. 29 – Honorarbedingungen Freie Journalisten.

[724] BGH NJW 1984, 1182 (1182 f.); BGH NJW 1993, 721 (722); BGH NJW 2001, 3480 (3482).

[725] Zur AGB-rechtlichen Unwirksamkeit BGH NJW 2004, 2586; BGH NJW 2006, 2115; BGH NJW-RR 2012, 907.

(2) § 307 Abs. 2 Nr. 2 BGB

Daneben ist bei bestimmten Verträgen auch denkbar, dass ein Verstoß gegen Kardinalpflichten zu einer unangemessenen Benachteiligung nach § 307 Abs. 2 Nr. 2 BGB führt. Dies kann vor allem bei gesetzlich nicht geregelten Vertragstypen, wie sie in digitalen Austauschprozessen häufig vorkommen, Relevanz erlangen.[726] Letztlich betrifft diese Fallgruppe jedoch wohl vor allem Sonderkonstellationen, in denen der Vertragszweck klar gerade im Schutz personenbezogener Daten besteht. Dies kann etwa bei Verträgen über Verschlüsselungssoftware der Fall sein. Eine Klausel, die eine Weiterleitung zu nicht funktional erforderlichen Zwecken legitimiert (sei es auch im Rahmen einer Einwilligung), verstößt dann gegen § 307 Abs. 2 Nr. 2 BGB.

(3) § 307 Abs. 1 S. 1 BGB

Als besonders schwierig stellt sich im hier verhandelten Kontext der Rückgriff auf die Generalklausel des § 307 Abs. 1 S. 1 BGB dar. Zwar wird die danach erforderliche unangemessene Benachteiligung durch die Rechtsprechung des EuGH und zum Teil auch des BGH näher präzisiert. Diese Kriterien lassen sich jedoch nur teilweise auf die Prüfung von Hauptleistungspflichten übertragen. Gesichert erscheint lediglich, dass das Datenschutzgrundrecht, auch wenn man lediglich von einer mittelbaren Drittwirkung unter Privaten ausgeht,[727] im Rahmen der Beurteilung der Klausel nach § 307 Abs. 1 S. 1 BGB Berücksichtigung finden muss.[728]

(a) Die Rechtsprechung von EuGH und BGH

Bei der Bestimmung der unangemessenen Benachteiligung nach § 307 Abs. 1 S. 1 BGB spielt die richtlinienkonforme Auslegung eine besondere Rolle. Nach Art. 3 Abs. 1 der Klauselrichtlinie ist eine Klausel als missbräuchlich zu werten, „wenn sie entgegen dem Gebot von Treu und Glauben zum Nachteil des Verbrauchers ein erhebliches und ungerechtfertigtes Mißverhältnis der vertraglichen Rechte und Pflichten der Vertragspartner verursacht." Der EuGH hat die beiden Kriterien des erheblichen und ungerechtfertigten Missverhältnisses einerseits und der Verletzung von Treu und Glauben andererseits in seiner Recht-

[726] Vgl. *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 72; *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 261.

[727] So im Ergebnis BVerfG GRUR 2020, 88 Rn. 97 – Recht auf Vergessen II (ähnliche Wirkung wie mittelbare Drittwirkung); ebenso *Streinz/W. Michl*, EuZW 2011, 384 (387); zur möglichen horizontalen Direktwirkung auf Grundlage der jüngeren EuGH-Rechtsprechung siehe unten, § 5 C.III.4.a)aa).

[728] *Helberger/Zuiderveen Borgesius/Reyna*, 54 Common Market Law Review 2017, 1427 (1449 f.); *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 55; *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 18.

sprechung, besonders den Urteilen *Aziz* und *Menéndez Álvarez*, separat analysiert und konkretisiert.

Danach besteht ein erhebliches und ungerechtfertigtes Missverhältnis zwischen den Rechten und Pflichten der Vertragspartner, wenn die in Rede stehende Klausel signifikant von den nationalen Regelungen abweicht, die ohne die Klausel zum Zuge kämen.[729] Das Missverhältnis bestimmt sich daher aus einem Vergleich der gesetzlichen Regelung mit der an ihre Stelle tretenden vertraglichen Vereinbarung. Die vertragliche Regelung muss insoweit für den Verbraucher signifikant weniger günstig sein als die gesetzliche.[730] Dabei kann sich die hinreichend schwerwiegende Beeinträchtigung nur aus „der rechtlichen Stellung ergeben, die der Verbraucher als Partei des betreffenden Vertrags nach den anwendbaren nationalen Rechtsvorschriften innehat, sei es in Gestalt einer inhaltlichen Beschränkung der Rechte, die er nach diesen Vorschriften aus dem Vertrag herleitet, oder einer Beeinträchtigung der Ausübung dieser Rechte oder der Auferlegung einer zusätzlichen, nach den nationalen Vorschriften nicht vorgesehenen Verpflichtung."[731]

Die Verletzung von Treu und Glauben hingegen bestimmte EuGH anhand eines hypothetischen Vertragsverhandlungsmechanismus.[732] Dieser Maßstab ist dem Schuldrecht auch sonst nicht fremd.[733] Nach dem EuGH sind nun solche Klauseln als treuwidrig einzustufen, bei denen der Verwender „bei loyalem und billigem Verhalten gegenüber dem Verbraucher vernünftigerweise [nicht] erwarten durfte, dass der Verbraucher sich nach individuellen Verhandlungen auf eine solche Klausel einlässt."[734] Der Verweis auf das loyale und billige Verhalten des Verwenders findet sich auch im 16. Erwägungsgrund der Klauselrichtlinie. Davon ausgehend muss mithin eine Als-ob-Betrachtung angestellt werden, die aus der Perspektive der Erkenntnismöglichkeiten eines loyalen Verwenders danach fragt, ob der Vertragspartner die Klausel akzeptiert hätte. Diese Ausrichtung des Maßstabs auf den Vertragspartner ist wegen vermeintlicher Subjektivierung der an sich objektiv-rechtlichen Kriterien der AGB-Kontrolle auf Kritik gestoßen,[735] kann jedoch durch eine hinreichende Objektivierung des normativen Referenzakteurs mit den Zielen der Inhaltskontrolle in Einklang gebracht werden.[736] Dabei muss jedoch auch in Rechnung gestellt

[729] EuGH, Urt. v. 14.3.2013 – Rs. C-415/11 (*Aziz*) – Rn. 68; Urt. v. 16.1.2014 – Rs. C-226/12 (*Menéndez Álvarez*) – Rn. 21.

[730] EuGH, Urt. v. 14.3.2013 – Rs. C-415/11 (*Aziz*) – Rn. 68; Urt. v. 16.1.2014 – Rs. C-226/12 (*Menéndez Álvarez*) – Rn. 21; vgl. auch *Fuchs* in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016, § 307 BGB Rn. 98.

[731] EuGH, Urt. v. 16.1.2014 – Rs. C-226/12 (*Menéndez Álvarez*) – Rn. 23.

[732] *Lüttringhaus*, Vertragsfreiheit und ihre Materialisierung im Europäischen Binnenmarkt, 2018, 377 f.

[733] *Eidenmüller*, JZ 2005, 216 (222), zu § 275 Abs. 2.

[734] EuGH, Urt. v. 14.3.2013 – Rs. C-415/11 (*Aziz*) – Rn. 69.

[735] *Ebers*, LMK 2013, 345483; *Marín López*, Revista CESCO de Derecho de Consumo 2013 (5), 35 (41 f.).

[736] Zur Frage des Referenzakteurs sogleich, § 5 C.II.1.e)bb)(3)(b)(bb).

werden, inwiefern der Vertragspartner nach dem einschlägigen (nationalen oder unionalen) Recht Möglichkeiten hat, die für ihn nachteilige Wirkung zu beseitigen.[737] Bei der Prüfung einer Einwilligung ist daher immer das Widerrufsrecht nach Art. 7 Abs. 3 DS-GVO zu berücksichtigen.

(b) Unangemessenheitskriterien für Hauptleistungspflichten

Diese Kriterien passen jedoch nur partiell für die Untersuchung der datenschutzrechtlich relevanten Klauseln oder Einwilligungen. Kaum zielführend zu operationalisieren ist insoweit das Erfordernis des Vergleichs mit Regelungen, die anstelle der jeweiligen Klauseln nach geltendem Recht greifen würden. Inwieweit man hier ein erhebliches Missverhältnis erkennen möchte, hängt davon ab, ob die jeweilige Klausel bzw. Einwilligung isoliert oder im Kontext der anderen Vertragsklauseln, insbesondere konnexer Leistungspflichten des Anbieters, zu beurteilen ist.[738]

Optiert man für eine isolierte Betrachtung, so ist zu konstatieren, dass es für eine Verpflichtung zur Abgabe einer Einwilligung bzw. zur Überlassung von Daten bereits an einer dispositiven Gesetzesregelung mangelt, sodass allenfalls auf die ergänzende Vertragsauslegung zurückgegriffen werden könnte.[739] Ohne die Einwilligung selbst hingegen müsste ein gesetzlicher Erlaubnistatbestand nach Art. 6 Abs. 1 DS-GVO eingreifen. Wo dies nicht der Fall ist, so könnte man meinen, weicht zumindest die Einwilligung zum Nachteil des Verbrauchers erheblich von der ohne Einwilligung bestehenden Rechtslage ab, da sie eine Datenverarbeitung gestattet. Bereits dies erscheint jedoch äußerst zweifelhaft, da die Datenverarbeitung auf Grundlage einer informierten und freien Einwilligung durchaus gewünscht sein kann und daher nicht pauschal nachteilig ist. Ferner ließe dies außer Acht, dass ohne die Einwilligung, wenn sie eine Gegenleistung darstellt, regelmäßig auch die vertragliche Pflicht des Anbieters zur Erbringung der Leistung entfällt.[740]

Daher erscheint es grundsätzlich vorzugswürdig, konnexe Leistungspflichten in die Betrachtung einzubeziehen.[741] Ein Vertrag beschreibt immer

---

[737] EuGH, Urt. v. 14.3.2013 – Rs. C-415/11 (*Aziz*) – Rn. 73; kritisch dazu *Ebers*, LMK 2013, 345483; *Marín López*, Revista CESCO de Derecho de Consumo 2013 (5), 35 (40).

[738] Dieses Problem wird sonst, soweit ersichtlich, lediglich für Klauseln diskutiert, die nicht den Hauptgegenstand des Vertrags ausmachen; die herrschende Meinung geht von einer grundsätzlich isolierten Prüfung aus, die jedoch im Einzelfall durch kompensierende und summierende Vertragselemente angereichert werden kann; siehe etwa *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 124 ff.; *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 38 ff.; *Fastrich*, Richterliche Inhaltskontrolle im Privatrecht, 1992, 302.

[739] Dazu im Einzelnen unten, § 5 C.II.1.f).

[740] Dies gilt jedenfalls für künftige Vertragschlüsse, für die der Anbieter dann nicht mehr die unwirksame Einwilligung als Gegenleistung akzeptieren wird. Aber auch bei bestehenden Verträgen kann die Leistungspflicht des Anbieters entfallen, wenn die Einwilligung unwirksam ist, siehe oben, Text bei § 5, Fn. 536.

[741] Zur Anerkennung der Kompensationwirkung konnexer Pflichten BGH NJW 2003,

ein Bündel von Rechten und Pflichten, dessen einzelne Hauptleistungspflichten nicht separat daraufhin untersucht werden können, ob sie ein erhebliches Missverhältnis zulasten des Verbrauchers bewirken: Die vertragliche Leistung steht in unabweislichem ökonomischen und auch rechtlichen Zusammenhang mit der datenbasierten Gegenleistung. Eine grundsätzlich auf konnexe Pflichten ausgeweitete Betrachtung zeichnet auch Art. 4 Abs. 1 der Klauselrichtlinie vor, wonach die Missbräuchlichkeit einer Klausel unter Berücksichtigung aller anderen Klauseln des Vertrags beurteilt werden muss.[742] Auch der EuGH hat in *Menéndez Álvarez* implizit anerkannt, dass bei der Feststellung des erheblichen Missverhältnisses berücksichtigt werden muss, inwiefern eine Klausel eine Gegenleistung zu anderen Vertragsklauseln darstellt, sofern eine derartige Konnexität denn tatsächlich vorliegt.[743]

Daher muss bei der Beurteilung der Belastung des Nutzers durch die Gegenleistungspflicht an sich der Vorteil des Anspruchs auf die Leistung kompensierend in Rechnung gestellt werden. Um jedoch zu eruieren, ob der Verbraucher durch die fragliche Klausel schlechter gestellt wird, müsste man daher, um dem vertraglichen Gefüge Rechnung zu tragen, untersuchen, inwiefern ein auffälliges Missverhältnis gerade zwischen Leistung und Gegenleistung besteht. Dies entspricht zwar durchaus dem Wortlaut von Art. 3 Abs. 1 der Klauselrichtlinie (in Verbindung mit der teleologischen Reduktion von Art. 4 Abs. 2 der Klauselrichtlinie), ist nach deutschem Verständnis jedoch, wie bereits erwähnt, der Kontrolle nach § 138 Abs. 1 BGB vorbehalten. Insgesamt passt die Prüfungsvorgabe des EuGH für das erhebliche Missverhältnis daher ersichtlich nicht auf die Kontrolle von Hauptleistungspflichten.

(aa) Der *Aziz*-Test

Letztlich erscheint es daher für die Prüfung der Hauptleistungspflichten vorzugswürdig, auf eine Differenzierung der unangemessenen Benachteiligung bzw. Missbräuchlichkeit in ein erhebliches Missverhältnis einerseits und die Verletzung von Treu und Glauben andererseits zu verzichten. Die Trennung der beiden Kriterien ist ohnehin in der Literatur umstritten[744] und wird in der Umsetzungspraxis der Mitgliedstaaten verschieden gehandhabt.[745] Stattdessen muss im Rahmen einer Gesamtabwägung geprüft werden, ob die jeweilige Klausel im Kontext des Gesamtvertrags eine unangemessene Benachteiligung

888 (890 f.); *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 38; *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 125 f.

[742] Siehe auch EuGH, Urt. v. 21.2.2013 – Rs. C-472/11 (*Banif Plus Bank*) – Rn. 40; Urt. v. 16.1.2014 – Rs. C-226/12 (*Menéndez Álvarez*) – Rn. 24.

[743] EuGH, Urt. v. 16.1.2014 – Rs. C-226/12 (*Menéndez Álvarez*) – Rn. 29.

[744] Ausführlich *Nebbia*, Unfair Contract Terms in European Law, 2007, 143 ff.; *Stempel*, Treu und Glauben im Unionsprivatrecht, 2016, 86; *Ebers*, LMK 2013, 345483.

[745] *Schulte-Nölke/Twigg-Flesner/Ebers*, EC Consumer Law Compendium: The Consumer Acquis and its transposition in the Member States, München 2008, 232; *Stempel*, Treu und Glauben im Unionsprivatrecht, 2016, 88.

hervorruft.[746] Dies ist im Rahmen einer umfassenden Interessenabwägung zu ermitteln,[747] die jedoch in spezifischer Weise operationalisiert werden kann durch den Test, den der EuGH gerade für das zweite Element der Unangemessenheit entwickelt hat: ob der Klausel bei hypothetischen, fairen, individuellen Vertragsverhandlungen zugestimmt worden wäre.

Dieser auf den hypothetischen Verhandlungsmechanismus reduzierte *Aziz*-Test erscheint aus drei Gründen angemessen. Erstens greift der Test gerade solche Klauseln heraus, die bei hypothetischer Behebung des für die AGB-Kontrolle entscheidenden Marktversagens, der rationalen Ignoranz, nicht vereinbart worden wären. Er entspricht damit einer teleologisch-funktionalen Interpretation der Inhaltskontrolle als Mechanismus zum Ausgleich der Folgen eines spezifischen Marktversagens.[748]

Zweitens ist das Kriterium auch in systematischer Hinsicht stimmig. So findet sich in der Rechtsprechung auch in anderen Bereichen des Marktordnungsrechts eine Als-ob-Betrachtung zur Korrektur von Marktversagen. Im Bereich des Konditionenmissbrauchs im Kartellrecht wird nach Art. 102 Abs. 2 lit. a AEUV und § 19 Abs. 2 Nr. 2 GWB ebenso danach gefragt, ob die in Rede stehenden Konditionen bei funktionierenden Marktverhältnissen vereinbart worden wären.[749] Auch dort wird dieses Erfordernis damit begründet, dass letztlich die Kausalität des jeweiligen Marktversagens für die Klausel nachgewiesen werden muss.[750]

Drittens handelt es sich um einen sekundär marktbezogenen Test, der zumindest den Anspruch erhebt, die richterliche Klauselkontrolle durch einen Aushandlungsmechanismus zu operationalisieren.[751] Zwar ist das Ergebnis dieses hypothetischen Verhandlungsmechanismus nicht immer zweifelsfrei feststellbar.[752] Dem kann jedoch dadurch Rechnung getragen werden, dass die Klauselkontrolle, wie es der Respekt vor der jedenfalls grundsätzlich marktbezogenen Preisfindung und der Privatautonomie der Vertragsparteien erfor-

[746] So auch *Stempel*, Treu und Glauben im Unionsprivatrecht, 2016, 88, 98; *Pfeiffer*, in: Grabitz/Hilf, Das Recht der Europäischen Union, 40. Aufl. 2009, Sekundärrecht, A5, Art. 3 Mißbrauchskontrolle Rn. 64, die beide den Grundsatz von Treu und Glauben für die Gesamtabwägung als zentral ansehen; anders *Grundmann*, Europäisches Schuldvertragsrecht, 1999, 2. Teil, § 5 III. Rn. 22, der das erhebliche Missverhältnis als konkreter und daher wichtiger darstellt, was allerdings bei Hauptleistungspflichten, wie dargelegt, nicht fruchten kann.

[747] Siehe nur BGH NJW 2000, 1110 (1112); *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 96.

[748] Ähnlich *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 43.

[749] BGH NVwZ-RR 2014, 515 Rn. 65; *Franck*, ZWeR 2016, 137 (153 f.); *Fuchs/Möschel*, in: Immenga/Mestmäcker, Wettbewerbsrecht, 5. Aufl. 2014, § 19 GWB Rn. 259; für das Unionsrecht ist der Maßstab allerdings deutlich unklarer, siehe *Franck*, ZWeR 2016, 137 (148 ff.); *Fuchs*, in: Immenga/Mestmäcker, Wettbewerbsrecht, 6. Aufl. 2019, Art. 102 AEUV Rn. 175 ff.

[750] *Franck*, ZWeR 2016, 137 (151 ff.).

[751] So auch *Kötz*, JuS 2003, 209 (213 f.).

[752] Dazu genauer unten, § 5, Fn. 769 f.

dert, nur zurückhaltend angewandt wird.[753] Lediglich dann, wenn es als hinreichend sicher erscheint, dass der hypothetische Verhandlungstest fehlschlägt, die Klausel also in individuellen Verhandlungen nicht vereinbart worden wäre, kann von einer Unangemessenheit ausgegangen werden.

(bb) Der relevante Referenzakteur

Rückt damit der hypothetische Aushandlungsmechanismus in den Mittelpunkt der Unangemessenheitsprüfung, so stellt sich mit verstärkter Dringlichkeit die Frage, von welchem Referenzakteur auf Seiten des Verbrauchers bzw. Nutzers ausgegangen werden muss. Der EuGH verwendet in seiner Rechtsprechung auch mit Blick auf den Verbraucherbegriff des AGB-Rechts seine Formel vom durchschnittlich informierten, situationsadäquat aufmerksamen, verständigen Durchschnittsverbraucher.[754] Zwar fragte der EuGH im Rahmen des *Aziz*-Tests danach, inwiefern „der Verbraucher" sich auf die Klausel eingelassen hätte.[755] Allerdings dürfte dies nicht als Abkehr von dem grundsätzlich abstrakt-generellen Auslegungsmaßstab der Klauselkontrolle zu verstehen sein,[756] der eine typisierende Interessenabwägung zum Gegenstand hat, Einzelfallumstände hingegen ausblendet[757] und auch für die Frage der Unangemessenheit Geltung beansprucht.[758] Zwar können bestimmte Eigenheiten einer durch eine Klausel angesprochenen Kundengruppe durchaus berücksichtigt werden.[759] Schon um die Transaktionskostenverringerung durch die Verwendung von AGB nicht vollkommen aufzuheben, verbietet es sich jedoch, grundsätzlich einen konkret-individuellen Prüfungsmaßstab anzulegen, der danach fragen würde, ob der jeweils konkret in Rede stehende Verbraucher der Klausel bei hypothetischen Vertragsverhandlungen zugestimmt hätte. Denn dies kann der Verwender regelmäßig nicht ohne unzumutbaren Aufwand feststellen. Daher muss für den Bereich des Datenprivatrechts grundsätzlich von einem Akteur mit durchschnittlichen, also mittelstark ausgeprägten, Datenschutzpräferenzen ausgegangen werden.

---

[753] Vgl. *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 5, 95; *Looschelders/Olzen*, in: Staudinger, BGB, 2015, § 242 Rn. 464; *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 526 ff., 541.

[754] EuGH, Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 74; *Rott*, in: Twigg-Flesner (Hrsg.), Research Handbook on EU Consumer and Contract Law, 287 (296).

[755] EuGH, Urt. v. 14.3.2013 – Rs. C-415/11 (*Aziz*) – Rn. 69.

[756] Für eine Relevanz des rationalen Verbrauchers im Zusammenhang mit dem hypothetischen Vertragstest auch *Iglesias Sánchez*, 51 Common Market Law Review 2014, 955 (966).

[757] BGH NJW 1982, 765; BGH NJW 1980, 1947; BGH GRUR 2012, 1031 Rn. 19 – Honorarbedingungen Freie Journalisten; BGH NJW 2017, 2762 Rn. 19; *Schlosser*, in: Staudinger, BGB, 2013, § 305c Rn. 126.

[758] *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 41.

[759] BGH NJW 2017, 2762 Rn. 19: „Verständnismöglichkeiten des durchschnittlichen Vertragspartners"; *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 305c Rn. 35.

Man kommt jedoch nicht umhin zu konstatieren, dass dieses Ergebnis angesichts der empirischen Ausprägung von Datenschutzpräferenzen äußerst unbefriedigend ist. Zumeist haben die Akteure entweder hohe oder niedrige Datenschutzpräferenzen,[760] und dies wird ihre Zustimmungsbereitschaft hinsichtlich datenschutzrechtlich relevanter Klauseln in hypothetischen Vertragsverhandlungen ganz entscheidend beeinflussen. Das Desiderat muss daher darin bestehen, heterogene Datenschutzpräferenzen auch hinsichtlich des Ausgangs des *Aziz*-Tests abzubilden, ohne zugleich dem Verwender, der unangemessene Klauseln vermeiden möchte, unzumutbare Nachforschungspflichten hinsichtlich der Präferenzen der jeweiligen Vertragspartner aufzuerlegen.

Daher bietet es sich an, den *Aziz*-Test und damit die Bestimmung der unangemessenen Benachteiligung gruppenspezifisch zu personalisieren, wenn für den Verwender klare Anhaltspunkte bestehen, dass der konkrete Verbraucher gegenüber der jeweiligen Klausel ablehnende Präferenzen hat. Dies ergibt sich zwanglos, wenn man mit einem Teil der Literatur von der grundsätzlichen Beachtlichkeit der Einzelfallumstände ausgeht.[761] Diese Ansicht findet für Verbraucherverträge eine Stütze in Art. 4 Abs. 1 der Klauselrichtlinie, wonach sich die Missbräuchlichkeit einer Klausel unter anderem auf Grundlage „aller den Vertragsabschluß begleitenden Umstände" beurteilt.[762] Diese Regelung wurde im deutschen Recht in § 310 Abs. 3 Nr. 3 BGB umgesetzt, wonach die den Vertragsschluss begleitenden Umstände für die Beurteilung der unangemessenen Benachteiligung berücksichtigt werden müssen.

Auf Grundlage der Transaktionskostenminimierungsstruktur der AGB kann dies jedoch nur dann überzeugen, wenn die Umstände für den Verwender klar erkennbar sind.[763] Dies folgt in dogmatischer Hinsicht auch daraus, dass der EuGH in *Aziz* eindeutig festgehalten hat, dass für die Bestimmung der Missbräuchlichkeit einer Klausel entscheidend ist, ob der Verwender *erwarten*

---

[760] Siehe oben, § 3, Fn. 163.

[761] *Schmidt*, in: BeckOK BGB, 51. Ed. 2019, § 305c Rn. 47.

[762] EuGH, Urt. v. 14.3.2013 – Rs. C-415/11 (*Aziz*) – Rn. 71; Urt. v. 21.2.2013 – Rs. C-472/11 (*Banif Plus Bank*) – Rn. 40; Urt. v. 16.1.2014 – Rs. C-226/12 (*Menéndez Álvarez*) – Rn. 24.

[763] Ähnlich *Schlosser*, in: Staudinger, BGB, 2013, § 305c Rn. 130; *Remien*, ZEuP 1994, 34 (54, 56); zur allgemeinen Kontroverse um die Interpretation von § 310 Abs. 3 Nr. 3 BGB siehe den Überblick bei *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 310 Rn. 110, 114 sowie *Damm*, JZ 1994, 161 (172–174); *Hommelhoff/Wiedenmann*, ZIP 1993, 562 (568 ff.); *Schmidt-Salzer*, BB 1995, 733 (736 f.); *Brandner*, MDR 1997, 312 (314); *Börner*, JZ 1995, 595; *Michalski*, DB 1999, 677; *Fuchs*, in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016, Vorbemerkungen zur Inhaltskontrolle Rn. 50; *Stempel*, Treu und Glauben im Unionsprivatrecht, 2016, 94 ff.; noch enger als hier *Becker*, in: BeckOK BGB, 51. Ed. 2019, § 310 Rn. 21 mit der (wohl nicht mehr richtlinienkonformen) Auslegung, dass nur „allgemeine äußere Umstände, die zum Vertragsschluss geführt haben und auf einen verallgemeinerbaren Willen des Verwenders schließen lassen", zu berücksichtigen sind; diese Formel findet sich abgewandelt bei BGH NJW 2018, 2117 Rn. 18; BAG NJW 2011, 101 Rn. 51, allerdings gerade nicht hinsichtlich der Unangemessenheit nach § 310 Abs. 3 Nr. 3 BGB, sondern als Maßstab der generellen Auslegung.

konnte, dass die andere Vertragspartei der Klausel zustimmt.[764] Eine solche Erwartung kann sich jedoch nur auf Umstände stützen, die dem Verwender bekannt sind. Dessen Erkenntnismöglichkeiten sind im vernetzten Umfeld freilich ungleich besser ausgeprägt als in der analogen Welt. Sie können sich etwa aus besonders ausgeprägten Datenschutzpräferenzen ableiten lassen, welche der Verwender, auch bei anderem Anlass, hinsichtlich dieses konkreten Verbrauchers festgestellt hat. Diese mögen sich entweder durch die aktive Auswahl von Datenschutzvoreinstellungen durch den Nutzer oder aber die z. B. durch Modelle maschinellen Lernens gestützte Analyse des Verhaltens des jeweiligen Nutzers ergeben. Sofern der Verwender Datenanalyse betreibt, um diese zum eigenen Vorteil hinsichtlich potenzieller Vertragsschlüsse mit dem Nutzer zu gebrauchen, muss er richtigerweise in Ausprägung des Rechtssatzes *qui habet commoda ferre debet onera*[765] auch hinnehmen, dass dieses Zusatzwissen im Rahmen der Ableitung des hypothetischen Verhandlungsergebnisses berücksichtigt wird. Kann also Facebook aus dem bisherigen Verhalten eines Nutzers schließen, dass dieser Datenschutzrechtsaktivist ist, so ist dies bei der Bewertung der Konsensfähigkeit der Klausel negativ zu berücksichtigen. Allerdings kann hier, zur Vermeidung von unzumutbaren Transaktionskosten des Anbieters, nur positives Wissen, nicht jedoch fahrlässige Unkenntnis, Berücksichtigung finden.[766] Damit lässt sich eine gewisse „Personalisierung" des *Aziz*-Tests erreichen, die freilich nur im Individualprozess, nicht aber im Verbandsklageverfahren, fruchten kann.[767]

(c) Ergebnis

Insgesamt ist damit festzustellen, dass für den Fall der Kontrolle von Hauptleistungspflichten die *Aziz*-Rechtsprechung des EuGH in adaptierter Form angewandt werden muss. Damit greift ein hypothetischer Aushandlungsmechanismus (*Aziz*-Test), der eine zumindest sekundär an Marktprozesse angeknüpfte Lösung ermöglicht und bei Kenntnis des Verwenders von den Datenschutzpräferenzen des Vertragspartners gruppenspezifisch personalisiert werden kann. Dabei ist die Inhaltskontrolle jedoch insgesamt zurückhaltend anzuwenden,[768] aus drei Gründen:

---

[764] EuGH, Urt. v. 14.3.2013 – Rs. C-415/11 (*Aziz*) – Rn. 69.

[765] Zu diesem Rechtssatz *Zimmermann*, The Law of Obligations, 1990, 201 Fn. 108 und 290.

[766] Zur Wissenszurechnung beim Einsatz KI-gestützter Systeme siehe *Hacker*, RW 9 (2018), 243 (270 ff.).

[767] Art. 4 Abs. 1 der Klauselrichtlinie nimmt das Verbandsklageverfahren nach Art. 7 der Richtlinie schon dem Wortlaut nach aus: BGH, NJW 2001, 2971 (2972); *Damm*, JZ 1994, 161 (173 f.); *Heinrichs*, NJW 1996, 2190 (2194); *Brandner*, MDR 1997, 312 (314); *Michalski*, DB 1999, 677 (680); *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 310 Rn. 114.

[768] Im Ergebnis ebenso *Schweitzer/Fetzer/Peitz*, Digitale Plattformen: Bausteine für

Erstens lässt sich das Ergebnis des hypothetischen Aushandlungsmechanismus nur selten mit hinreichender Exaktheit bestimmen.[769] GA *Kokott* suchte in ihren Schlussanträgen zu *Aziz* nach Kriterien und fand diese in einem weiten Strauß von Parametern: Zu berücksichtigen seien unter anderem die Üblichkeit der Klausel im Rechtsverkehr,[770] ein eventueller sachlicher Grund für die Klausel sowie residuale Schutzmechanismen zugunsten des Verbrauchers bezüglich des Regelungsgegenstands der Klausel.[771] Diese Auswahl an Kriterien macht das Ergebnis jedoch kaum präziser bestimmbar,[772] zumal im Kontext des Datenschutzprivatrechts dem Datenschutzgrundrecht und den Datenschutzpräferenzen erhebliche Bedeutung zukommt.

Zweitens gebietet es der Respekt vor der grundsätzlich marktorientierten Findung der Hauptleistungspflichten und der Privatautonomie der Parteien, deren Bedeutung durch rationale Ignoranz zwar gemindert, aber nicht vollständig aufgehoben wird, bei der Kontrolle der Hauptleistungspflichten durch die Rechtsprechung Zurückhaltung obwalten zu lassen.[773]

Schließlich ist nicht zu verkennen, dass eine über das Datenschutzrecht hinausgehende Verkürzung der Möglichkeit der Datengewinnung für KMUs, die selbst noch nicht über hinreichende Daten verfügen, eine genuine Marktzutrittsbarriere darstellt.[774] Daher sollte eine unangemessene Benachteiligung § 307 Abs. 1 S. 1 BGB nur dann angenommen werden, wenn eine hinreichende Konfidenz besteht, dass der *Aziz*-Test negativ ausfällt.

---

einen künftigen Ordnungsrahmen, ZEW Discussion Paper No. 16–042, 2016, ftp.zew.de/pub/zew-docs/dp/dpl6042.pdf, 23; grundsätzlich auch *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 5, 95.

[769] In der rechtsökonomischen Literatur wird hier vorgeschlagen, eine Einigung auf eine Klausel nach dem Prinzip des *cheapest cost avoider* oder des *cheapest insurer* anzunehmen, vgl. etwa *Kötz*, NJW 1984, 2447 (2447); *Kötz*, JuS 2003, 209 (214); *Stoffels/Lohmann*, VersR 2003, 1343; *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 44. Dies kann jedoch im Kontext des Datenschutzprivatrechts nicht überzeugen, da die Zustimmung des Nutzers vor allem von seinen Datenschutzpräferenzen abhängen wird und potenzielle Schadenskosten regelmäßig kaum quantifiziert werden können.

[770] Dieses Kriterium ist schon grundsätzlich abzulehnen, da die Verbreitung einer Klausel auf dem Markt nichts über die normative Frage der Unangemessenheit aussagt; siehe auch *Stempel*, Treu und Glauben im Unionsprivatrecht, 2016, 134.

[771] GA *Kokott*, Schlussanträge v. 8.11.2012 – Rs. C-415/11 (*Aziz*) – Rn. 75.

[772] *Marín López*, Revista CESCO de Derecho de Consumo 2013 (5), 35 (41 f.), der allerdings schlussendlich – nicht überzeugend – annimmt, dass jede Abweichung vom dispositiven Recht in hypothetischen Vertragsverhandlungen abgelehnt würde (ebd., 42); unklar ist auch die Relevanz des Preisarguments, *Stempel*, Treu und Glauben im Unionsprivatrecht, 2016, 134; insgesamt handelt es sich jedoch um einen tendenziell strengen Standard, *Riesenhuber*, EU-Vertragsrecht, 2013, 170.

[773] Siehe die Nachweise oben, § 5, Fn. 753.

[774] *Schweitzer/Fetzer/Peitz*, Digitale Plattformen: Bausteine für einen künftigen Ordnungsrahmen, ZEW Discussion Paper No. 16–042, 2016, ftp.zew.de/pub/zew-docs/dp/dpl6042.pdf, 23.

cc) Anwendung auf die drei Leitfälle

Diese Kriterien können wiederum auf die drei Leitfälle angewandt werden. Dabei interessiert einerseits die Inhaltskontrolle von Einwilligungserklärungen und andererseits die von Vertragsklauseln, die eine Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO ermöglichen. Naturgemäß können hierbei nicht alle in Betracht kommenden Klauseln gewürdigt werden.[775]

(1) Datenweiterleitung an und Datenerhebung durch Dritte

Im Rahmen des ersten und zweiten Leitfalles sind Einwilligungen und Vertragsklauseln relevant, welche die Weiterleitung von Daten an Dritte und die Datenerhebung durch Dritte, etwa durch Tracking-Instrumente, ermöglichen.

(a) Einwilligung

Wie die datenschutzrechtliche Analyse gezeigt hat, scheitert die Einwilligung häufig bereits an den engen Voraussetzungen der DS-GVO im Rahmen der ersten beiden Leitfälle. Dann ist jedoch, wie eben gesehen, bereits § 307 Abs. 2 Nr. 1 BGB einschlägig. Anders kann sich dies allerdings darstellen, wenn Anbieter eine datenschonende Option neben dem einwilligungsbasierten Regime anbieten. Dann greift das Koppelungsverbot nach Art. 7 Abs. 4 DS-GVO nicht mehr und es ist denkbar, dass die Einwilligung in datenschutzrechtskonformer Weise auch auf die Datenweiterleitung zum Zwecke personalisierter Werbung und auf das Einverständnis mit der Nutzung von Tracking-Instrumenten erstreckt wird.

Damit erhebt sich die Frage, ob eine derartig weit gespannte Einwilligung eine unangemessene Benachteiligung des Nutzers nach § 307 Abs. 1 S. 1 BGB darstellen kann. Die Einwilligung ist, wie gesehen, wegen der rechtsgestaltenden Wirkung uneingeschränkt kontrollfähig. Es ist daher danach zu fragen, ob die spezifische Einwilligung das Ergebnis eines hypothetischen Verhandlungsmechanismus sein könnte. Dabei muss, wie ausgeführt, der gesamte Vertragskontext in den Blick genommen werden. Insbesondere muss die Widerruflichkeit der Einwilligung berücksichtigt und auch in Rechnung gestellt werden, wenn eine datenschonende Option angeboten wird. Denn auch sonst ist anerkannt, dass im Rahmen einer Tarifwahl eine Preisreduzierung solchen Klauseln, die bei höherpreisigen Tarifen unangemessen wären, zur Wirksamkeit verhelfen kann, wenn die Verknüpfung von geringerem Preis und anderweitiger Belastung des Vertragspartners für diesen transparent gemacht wird.[776]

[775] Zur AGB-Kontrolle von Klauseln in datenbasierten Rabattmodellen etwa ausführlich *Rudkowski* ZVersWiss 2017, 453 (466 ff., 487 ff., 494 ff.); ferner *Hacker*, ZfPW 2019, 148 (190).

[776] *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 310 Rn. 116; *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 49; *Fuchs* in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016, § 307 BGB Rn. 148; *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 138; *Fastrich*, Richterliche

Dies kann zwar nicht implizieren, dass im Rahmen der monetär kostenlosen, einwilligungsbasierten Option „alles erlaubt" ist. Dies ist jedoch schon deshalb nicht der Fall, weil die DS-GVO auch für die nicht datenschonende Option unverändert gilt.

Vor diesem Hintergrund darf ein Verfehlen des *Aziz*-Tests nur in besonderen Ausnahmesituationen mit hinreichender Konfidenz angenommen werden.[777] Der BGH hat in seiner *SCHUFA*-Entscheidung von 1985 entschieden, dass eine Generaleinwilligung unangemessen ist, mit der das Einverständnis in die Übermittlung sämtlicher Kreditinformationen an die SCHUFA erklärt wird.[778] Der BGH hat dies damit begründet, dass das BDSG aF sich „grundsätzlich für den Schutz personenbezogener Daten entschieden" habe.[779] Dem muss man jedoch hinzufügen, dass der DS-GVO die bereits mehrfach erwähnte doppelte Schutzrichtung innewohnt, die auch die Interessen und Rechte des Verantwortlichen an einer Nutzung personenbezogener Daten anerkennt. Daher wird man lediglich in Extremfällen annehmen können, dass eine durch Einwilligung erteilte Befugnis zur Datenweiterleitung oder zum Tracking unangemessen wäre, da ein hinreichend informierter Vertragspartner mit durchschnittlichen Datenschutzpräferenzen ihr im Rahmen individueller Verhandlungen nicht zugestimmt hätte. Dies kann etwa der Fall sein, wenn sich die Einwilligung auf praktisch alle Datentypen und Lebensbereiche erstreckt oder wegen der Weiterleitung ins EU-Ausland besondere Gefahren mit sich bringt.[780] Allerdings dürfte in diesen Fällen die Einwilligung parallel bereits an einem Verstoß gegen das Gebot der Bestimmtheit (Art. 4 Nr. 11 DS-GVO), den Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DS-GVO) oder auch der Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO) oder, bei Weiterleitung ins EU-Ausland, gegen die Anforderungen nach Art. 49 Abs. 1 lit. a DS-GVO scheitern. Insofern wird regelmäßig die DS-GVO für die Einwilligung das Maß aller Dinge bleiben.

(b) Vertragsklauseln

Bei der Inhaltskontrolle von datenschutzrechtlich relevanten Vertragsklauseln ist wiederum zwischen verschiedenen Typen zu differenzieren: der Verpflichtung zur Abgabe einer Einwilligung; der Verpflichtung zur Überlassung von personenbezogenen Daten; sowie schließlich der besonders relevanten weiten (Neben)Leistungspflicht.

Inhaltskontrolle im Privatrecht, 1992, 302; dies erwägend BGH NJW 1980, 1953 (1955); BGH NJW-RR 1989, 243 (244).

777 Siehe auch *Hacker*, ZfPW 2019, 148 (191 f.).

778 BGH NJW 1986, 46 (47); zuletzt auch OLG Düsseldorf MMR 2007, 387 (388).

779 BGH NJW 1986, 46 (47); ebenso OLG Düsseldorf MMR 2007, 387 (388).

780 Zur Unangemessenheit wegen Weiterleitung der Daten ins Ausland siehe ebenfalls BGH NJW 1986, 46 (47).

(aa) Verpflichtung zur Einwilligung

Die Verpflichtung zur Abgabe einer Einwilligung wird regelmäßig keine unangemessene Benachteiligung darstellen. Denn der Nutzer kann sich dieser Verpflichtung jederzeit durch Widerruf der Einwilligung entziehen. Dies ist nach der *Aziz*-Rechtsprechung explizit zu berücksichtigen.[781] Allenfalls ist die genannte Verpflichtung dann im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO relevant und streitet für ein Überwiegen der Interessen des Anbieters, auch dies jedoch nur, wenn die Verpflichtung in besonders sichtbarer Weise, also nicht lediglich in AGB, gegenüber dem Nutzer offengelegt wurde.[782] Auch in diesem Fall ist jedoch, da insofern keine rationale Ignoranz vorliegt, keine unangemessene Benachteiligung zu erkennen.

(bb) Verpflichtung zur Datenüberlassung

Die Verpflichtung, Daten zu überlassen, ist neben der Verpflichtung zur Abgabe einer Einwilligung die zweite mögliche Variante der Gegenleistung im Geschäftsmodell Dienst gegen Daten.[783] Sie führt zwar wegen der hier vertretenen datenschutzrechtlichen Irrelevanz von Nutzerpflichten nicht zur Legitimierung der Datenverarbeitung,[784] ist aber insoweit relevant, als ein Schadensersatz des Anbieters möglich ist, wenn eine derartige Verpflichtung wirksam vereinbart wird, Daten jedoch nicht oder fehlerhaft überlassen werden.[785] Eine Unangemessenheit wird sich dabei, wie gesehen, regelmäßig lediglich aus dem Verhältnis zur Leistung des Anbieters ableiten lassen. Dessen Evaluation ist jedoch, wie ausgeführt, einer Analyse im Rahmen von § 138 Abs. 1 BGB überlassen. Dass die Verpflichtung, Daten zu überlassen, als solche im Rahmen des Vertragskontextes als unangemessen beurteilt wird, ist lediglich für krasse Ausnahmefälle denkbar, in denen auch die Einwilligung unangemessen wäre (z. B. Verpflichtung zur Überlassung praktisch aller Datentypen in allen Lebensbereichen) und daher auch unabhängig von der Leistungspflicht des Anbieters der *Aziz*-Test mit hinreichender Wahrscheinlichkeit fehlschlägt.

(cc) Weite vertragliche Leistungspflichten

Besonders relevant ist die Inhaltskontrolle für weit gespannte Pflichten der datenschutzrechtlich Verantwortlichen, die zu einer Legitimierung der dafür er-

[781] EuGH, Urt. v. 14.3.2013 – Rs. C-415/11 (*Aziz*) – Rn. 73.
[782] Siehe oben, § 4 C.I.2.c)bb)(2).
[783] Zur unangemessenen Benachteiligung durch eine Klarnamenpflicht siehe LG Berlin, MMR 2018, 328 Rn. 63 f.; für die Rechtslage ab Geltungsbeginn der DS-GVO *Hacker*, ZfPW 2019, 148 (189 f.); zur Klauselkontrolle sonstiger, nicht unmittelbar datenbezogener Vertragsbedingungen im Online-Bereich siehe *Loos/Luzak*, 39 Journal of Consumer Policy 2016, 63 (65 ff.).
[784] Siehe oben, § 4 B.II.2.b)bb)(2).
[785] Siehe oben, § 4 B.I.3.b)(3)(a).

forderlichen Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO führen sollen (weite Leistungspflichten). Wie bereits mehrfach erörtert, könnte ein Verarbeiter sich gegenüber dem Nutzer verpflichten, personalisierte Werbung zu schalten, um dadurch die Zulässigkeit der darauf bezogenen Datenverarbeitung, auch unter Einsatz von Tracking-Tools,[786] zu erreichen.[787] In diesen Fällen erscheint eine vertragsrechtliche Kontrolle besonders wichtig, weil die durch die DS-GVO etablierten Schutzmechanismen für die Einwilligung nicht greifen.[788] Dies betrifft vor allem das Separierungsgebot, Art. 7 Abs. 2 S. 1 DS-GVO; die Widerruflichkeit der Einwilligung, Art. 7 Abs. 3 DS-GVO; sowie das Kopplungsverbot, Art. 7 Abs. 4 DS-GVO.[789] Da sich die Vertragsklausel jedoch hinsichtlich ihrer Legitimationswirkung als Einwilligungssubstitut darstellt, fällt dem Vertragsrecht die Aufgabe zu, auch geeignete Schutzsubstitute zu entwickeln. Die AGB-rechtliche Inhaltskontrolle erscheint aufgrund ihrer Wertungsoffenheit, aber auch ihrer klaren normativen Bezogenheit auf Grenzen der Privatautonomie prädestiniert für eine wirksame Kontrolle derartig weiter Leistungspflichten.[790]

Die Schwierigkeit liegt jedoch darin, einen Test zu entwickeln, der mit hinreichender Genauigkeit Klauseln, die primär der Umgehung der Einwilligungserfordernisse dienen, von solchen scheidet, die dem Nutzer genuine Vorteile in Form besonderer Leistungsversprechen verschaffen. Nur in ersterem Fall ist mit hinreichender Sicherheit davon auszugehen, dass der *Aziz*-Test fehlschlägt. Dafür sind nach hier vertretener Auffassung insgesamt drei Kriterien ausschlaggebend.[791] Erstens darf die Leistungspflicht mit der Hauptleistungspflicht des Anbieters in keinem funktionalen Zusammenhang stehen. Eine derartige Inkonnexität liegt etwa vor, wenn seitens des Anbieters eines sozialen Netzwerks personalisierte Werbung versprochen wird. Denn aus der für den *Aziz*-Test maßgeblichen Sicht des Vertragspartners des Verwenders liegt die primäre Leistung des Anbieters in diesem Fall typischerweise in der Eröffnung des Zugangs zum sozialen Netzwerk, nicht hingegen in der Möglichkeit, Werbung konsumieren zu können. Auch besteht zwischen beiden Leistungspflichten lediglich ein ökonomischer, nicht jedoch ein technisch-funktionaler Zusammenhang, da der Zugang ohne Weiteres auch ohne personalisierte Werbung verschafft werden kann.

Dieses Konnexitätserfordernis ist legitim, um funktional notwendige Leistungspflichten von solchen zu trennen, die darüber hinaus dem Leistungs-

---

[786] Zum Rückgriff auf Art. 6 Abs. 1 lit. b DS-GVO beim Einsatz von Tracking-Instrumenten siehe oben, § 4 B.I.4.b)bb).

[787] Siehe nur das Vorbringen von Facebook in Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 688 ff.

[788] *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3747).

[789] Hinzu kommt der partiell stärkere Schutz von Minderjährigen, siehe oben, § 4 B.I.3.b)cc).

[790] Siehe bereits oben, Text bei § 4, Fn. 546.

[791] Siehe bereits *Hacker*, ZfPW 2019, 148 (190 f.).

paket hinzugefügt werden. Es ist letztlich auch nicht denselben Einwänden ausgesetzt wie der objektive Erforderlichkeitsmaßstab im Rahmen von Art. 6 Abs. 1 lit. b, Art. 7 Abs. 4 DS-GVO.[792] Denn erstens wird nicht ein objektiver Hauptzweck des Vertrags postuliert, sondern konsequent subjektiv, allerdings aus der Sicht des Nutzers, die primäre Leistung des Anbieters bestimmt. Dies dürfte regelmäßig möglich sein[793] und entspricht dem Fokus des *Aziz*-Tests auf den Verständnis- und Entscheidungshorizont des Nutzers. Zweitens erscheint das wertende Moment der Trennung in Haupt- und Nebenleistungspflichten im Rahmen der Ausfüllung des genuin normativen Tatbestandsmerkmals der Unangemessenheit einer Benachteiligung, anders als bei Auslegung des funktionalen Kriteriums der Vertragserforderlichkeit, durchaus gerechtfertigt. Insbesondere ist diese Unterscheidung auch in Art. 4 Abs. 2 der Klauselrichtlinie angelegt („Hauptgegenstand des Vertrags").

Das zweite Kriterium für die Unangemessenheit einer weiten Leistungspflicht sollte der Umstand sein, dass diese Leistungspflicht für den Nutzer im Prinzip wertlos ist. Dies kann insbesondere dann angenommen werden, wenn die angebotene Leistung ohnehin dem Marktstandard entspricht. So liegt es etwa bei personalisierter Werbung im Bereich vieler Onlinedienste: Auch ohne eine eigene Verpflichtung personalisieren Suchmaschinen, Anbieter von sozialen Netzwerken oder sonstige Content-Provider Werbeanzeigen, sodass für den Nutzer durch eine dahingehende Verpflichtung nichts gewonnen ist. Ist hingegen für den Nutzer ein signifikanter Wert gerade mit der Pflicht des Anbieters zur Leistung verbunden, so kann nicht von einem Fehlschlagen des *Aziz*-Tests ausgegangen werden, auch wenn die Folge ist, dass bestimmte Datenverarbeitungsvorgänge dadurch erlaubt werden.

Drittens muss hinzukommen, dass durch die Verwendung der Klausel die oben genannten Schutzmechanismen der DS-GVO ausgehebelt werden, diese also nicht etwa vertraglich mit Bezug auf die Klausel dem Nutzer wieder eingeräumt werden.

Sind diese drei Bedingungen erfüllt, kann gefolgert werden, dass die Klausel nicht funktional notwendig ist, dem Nutzer keinen Mehrwert bietet, aber zugleich datenschutzrechtliche Schutzvorschriften unterläuft. Daher ist mit hinreichender Sicherheit anzunehmen, dass der informierte Nutzer bei individuellen Vertragsverhandlungen der Klausel – unabhängig von seinen Datenschutzpräferenzen – nicht zugestimmt hätte. Sie hält mithin dem *Aziz*-Test nicht stand und ist unwirksam nach § 307 Abs. 1 S. 1 BGB. Die Inhaltskontrolle reproduziert damit funktional die genannten Schutzmechanismen der DS-GVO, insbesondere das Kopplungsverbot nach Art. 7 Abs. 4 DS-GVO.[794] Sie

[792] Dazu oben, § 4 C.I.3.a)dd)(3)(bb)b.

[793] Zu allgemeinen Abgrenzungsschwierigkeiten zwischen Haupt- und Nebenleistungspflichten allerdings *Medicus/Petersen*, BGB AT, 11. Aufl. 2016, Rn. 206 ff.; *Bachmann*, in: MüKo, BGB, 8. Aufl. 2019, § 241 Rn. 29 f.

[794] *Hacker*, ZfPW 2019, 148 (191).

füllt insofern vertragsrechtlich die Lücke, die datenschutzrechtlich durch die Substituierung der Einwilligung durch die Vertragsklausel entsteht.

(2) Vertragliche Einbindung Dritter

Im Rahmen des dritten Leitfalls lässt sich schließlich fragen, inwiefern Klauseln, die eine Datenerhebung bei Nicht-Primärnutzern von IoT-Geräten ermöglichen, einer Inhaltskontrolle im engeren Sinne standhalten. Wie bereits gesehen, wird der Abschluss eines Vertrags mit Drittnutzern häufig bereits am Fehlen der im Rahmen der Rechtsgeschäftslehre notwendigen Voraussetzungen scheitern.[795] Ferner ist die Parteistellung solcher Drittanbieter, mit denen der Nutzer nicht rechnet, typischerweise überraschend im Sinne von § 305c Abs. 1 BGB.[796] Sofern nach Maßgabe dieser Regeln überhaupt ein Vertrag zustande kommt, ergeben sich für die Inhaltskontrolle letztlich keine Besonderheiten.

Was die Verpflichtung eines Anbieters gegenüber dem Drittnutzer anbelangt, so können die soeben diskutierten Kriterien für die Beurteilung der Unangemessenheit besonders weiter, die Datenverarbeitung legitimierender Pflichten Anwendung finden. Hinsichtlich der Pflichten des Nutzers wiederum gilt das soeben zur Verpflichtung der Abgabe einer Einwilligung und der Überlassung von Daten Gesagte.

dd) Erweiterung der §§ 308 f. BGB

Die Diskussion der Leitfälle hat gezeigt, dass zwar bei Anwendung der Kriterien der Unangemessenheit sachgerechte Ergebnisse erzielt werden können, diese jedoch noch mit erheblicher Rechtsunsicherheit behaftet sind. Wie bei Art. 6 Abs. 1 lit. f DS-GVO[797] erscheint es daher auch im AGB-rechtlichen Bereich sinnvoll, bestimmte Formen besonders unerwünschter Datenverarbeitung in die schwarze und graue Liste unangemessener Klauseln (§§ 308 f. BGB) aufzunehmen. Damit ließe sich die AGB-Kontrolle von Einwilligungserklärungen und Vertragsklauseln deutlich rechtsicherer und vorhersehbarer gestalten. Ein Kandidat für die Aufnahme in eine schwarze Liste wären weite Leistungspflichten unter den oben genannten Bedingungen.

f) Rechtsfolgen: Das Schicksal des Vertrags

Eine unangemessene Benachteiligung durch datenschutzrechtlich relevante AGB kommt mithin in drei Fällen in Betracht: erstens bei einem Verstoß gegen datenschutzrechtliche Vorschriften, besonders bei der Einwilligung; zweitens ausnahmsweise bei einer isoliert exzessiven Pflicht zur Datenüberlassung; sowie drittens bei weiten, inkonnexen Nebenleistungspflichten.

---

795 Siehe oben, § 4 A.I.1.b.bb)(2).
796 Siehe oben, § 4 A.II.2.a)cc)(2)(b).
797 Siehe oben, Text bei § 4, Fn. 1038.

Nicht ohne Weiteres evident sind in diesen Fällen jedoch die Rechtsfolgen der unangemessenen Benachteiligung. Klar ist insoweit lediglich, dass gemäß § 307 Abs. 1 S. 1 BGB die betreffliche Klausel unwirksam ist. Schon grundsätzlich umstritten ist im AGB-Recht jedoch das Schicksal des Vertrags im Übrigen. Art. 6 Abs. 1 der Klauselrichtlinie gibt dazu vor, dass „der Vertrag für beide Parteien […] bindend bleibt, wenn er ohne die mißbräuchlichen Klauseln bestehen kann." Dies ist im deutschen Recht mit signifikanten Differenzen in § 306 BGB umgesetzt, der drei Stufen des Umgangs mit dem Vertrag unterscheidet. Nach dem ersten Absatz bleibt der Vertrag, in Abkehr von der Regelung des § 139 BGB, grundsätzlich wirksam. Sein Inhalt bestimmt sich, soweit Klauseln nicht Vertragsbestandteil geworden oder unwirksam sind, durch gesetzliche Vorschriften, § 306 Abs. 2 BGB. Der Vertrag ist jedoch nach § 306 Abs. 3 BGB insgesamt unwirksam, wenn auch unter Berücksichtigung einer Änderung nach dem zweiten Absatz das Festhalten am Vertrag eine unzumutbare Härte für eine der Parteien darstellen würde.

Damit stellen sich insgesamt zwei Fragen hinsichtlich der Rechtsfolgen der AGB-Kontrolle, die auch für datenbasierte Austauschprozesse unmittelbar relevant sind: Inwieweit kann eine an sich unwirksame Klausel durch inhaltliche Revision oder selektive Streichung einzelner Teile vor der Unwirksamkeit bewahrt werden? Und welches Schicksal ist dem Vertrag im Übrigen bestimmt?

aa) Deutsche Rechtsprechung und Literatur zu § 306 BGB

In der deutschen Rechtsprechung und Literatur wird die geltungserhaltende Reduktion einer unwirksamen Klausel gemeinhin als mit dem Schutzzweck der AGB-Kontrolle unvereinbar abgelehnt,[798] da der Verwender andernfalls keinen Anreiz hätte, auf unangemessene Klauseln zu verzichten. Allerdings hält die herrschende Meinung inklusive des BGH die Streichung einzelner Teile einer Klausel, welche die Unwirksamkeit herbeiführen, für möglich (*blue pencil test*).[799]

Ist eine Klausel hingegen nicht Vertragsbestandteil geworden oder unwirksam, so ist nach dem BGH zur Lückenfüllung primär das dispositive Recht und nur subsidiär die ergänzende Vertragsauslegung berufen,[800] die als im Gesetz nach §§ 133, 157 BGB angelegte Regelung nach herrschender Meinung auch von

[798] BGH NJW 2000, 1110 (1113 f.); *Fornasier*, Freier Markt und zwingendes Vertragsrecht, 2013, 184 f.; *Fuchs*, in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016, Vorbemerkungen zur Inhaltskontrolle Rn. 99; *Schlosser*, in: Staudinger, BGB, 2013, § 306 Rn. 22.

[799] BGH NJW 2015, 928 Rn. 23 f.; BGH NJW 2014, 141 Rn. 14; *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 306 Rn. 22 f.; *Schlosser*, in: Staudinger, BGB, 2013, § 306 Rn. 20; kritisch *Thüsing*, BB 2006, 661 (662); *Stürner*, ZEuP 2013, 666 (680); *Rott*, in: Twigg-Flesner (Hrsg.), Research Handbook on EU Consumer and Contract Law, 287 (303); *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 306 Rn. 10.

[800] BGH NJW 2000, 1110 (1114); BGH NJW 2002, 3098 (3099); *Thomas*, AcP 209 (2009), 84 (122 f.); *Schmidt*, in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016, § 306 BGB Rn. 34; *Ulmer*, NJW 1981, 2025 (2031).

§ 306 Abs. 2 BGB umfasst ist.[801] Allerdings darf diese nicht zu einer geltungserhaltenden Reduktion durch die Hintertür führen.[802]

bb) Die Rechtsprechung des EuGH

Diese Grundsätze sind mit der Rechtsprechung des EuGH zu Art. 6 Abs. 1 der Klauselrichtlinie jedoch, entgegen den Beteuerungen des BGH,[803] in großen Teilen nicht vereinbar.[804] Der Gerichtshof stellt nunmehr, deutlich stärker als der auf einen Interessenausgleich bedachte BGH,[805] den Schutz des Verbrauchers in den Vordergrund.[806]

(1) Geltungserhaltende Reduktion und selektive Streichung der Klausel

So hat der EuGH geurteilt, dass missbräuchliche Klauseln durch das nationale Gericht nicht inhaltlich abgeändert und insbesondere nicht auf das gerade noch gesetzlich zulässige Maß zurückgeschnitten werden dürfen.[807] Vielmehr muss der Vertrag jenseits der betroffenen Klausel, soweit nach nationalem Recht möglich, unverändert fortbestehen.[808] Daher darf beispielsweise eine unangemessene Vertragsstrafe nicht auf ein zulässiges Maß reduziert werden, sondern muss gänzlich unangewendet bleiben.[809]

---

[801] Grundlegend BGH NJW 1984, 1177 (1178); BT-Drucks. 7/5422, 5; *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 306 Rn. 31, 36 f.; *Schlosser*, in: Staudinger, BGB, 2013, § 306 Rn. 12; *Thomas*, AcP 209 (2009), 84 (121); *Thüsing*, VersR 2015, 927 (929); zum Streit um die Zulässigkeit nach deutschem Recht ausführlich *Schmidt*, in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016, § 306 BGB Rn. 33 ff.

[802] *Fuchs*, in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016, Vorbemerkungen zur Inhaltskontrolle Rn. 99a; *Thüsing*, VersR 2015, 927 (930); *Rott*, in: Twigg-Flesner (Hrsg.), Research Handbook on EU Consumer and Contract Law, 287 (303); *Fastrich*, Richterliche Inhaltskontrolle im Privatrecht, 1992, 337.

[803] BGH NJW 2017, 320 Rn. 23 ff.

[804] *Graf von Westphalen*, BB 2019, 67 (71 ff.); *Graf von Westphalen*, MDR 2019, 76 (81 ff.).

[805] BGH NJW 1998, 450 (451); BGH NJW 2002, 3098 (3099); BGH NJW 2017, 320 Rn. 29; *Thomas*, AcP 209 (2009), 84 (122, 127).

[806] Siehe etwa EuGH, Urt. v. 31.5.2018 – Rs. C-483/16 (*Sziber*) – Rn. 34 zum Ziel der „Wiederherstellung der Sach- und Rechtslage, in der sich der Verbraucher ohne die missbräuchliche Klausel befände"; ferner auch *Keirsbilck*, 50 Common Market Law Review 2013, 247 (259).

[807] EuGH, Urt. v. 7.11.2019 – verb. Rs. C-349/18 bis C-351/18 (*NMBS*) – Rn. 67–69; Urt. v. 26.3.2019 – verb. Rs. C-70/17 und C-179/17 (*Abanca Corporación Bancaria*) – Rn. 53; Urt. v. 7.8.2018 – verb. Rs. C-96/16 und C-94/17 (*Banco Santander*) – Rn. 73; Urt. v. 21.1.2015 – verb. Rs. C-482/13, C-484/13, C-485/13 und C-487/13 (*Unicaja Banco und Caixabank*) – Rn. 28; Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 77; Urt. v. 30.5.2013 – Rs. C-488/11 (*Asbeek Brusse*) – Rn. 57; Urt. v. 14.6.2012 – Rs. C-618/10 (*Banco Español de Crédito*) – Rn. 71.

[808] Siehe die Nachweise in § 5, Fn. 807.

[809] EuGH, Urt. v. 21.1.2015 – verb. Rs. C-482/13, C-484/13, C-485/13 und C-487/13 (*Unicaja Banco und Caixabank*) – Rn. 29; Urt. v. 30.5.2013 – Rs. C-488/11 (*Asbeek Brusse*) – Rn. 59.

Zur Begründung verweist der EuGH neben dem Wortlaut des Art. 6 Abs. 1[810] auf das in Art. 7 Abs. 1 und dem 24. Erwägungsgrund der Klauselrichtlinie artikulierte Ziel, der Verwendung von missbräuchlichen Klauseln ein Ende zu setzen.[811] Der dies befördernde und mit der Unwirksamkeit intendierte Abschreckungseffekt träte jedoch, wofür in der Tat alles spricht, nicht ein, wenn der Vertrag so abgeändert würde, dass das Interesse des Verwenders weitestmöglich gewahrt wird.[812] Diese Erwägung schiebt jedoch nicht nur der geltungserhaltenden Reduktion einen Riegel vor. In der Rechtssache *Abanca Corporación Bancaria* hat der EuGH vielmehr ausdrücklich entschieden, dass auch die Streichung einzelner Teile einer Klausel nicht zulässig ist, da auch insofern die Präventionswirkung Schaden nimmt.[813] Die Vereinbarkeit dieser Praxis mit den Vorgaben der Richtlinie war bereits zuvor auf Bedenken gestoßen.[814] In der Tat ist nicht ersichtlich, warum syntaktische Differenzen (streichbare Bestandteile oder nicht) bei identischem Inhalt von Klauseln auf die Rechtsfolge einen Einfluss haben sollen.[815] Die deutsche Rechtsprechung wird die Anwendung des *blue pencil test* daher, jedenfalls bei erkennbar einheitlicher Regelung innerhalb der an sich durch Streichung trennbaren Klausel,[816] aufgeben müssen.

(2) Gesamtunwirksamkeit des Vertrags

Die Nichteinbeziehung oder Unwirksamkeit einer Klausel hat die Gesamtunwirksamkeit des Vertrags nach dem EuGH, anders als in § 306 Abs. 3 BGB vorgesehen, nur zur Folge, wenn dieser objektiv-rechtlich nicht aufrechterhal-

---

[810] EuGH, Urt. v. 14.6.2012 – Rs. C-618/10 (*Banco Español de Crédito*) – Rn. 65.

[811] EuGH, Urt. v. 7.11.2019 – verb. Rs. C-349/18 bis C-351/18 (*NMBS*) – Rn. 69; Urt. v. 26.3.2019 – verb. Rs. C-70/17 und C-179/17 (*Abanca Corporación Bancaria*) – Rn. 54; Urt. v. 21.1.2015 – verb. Rs. C-482/13, C-484/13, C-485/13 und C-487/13 (*Unicaja Banco und Caixabank*) – Rn. 30; Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 78; Urt. v. 30.5.2013 – Rs. C-488/11 (*Asbeek Brusse*) – Rn. 58; Urt. v. 14.6.2012 – Rs. C-618/10 (*Banco Español de Crédito*) – Rn. 68 f.

[812] EuGH, Urt. v. 7.11.2019 – verb. Rs. C-349/18 bis C-351/18 (*NMBS*) – Rn. 69; Urt. v. 26.3.2019 – verb. Rs. C-70/17 und C-179/17 (*Abanca Corporación Bancaria*) – Rn. 54; Urt. v. 21.1.2015 – verb. Rs. C-482/13, C-484/13, C-485/13 und C-487/13 (*Unicaja Banco und Caixabank*) – Rn. 31; Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 79; Urt. v. 14.6.2012 – Rs. C-618/10 (*Banco Español de Crédito*) – Rn. 69; zum Abschreckungseffekt auch EuGH, Beschl. v. 16.11.2010 – Rs. C-76/10 (*Pohotovost'*) – Rn. 41; zur Präventionsfunktion des AGB-Rechts generell *Fornasier*, Freier Markt und zwingendes Vertragsrecht, 2013, 182 ff.; *Thüsing*, VersR 2015, 927 (930 f.); *Graf von Westphalen*, BB 2019, 67 (67 f.); *Rott*, in: Twigg-Flesner (Hrsg.), Research Handbook on EU Consumer and Contract Law, 287 (303).

[813] EuGH, Urt. v. 26.3.2019 – verb. Rs. C-70/17 und C-179/17 (*Abanca Corporación Bancaria*) – Rn. 53 mit 64.

[814] *Stürner*, ZEuP 2013, 666 (680); *Rott*, in: Twigg-Flesner (Hrsg.), Research Handbook on EU Consumer and Contract Law, 287 (303); *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 306 Rn. 10.

[815] *Thüsing*, BB 2006, 661 (662); *Fastrich*, Richterliche Inhaltskontrolle im Privatrecht, 1992, 337.

[816] Vgl. *Thüsing*, BB 2006, 661 (663).

ten werden kann.[817] Irrelevant ist dabei aus unionsrechtlicher Perspektive, ob die Gesamtunwirksamkeit für den Verbraucher günstiger wäre als die Aufrechterhaltung des Vertrags ohne die beanstandete Klausel.[818] Denn dadurch würde, so der EuGH, die Rechtssicherheit über Gebühr strapaziert.[819] Da die Richtlinie jedoch nur eine Mindestharmonisierung vorgibt, kann das nationale Recht eine Gesamtunwirksamkeit des Vertrags vorsehen, wenn der Verbraucher dadurch besser geschützt wird.[820] Demnach muss § 306 Abs. 3 BGB in richtlinienkonformer Anwendung für die Unwirksamkeit von Vertragsklauseln, die gegenüber einem Verbraucher Verwendung finden werden, auf Härtefälle zulasten des Verbrauchers reduziert werden.[821]

(3) Vertragliche Lückenfüllung

Auch hinsichtlich der Lückenfüllung setzt der EuGH nunmehr neue Maßstäbe. Zwar ist auch nach seiner Rechtsprechung eine Ersetzung einer Klausel durch dispositives Recht möglich. Nach der Formulierung der älteren Rechtsprechung des EuGH bis 2014 sollte dies grundsätzlich mit dem Ziel erfolgen, „die formale Ausgewogenheit der Rechte und Pflichten der Vertragsparteien durch eine materielle Ausgewogenheit zu ersetzen und so deren Gleichheit wiederherzustellen."[822] Dies passte gut zu einer vorbehaltslosen Anwendung

[817] EuGH, Urt. v. 30.5.2013 – Rs. 397/11 (*Jőrös*) – Rn. 47; Urt. v. 15.3.2012 – Rs. C-453/10 (*Pereničová und Perenič*) – Rn. 32.

[818] EuGH, Urt. v. 15.3.2012 – Rs. C-453/10 (*Pereničová und Perenič*) – Rn. 32 f.

[819] EuGH, Urt. v. 30.5.2013 – Rs. 397/11 (*Jőrös*) – Rn. 47; Urt. v. 15.3.2012 – Rs. C-453/10 (*Pereničová und Perenič*) – Rn. 32.

[820] EuGH, Urt. v. 30.5.2013 – Rs. 397/11 (*Jőrös*) – Rn. 47; Urt. v. 15.3.2012 – Rs. C-453/10 (*Pereničová und Perenič*) – Rn. 34 f.

[821] So auch *Hennigs*, GRUR 2012, 641 (642); weitergehend *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 306 Rn. 6 f., der eine individuelle Härte, entgegen den Nachweisen in der vorangegangenen Fußnote, überhaupt nicht berücksichtigen will und daher § 306 Abs. 3 BGB insgesamt für richtlinienwidrig hält; ähnlich *Schmidt*, in: Ulmer/Brandner/Hensen, AGB-Recht, 12. Aufl. 2016, § 306 BGB Rn. 4e, der einen Anwendungsbereich für die verwenderbezogene Härte erhalten möchte, aber übersieht, dass dieser im überschießenden Bereich gegeben ist (siehe dazu grundsätzlich *Herresthal*, Rechtsfortbildung im europarechtlichen Bezugsrahmen, 2006, 323); wohl ebenso *Graf von Westphalen*, BB 2019, 67 (74); eine richtlinienkonforme Auslegung halten hingegen auch *Heinrichs*, NJW 1996, 2190 (2195); *Werkmeister*, EuZW 2012, 303 (304); *Graf von Westphalen*, NJW 2012, 1770 (1772 f.) für möglich und ausreichend. Im überschießenden Bereich hingegen ist wegen der grundsätzlich differenten Wertungsgesichtspunkte (kein Schutz von Verbraucherinteressen) die Unzumutbarkeit für den Verwender zu berücksichtigen, die Norm damit insgesamt gespalten auszulegen; zur Zulässigkeit der gespaltetenen Auslegung wegen abweichender Wertungsgesichtspunkte außerhalb des Verbraucherrechts ausführlich *Habersack/Mayer*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 297 (319 Rn. 46); siehe auch BGH NJW 2017, 1596 Rn. 27 ff.

[822] EuGH, Urt. v. 15.3.2012 – Rs. C-453/10 (*Pereničová und Perenič*) – Rn. 28; so auch zuvor bereits EuGH, Urt. v. 26.10.2006 – Rs. C-168/05 (*Mostaza Claro*) – Rn. 36; Urt. v. 4.6.2009 – Rs. C-243/08 (*Pannon GSM*) – Rn. 31; Urt. v. 6.10.2009 – Rs. C-40/08 (*Asturcom Telecomunicaciones*) – Rn. 30; Urt. v. 9.11.2010 – Rs. C-137/08 (*VB Pénzügyi Lízing*) – Rn. 47; ferner Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 82; Urt. v. 14.6.2012 – Rs. C-618/10

von dispositiven Gesetzesnormen oder der an einem beiderseitigen Interessenausgleich orientierten ergänzenden Vertragsauslegung.[823]

Von diesem Versuch, durch dispositives Recht oder ergänzende Vertragsauslegung eine Balance zwischen den Vertragsparteien unter Berücksichtigung beiderseitiger Interessen herzustellen, hat sich der EuGH in der Folge jedoch mit den Urteilen in den Rechtssachen *Unicaja Banco und Caixabank*, *Banco Santander* und *Abanca Corporación Bancaria* schroff abgewandt. Maßstab sind fürderhin allein das Wohl und der Schutz des Verbrauchers, um eine maximale Abschreckungswirkung zu erzielen.[824] Daher ist der Rückgriff auf dispositives Recht, und a fortiori auf ergänzende Vertragsauslegung, nur noch unter der doppelten Prämisse gestattet, dass der Vertrag (i) sonst *in toto* unwirksam wäre und (ii) der Verbraucher infolgedessen geschädigt[825] bzw. bestraft[826] würde.[827] Insbesondere kann daher auch eine unwirksame Darlehenszinsklausel (konkret betreffend Verzugszinsen) ersatzlos gestrichen werden, ohne dass sie durch nach dispositivem Recht geschuldete Verzugszinsen ersetzt wird.[828] Der Ersetzung einer nicht einbezogenen oder unwirksamen Klausel durch dispositives Recht und ergänzende Vertragsauslegung werden daher äußerst enge Grenzen gezogen, die bei Verbraucherverträgen in richtlinienkonformer Auslegung von § 306 Abs. 2 BGB berücksichtigt werden müssen:[829] Beide Ersetzungsmechanismen kommen nur in Betracht, sofern der Verbraucher andernfalls erheblich benachteiligt würde; und auch dann muss der Abschreckungseffekt im Einzelfall erhalten bleiben.[830] Wie sogleich zu zeigen sein wird, passen diese Erwägungen jedoch nicht auf den Wegfall von Hauptleistungspflichten bei datenbasierter Gegenleistung.

cc) Lösungen für das Datenprivatrecht

Die Vorgaben des EuGH müssen daher berücksichtig werden, um Lösungen zu schaffen für die teilweise atypischen Konstellationen, in denen in daten-

(*Banco Español de Crédito*) – Rn. 40; zuletzt auch Urt. v. 31.5.2018 – Rs. C-483/16 (*Sziber*) – Rn. 32, dort aber bereits relativiert durch die unmittelbare Bezugnahme auf das Abschreckungserfordernis, ebd. Rn. 33; siehe *Graf von Westphalen*, MDR 2019, 76 (79).

[823] Insoweit zutreffend BGH NJW 2017, 320 Rn. 23 ff.

[824] *Graf von Westphalen*, BB 2019, 67 (72).

[825] EuGH, Urt. v. 26.3.2019 – verb. Rs. C-70/17 und C-179/17 (*Abanca Corporación Bancaria*) – Rn. 56; Urt. v. 30.4.2014 – Rs. C-26/13 (*Kásler*) – Rn. 80–84.

[826] EuGH, Urt. v. 7.11.2019 – verb. Rs. C-349/18 bis C-351/18 (*NMBS*) – Rn. 70; Urt. v. 7.8.2018 – verb. Rs. C-96/16 und C-94/17 (*Banco Santander*) – Rn. 74; Urt. v. 21.1.2015 – verb. Rs. C-482/13, C-484/13, C-485/13 und C-487/13 (*Unicaja Banco und Caixabank*) – Rn. 33 (in der spanischen Verfahrenssprache: *penalización*).

[827] Siehe auch *Graf von Westphalen*, BB 2019, 67 (69) („doppelstufige Prüfung").

[828] EuGH, Urt. v. 7.8.2018 – verb. Rs. C-96/16 und C-94/17 (*Banco Santander*) – Rn. 78 f.

[829] Für die Notwendigkeit eines Einschreitens des Gesetzgebers hingegen *Graf von Westphalen*, BB 2019, 67 (74); es gilt jedoch das zu § 306 Abs. 3 BGB Gesagte entsprechend, siehe § 5, Fn. 821.

[830] *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 306 Rn. 9.

schutzrechtlich relevanten Kontexten Vertragsklauseln oder Einwilligungserklärungen AGB-rechtlich unwirksam sind.

(1) Unwirksame Einwilligung

Eine unwirksame Einwilligung kann nicht entsprechend den Regeln zu ergänzender Vertragsauslegung – unabhängig von der Diskussion um ihre Anwendbarkeit – teilweise aufrechterhalten werden.[831] Denn dies widerspräche klar nicht nur dem Gebot der Unmissverständlichkeit, sondern auch der Bestimmtheit und Informiertheit der Einwilligung, die in Art. 4 Nr. 11 DS-GVO niedergelegt sind. Insofern kommt der DS-GVO vor den durch die Klauselrichtlinie ermöglichten Ergänzungsmechanismen sachintegrativer Vorrang zu. Der Schutzstandard der DS-GVO darf nicht durch das AGB-Recht unterminiert werden.[832]

Von einem die Einwilligung begleitenden Vertrag ist die Einwilligung dogmatisch ohnehin strikt zu trennen. Allerdings kann nach dem bereits Erörterten die Wirksamkeit der Einwilligung eine Geschäftsgrundlage nach § 313 BGB darstellen, wenn der Verwender einen Anspruch auf Erteilung der Einwilligung in den Vertrag aufgenommen hat.[833] In diesen Fällen ist die Abweichung vom Rechtsgedanken des § 306 Abs. 1 BGB dadurch gerechtfertigt, dass, anders als bei sonstigen AGB, mit der Einwilligung der Kern des Vertrages betroffen sein kann[834] und zusätzlich der Effektivitätsgrundsatz des Unionsrechts, wie oben bereits erörtert,[835] nicht betroffen ist, da die Abschreckungswirkung bei infolge der Unwirksamkeit der Einwilligung datenschutzwidriger Verarbeitung durch das Sanktionsinstrumentarium der DS-GVO hinreichend sichergestellt ist.

(2) Unwirksame Hauptleistungspflicht

Besonders schwierig stellt sich der Umgang mit der, allerdings äußerst seltenen, AGB-rechtlichen Unwirksamkeit einer vertraglichen Hauptleistungspflicht dar. Die einzige im hiesigen Kontext denkbare Konstellation ist die Verpflichtung zur isoliert exzessiven Datenüberlassung.[836]

Hier ist zunächst die Gesamtunwirksamkeit des Vertrags gemäß § 306 Abs. 3 BGB zu erwägen. Denn, so könnte man argumentieren, für den Anbieter würde der isolierte Wegfall der Gegenleistungspflicht zu einer unzumutbaren Härte führen, da er dann seine Leistung zu erbringen hätte, ohne vom Vertragspartner kompensiert zu werden. Allerdings ist § 306 Abs. 3 BGB,

831 Im Ergebnis ebenso *Langhanke*, Daten als Leistung, 2018, 218.
832 *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3748).
833 Siehe oben, Text bei § 5, Fn. 534.
834 *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 306 Rn. 2.
835 Siehe oben, Text bei § 5, Fn. 546.
836 Siehe oben, § 5 C.II.1.e)cc)(b)(bb).

wie gesehen, in richtlinienkonformer Anwendung bei Verbraucherverträgen grundsätzlich nicht zugunsten des Verwenders anwendbar.

Infolgedessen ließe sich argumentieren, dass auch bei Unwirksamkeit der Gegenleistungspflicht des Nutzers der Vertrag im Übrigen, und somit auch die Leistungspflicht des Anbieters, erhalten werden müsse. Eine Gesamtunwirksamkeit erscheint jedenfalls nicht von vornherein objektiv nach deutschem Recht erforderlich, wie es die Rechtsprechung des EuGH fordert: Einseitig verpflichtende Verträge ohne Gegenleistung kennt die deutsche Rechtsordnung ohne Weiteres.[837]

Allerdings kommen solche Verträge nur wirksam zustande, wenn die einseitige Verpflichtung von beiden Seiten, insbesondere der verpflichteten Partei, so gewollt ist. Davon kann jedoch im Falle der Unwirksamkeit der Gegenleistungspflicht keine Rede sein. Zwar ist die Rechtsfolge der Unwirksamkeit einer Hauptleistungspflicht im deutschen Recht nicht ausdrücklich geregelt. Aus einer Gesamtschau verschiedener Regelungen ergibt sich jedoch, dass die Rechtsfolge grundsätzlich die Unwirksamkeit der korrespondierenden Hauptleistungspflicht und damit die Gesamtnichtigkeit des Vertrags sein muss. So ist anerkannt, dass ein Vertrag bei einem offenen oder versteckten Dissens über ein *essentialium negotii* schon gar nicht zustande kommt,[838] insbesondere auch bei nicht bestimmbarer Vergütungspflicht.[839] Ferner zeigt auch der Blick auf § 326 Abs. 1 S. 1 BGB, dass der Wegfall einer synallagmatischen Leistungspflicht grundsätzlich den Ausschluss der korrespondierenden Gegenleistungspflicht nach sich zieht. Eine halbseitige Teilnichtigkeit ist gesetzlich gerade nicht vorgesehen;[840] wenn überhaupt, so ist § 306 Abs. 3 BGB für die AGB-Kontrolle gerade das Gegenteil zu entnehmen. Auch für § 306 Abs. 1 BGB ist anerkannt, dass die Regel der Aufrechterhaltung des Vertrags im Übrigen voraussetzt, dass nicht der Vertragskern betroffen ist.[841] Die Gesamtunwirksamkeit des Vertrags folgt daher nach deutschem Recht bereits objektiv-rechtlich aus der Unwirksamkeit der Hauptleistungspflicht. Sie steht jedoch auch mit dem Effektivitätsgrundsatz des Unionsrechts im Einklang und ist die interessengerechte Lösung.

Zunächst ist nicht ersichtlich, dass eine Aufrechterhaltung der Leistungspflicht des Anbieters eine signifikante Abschreckungswirkung generieren würde. Daher fruchtet das Argument des EuGH nicht, dass Art. 7 Abs. 1 der Klauselrichtlinie die Aufrechterhaltung des Vertrags zulasten des Verwenders erfordert. Denn die Missbräuchlichkeit der Gegenleistungsklausel

---

[837] Siehe nur *Emmerich*, in: MüKo, BGB, 8. Aufl. 2019, Vor § 320 Rn. 2.

[838] *Zimmermann*, Richterliches Moderationsrecht oder Totalnichtigkeit?, 1979, 81; *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 155 Rn. 2; *Eckert*, in: BeckOK BGB, 51. Ed. 2019, § 154 Rn. 5; vgl. auch BGH NJW 2013, 598 Rn. 20 f.; BGH NJW 2006, 2843 Rn. 13.

[839] BGH NJW 1997, 2671 (2672); *Zimmermann*, Richterliches Moderationsrecht oder Totalnichtigkeit?, 1979, 81; *Busche*, in: MüKo, BGB, 8. Aufl. 2018, § 154 Rn. 3.

[840] Dazu oben, § 5 C.I.1.c)aa).

[841] *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 306 Rn. 2.

hat, wie bereits angedeutet und zugleich noch im Einzelnen nachzuweisen, regelmäßig zur Folge, dass die Verarbeitung der infolge der Klausel überlassenen Daten gegen die DS-GVO verstößt.[842] Dann jedoch greift, wie auch bei Unwirksamkeit der Einwilligungserklärung, das volle Sanktionsinstrumentarium der DS-GVO. Es ist nicht erkennbar, dass die Aufrechterhaltung des Vertrags im Übrigen signifikante zusätzliche Anreize für eine Vermeidung missbräuchlicher Klauseln über die Gegenleistung setzen würde. Denn nicht nur fallen die Kosten der Vertragserfüllung für den Anbieter neben den Sanktionen des Datenschutzrechts regelmäßig praktisch nicht ins Gewicht;[843] vielmehr ist eine Klausel, die auf Überlassung von Daten gerichtet ist, deren Verarbeitung durch die DS-GVO untersagt ist, für den Verwender überflüssig und generiert lediglich negative Reputationseffekte. Aufgrund des öffentlichen Durchsetzungsmechanismus der DS-GVO, aber auch der Klagebefugnis nach §§ 1, 2 Abs. 2 Nr. 11, 3 UKlaG kann er auch nicht darauf vertrauen, der Nutzer werde die Klausel schon „schlucken". Daher bestehen bereits signifikante Anreize, derartige Klauseln nicht zu verwenden. Diese Anreize würden durch eine einseitige Aufrechterhaltung des Vertrags nicht in erheblicher Weise gesteigert. Der Effektivitätsgrundsatz des Unionsrechts kann daher die einseitige Aufrechterhaltung im datenprivatrechtlichen Kontext nicht verlangen.

Eine Gesamtunwirksamkeit ist daher objektiv-rechtlich nach deutschem Recht erforderlich und mit Unionsrecht vereinbar. Sie ist jedoch auch interessengerecht, sodass eine ergänzende Vertragsauslegung zugunsten des Verbrauchers ebenfalls nicht in Betracht kommt. Dieser wird dadurch nicht etwa geschädigt oder bestraft, was nach dem EuGH, wie gesehen, Voraussetzung für eine Anwendung der ergänzenden Vertragsauslegung wäre. Vielmehr kann der Nutzer nicht erwarten, in den Genuss der Leistung des Anbieters zu gelangen, wenn dieser von ihm selbst keine Gegenleistung erhält.[844] Zwar steht es dem Anbieter frei, von einer anderen Marktseite auch ohne Datenüberlassung ein Entgelt für seine Leistung zu erwirtschaften, etwa durch die Schaltung von nicht personalisierter Werbung. Jedoch hatte sich der Anbieter gerade dafür entschieden, die Leistung nicht lediglich durch nicht personalisierte Werbung zu finanzieren, die regelmäßig deutlich weniger Einnahmen generiert.[845] Etwaige Aufwendungen, welche der Verbraucher im Vertrauen auf den Erhalt der Leistung getätigt hat, können über die bei schuldhafter Verwendung von unwirksamen AGB einschlägige *culpa in contrahendo* ersetzt werden,[846] so-

[842] Siehe unten, § 5 C.II.1.g).

[843] Siehe oben, Text bei § 5, Fn. 545.

[844] Vgl. *Metzger*, AcP 216 (2016), 817 (835).

[845] *Arning/Moos*, ZD 2014, 242 (243); *Hacker/Petkova*, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1 (23).

[846] BGH NJW 2009, 2590; BGH NJW 1988, 197 (198); BGH NJW 1984, 2816 (2817); OLG Köln NJW-RR 1995, 1333 (1334); *Graf von Westphalen*, NJW 2012, 2243 (2244); *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 306 Rn. 49; siehe auch unten, § 5 C.III.3.

dass der Verbraucher auch insoweit geschützt ist. Einem Wertersatzanspruch des Anbieters aus ungerechtfertigter Bereicherung steht, sofern es bereits zu einem Leistungsaustausch gekommen ist, der Effektivitätsgrundsatz des Unionsrechts entgegen.[847] Lediglich das positive Interesse des Verbrauchers am Erhalt der Leistung ist daher nicht geschützt.[848] Dies erscheint jedoch nicht als hinreichende Schädigung oder Strafe im Sinne der Rechtsprechung des EuGH, um eine dahingehende ergänzende Vertragsauslegung vornehmen zu können. Denn insofern greift wiederum der Gedanke, dass der Nutzer mit der Leistung des Anbieters insoweit nicht rechnen darf, als er selbst keine Gegenleistung erbringen muss.

Anders stellt sich die Sachlage nur dann dar, wenn der Nutzer bereits mit seinen Daten in Vorleistung gegangen ist und die Leistung des Anbieters noch nicht erhalten hat. In diesen Fällen würde eine Gesamtunwirksamkeit in der Tat eine Bestrafung des Verbrauchers darstellen, da sich die datenschutzrechtlichen Risiken bereits verwirklicht haben, ohne dass der Nutzer dafür kompensiert worden wäre. Ein Beispiel ist die Feststellung der Unwirksamkeit der Datenüberlassung für eine Rabattklausel, bevor der Rabatt gewährt wurde, aber nachdem der Kunde bereits signifikante Daten überlassen hat. In diesem Fall muss eine ergänzende Vertragsauslegung vorgenommen werden, die dem Nutzer einen Rabatt zubilligt, der in einem interessengerechten Verhältnis zu den tatsächlich überlassenen Daten steht.[849]

Insgesamt kann der Vertrag bei Unwirksamkeit der Gegenleistungspflicht daher nicht ohne die missbräuchliche Klausel bestehen, wie Art. 6 Abs. 1 der Klauselrichtlinie formuliert. *Pro futuro* bestehen daher keine Leistungspflichten. Eine Rückabwicklung zulasten des Verbrauchers ist jedoch durch den Effektivitätsgrundsatz des Unionsrechts gesperrt. Eine ergänzende Vertragsauslegung zugunsten des Verbrauchers kommt nur in Betracht, wenn dieser mit seinen Daten in Vorleistung gegangen ist.

(3) Unwirksame weite Nebenleistungspflicht

Hinsichtlich weiter, inkonnexer Nebenleistungspflichten dürfte gelten, dass diese bei Unwirksamkeit ersatzlos entfallen. Denn der Vertrag kann im Übrigen ohne Weiteres nach § 306 Abs. 1 BGB aufrechterhalten werden. Für eine ergänzende Vertragsauslegung ist daher nach dem EuGH kein Raum. Danach besteht jedoch auch kein Bedürfnis, da die Klausel ohnehin nur die Funktion hat, die datenschutzrechtliche Legitimierungswirkung herbeizuführen, die ihr jedoch gerade, sofern sie unwirksam ist, versagt werden soll.

---

[847] Siehe oben, Text bei § 5, Fn. 550.

[848] BGH NZM 2011, 478 Rn. 2; *Graf von Westphalen*, NJW 2012, 2243 (2244); *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 306 Rn. 49.

[849] Vgl. auch *Rudkowski*, ZVersWiss 2017, 453 (472); *Klimke*, r + s 2015, 217 (219 f.); *Hacker*, ZfPW 2019, 148 (192).

g) Wechselwirkungen mit der DS-GVO

Die AGB-rechtliche Unwirksamkeit oder Nichteinbeziehung einer Vertragsklausel oder Einwilligungserklärung hat demnach grundsätzlich zur Folge, dass die Klausel oder Erklärung ersatzlos wegfällt. Damit stellt sich in einem letzten Schritt noch die Frage nach den datenschutzrechtlichen Konsequenzen dieses Befundes. Eine enge Verbundenheit zwischen der DS-GVO und den Wertungen der Klauselrichtlinie ist durch den Verweis auf letztere im 42. Erwägungsgrund der DS-GVO bereits angelegt. Im Einzelnen muss jedoch erörtert werden, (aa)) welche Folgen für die privatautonomen Grundlagen der Datenverarbeitung in Art. 6 Abs. 1 lit. a und b DS-GVO sowie (bb)) für die Interessenabwägungsklausel in Art. 6 Abs. 1 lit. f DS-GVO bestehen. Ferner ist für ein integriertes Marktordnungsrecht entscheidend, ob die Missbräuchlichkeit einer Klausel nach dem AGB-Recht einen Verstoß gegen den datenschutzrechtlichen Fairnessgrundsatz impliziert (cc)). Methodische Erwägungen beschließen den Abschnitt (dd)).

aa) Keine Grundlage der Datenverarbeitung nach Art. 6 Abs. 1 lit. a, b DS-GVO

Im hiesigen Kontext zu beurteilende Klauseln oder Einwilligungserklärungen bilden typischerweise die Grundlage für eine Datenverarbeitung nach Art. 6 Abs. 1 lit. a oder b DS-GVO. Die Nichteinbeziehung oder Unwirksamkeit einer derartigen Klausel oder Einwilligung nach AGB-Recht führt daher dazu, dass die genannten Erlaubnistatbestände insoweit nicht einschlägig sind.[850] Allerdings kann Art. 6 Abs. 1 lit. b DS-GVO durchaus in Anspruch genommen werden, sofern die Datenverarbeitung nicht auf die betroffene Klausel, sondern auf einen anderen Vertragsteil gestützt wird, der wirksam bleibt. Insofern spricht aus datenschutzrechtlicher Perspektive nichts dagegen, eine zivilrechtlich wirksame Verpflichtung des Anbieters auch durch vertragsnotwendige Datenverarbeitung (nach Maßgabe des subjektiven Erforderlichkeitsmaßstabs unter Ausblendung von Nutzerpflichten[851]) zu erfüllen.[852]

bb) Auswirkungen auf Art. 6 Abs. 1 lit. f DS-GVO

Ferner indiziert die Missbräuchlichkeit der Klausel, sofern eine Inhaltskontrolle lediglich nach § 307 Abs. 1 S. 1 BGB erfolgt, dass die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO, zugunsten der betroffenen Person ausfällt.[853] Denn die Beurteilung der unangemessenen Benachteiligung erfolgt dann gera-

[850] *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3749), siehe auch bereits oben, § 4 B.II.2.a.

[851] Siehe oben, § 4 B.II.2.b)bb).

[852] Vgl. auch *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3749).

[853] So auch *Wendehorst/Graf von Westphalen*, NJW 2016, 3745 (3749), die allerdings nicht nach verschiedenen Gründen der Unwirksamkeit differenzieren.

de auf Grundlage einer umfassenden Interessenabwägung nach Maßgabe des *Aziz*-Tests. Typischerweise werden dieselben Gründe, die für eine unangemessene Benachteiligung sprechen, auch für ein Überwiegen der Interessen der betroffenen Person streiten. Ausnahmsweise kann dies anders sein, sofern im Rahmen der datenschutzrechtlichen Abwägung Drittinteressen zu berücksichtigen sind. Diesen wird im Rahmen der AGB-rechtlichen Abwägung grundsätzlich keine Rechnung getragen.[854] Positive Externalitäten der Datenverarbeitung können daher zu einer Divergenz der datenschutzrechtlichen Interessenabwägung von der AGB-rechtlichen nach § 307 Abs. 1 S. 1 BGB führen. Entsprechendes gilt für eine Unwirksamkeit bei Verstoß gegen Kardinalpflichten nach § 307 Abs. 2 Nr. 2 BGB. Stützt sich hingegen die AGB-rechtliche Unwirksamkeit wegen einer Verletzung genuin datenschutzrechtlicher Pflichten auf § 307 Abs. 2 Nr. 1 BGB, so hat dies nach hier vertretener Auffassung keinerlei Auswirkungen auf die datenschutzrechtliche Interessenabwägung. Andernfalls würde beispielsweise ein Verstoß gegen spezifische Vorschriften des Einwilligungsregimes die davon datenschutzrechtlich streng zu trennende Interessenabwägung zulasten des Verarbeiters präjudizieren. Zwar können bestimmte datenschutzrechtliche Verstöße (zum Beispiel gegen Art. 25 DS-GVO[855]) durchaus die datenschutzrechtliche Interessenabwägung beeinflussen. Dies ist jedoch völlig unabhängig von dem Umstand, dass der datenschutzrechtliche Verstoß reflexhaft auch eine unangemessene Benachteiligung nach dem AGB-Recht darstellen kann.

Man wird also sagen können, dass immer dann, wenn eine genuin AGB-rechtliche Prüfung der unangemessenen Benachteiligung nach § 307 Abs. 1 S. 1 BGB erfolgt, die Datenverarbeitung typischerweise bei Missbräuchlichkeit der Klausel auch nicht durch die datenschutzrechtliche Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO legitimiert werden kann. Insofern ist in diesem Fall grundsätzlich der Legalitätsgrundsatz verletzt.

cc) Rechtsgebietsübergreifende Fairness:
Auswirkungen auf Art. 5 Abs. 1 lit. a Var. 2 DS-GVO

Schließlich stellt sich die für ein integriertes Marktordnungsrecht besonders relevante Frage, ob eine unangemessene Benachteiligung nach dem AGB-Recht zugleich eine Verletzung des datenschutzrechtlichen Grundsatzes von Treu und Glauben impliziert, wenn der Verantwortliche die in der unwirksamen Klausel oder Einwilligung angelegte Datenverarbeitung tatsächlich vollzieht. Eine begriffliche Nähe wird bereits durch die englischen Sprachfassungen aufgebaut, die jeweils, für die Missbräuchlichkeit einerseits und für Treu und Glauben an-

[854] BGH NJW 1982, 178 (180); OLG Jena, OLG-NL 2005, 265 (266); *Wurmnest*, in: MüKo, BGB, 8. Aufl. 2019, § 307 Rn. 52 f.; *Coester*, in: Staudinger, BGB, 2013, § 307 Rn. 145; aA *Baetge*, AcP 202 (2002), 972 (979 ff.) für Allgemeininteressen.

[855] Siehe etwa *Herfurth*, ZD 2018, 514 (517, 519).

dererseits, den Begriff der *(un)fairness* nutzen. In der Literatur wurde die Frage des Zusammenhangs der beiden Konzepte bereits gelegentlich behandelt, wenn auch mit stark divergierenden Ergebnissen.

Teilweise wird eine strenge Trennung der beiden Begrifflichkeiten postuliert, allerdings auf Grundlage des engen, zur DSRL vertretenen Konzepts des datenschutzrechtlichen Fairnessgrundsatzes als Transparenzgebot.[856] Diese Interpretation kann jedoch unter Geltung der DS-GVO, wie gesehen,[857] nicht mehr aufrechterhalten werden, sodass eine Ausstrahlung der AGB-rechtlichen Wertung auf das Datenschutzrecht nicht aus diesem Grund abgelehnt werden kann. Andere bestimmen das Verhältnis von Datenschutzrecht und AGB-Recht mit Blick auf die jeweiligen Fairnessgrundsätze als unabhängig, aber komplementär,[858] ohne jedoch näher zu erläutern, wie sich dies auf die spezifische Wechselwirkung zwischen den Begriffen auswirkt. Umgekehrt wird ferner, gleichermaßen pauschal, für einen einheitlichen Prüfungsmaßstab zwischen AGB-Recht und Datenschutzrecht plädiert.[859]

Nach hier vertretener Auffassung dürfte es vorzugswürdig sein, der AGB-rechtlichen Missbräuchlichkeit eine Indizwirkung für die Verletzung des datenschutzrechtlichen Grundsatzes von Treu und Glauben zukommen zu lassen,[860] sofern eine eigenständige Prüfung der AGB-rechtlichen Benachteiligung erfolgt ist. Dies respektiert, wie oben bereits ausgeführt, einerseits idiosynkratische Argumentationsbestände der jeweiligen Rechtsgebiete und erhält ihre spezifische Eigenheit, sorgt zugleich jedoch für eine systematische Kohärenz unionsrechtlich determinierter Regelungsmaterien.[861]

Bereits im Ansatz kommt eine Auswirkung der AGB-rechtlichen Missbräuchlichkeit auf den datenschutzrechtlichen Fairnessgrundsatz nicht in Betracht, wenn erstere lediglich eine Reflexwirkung der Verletzung spezifischer datenschutzrechtlicher Pflichten darstellt. Denn insofern gelten dieselben Argumente wie für die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO: Die Verletzung etwa von spezifischen Vorschriften des Einwilligungsregimes kann nicht, über den Umweg der Qualifikation als AGB-rechtlich unangemessene Benachteiligung, die Verletzung des datenschutzrechtlichen Fairnessgrundsatzes bedingen. Denn sonst würde, über die AGB-rechtliche Schleife, jede Verletzung spezieller datenschutzrechtlicher Pflichten zu einer Verletzung des

---

856 *Rhoen*, 5(1) Internet Policy Review 2016, 1 (6).

857 Siehe oben, § 4 A.III.2.b)bb).

858 *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (695); siehe auch ebd., 690: „concurrent, but substantively distinct, fairness assessments".

859 *Nietsch*, CR 2014, 272 (276).

860 Ähnlich: *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (170), allerdings ohne Differenzierung nach dem Grund der AGB-rechtlichen Unwirksamkeit; eine Anküpfung des datenschutzrechtlichen Grundsatzes an die Maßstäbe des AGB-Rechts erwägt auch *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 47.

861 Dazu im Einzelnen oben, § 5 A.II.1.b).

Grundsatzes von Treu und Glauben stilisiert. Dies ist jedoch schon in systematischer Perspektive unhaltbar, da dafür in Art. 83 Abs. 4 lit. a und Abs. 5 lit. a DS-GVO zum Teil unterschiedlich hohe Sanktionen vorgesehen sind.

Erfolgt hingegen eine eigenständige Prüfung der AGB-rechtlichen unangemessenen Benachteiligung nach § 307 Abs. 1 S. 1 BGB, so ist jedenfalls grundsätzlich von einer Verletzung des datenschutzrechtlichen Fairnessgrundsatzes nach Art. 5 Abs. 1 lit. a Var. 2 DS-GVO auszugehen. Dass hier einerseits kein Automatismus im Sinne eines strikten Durchschlagens der AGB-rechtlichen Wertung auf die datenschutzrechtliche Frage angenommen werden kann, ergibt sich aus denselben Gründen, die den EuGH in den Rechtssachen *Pereničová und Perenič* und *Bankia* bewogen haben, die Unlauterkeit einer Geschäftspraxis lediglich als zu berücksichtigen Umstand für die Frage der Missbräuchlichkeit einer Klausel anzusehen.[862] Denn hier wie dort ist nicht ausgeschlossen, dass weitere Gesichtspunkte infolge der Eigenart des einen Rechtsbereichs hinzutreten, welche für das Verdikt nach dem anderen Rechtsbereich nicht berücksichtigt wurden.[863] Wie bereits aufgezeigt, kann im Datenschutzrecht zum Beispiel, deutlich stärker als im AGB-Recht, Drittinteressen Rechnung getragen werden. Daher ist nicht ausgeschlossen, dass positive Externalitäten auch hinsichtlich des datenschutzrechtlichen Fairnessgrundsatzes eine Abweichung von der AGB-rechtlichen Beurteilung verlangen.[864]

Andererseits ist das AGB-rechtliche Verdikt jedoch für die Frage der Verletzung des Grundsatzes von Treu und Glauben auch nicht irrelevant. Dafür spricht nicht nur der ausdrückliche Verweis auf die Klauselrichtlinie im 42. Erwägungsgrund der DS-GVO, sondern auch der Umstand, dass sowohl die Klauselrichtlinie (16. Erwägungsgrund) als auch die DS-GVO (43. Erwägungsgrund) einen Schutz gegen Ungleichgewichte in der Verhandlungsposition bieten sollen.[865] Diese konvergente Zielrichtung öffnet der Berücksichtigung nicht genuin datenschutzrechtlicher Belange bei der Auslegung des datenschutzrechtlichen Fairnessgrundsatzes die Tür. Da jedoch keine Zieliden-

---

[862] Dazu oben, § 5 A.II.1.

[863] Vgl. EuGH, Urt. v. 15.3.2012 – Rs. C-453/10 (*Pereničová und Perenič*) – Rn. 43 f.; Urt. v. 19.9.2018 – Rs. C-109/17 (*Bankia*) – Rn. 49; siehe auch *Alexander*, WRP 2012, 515 (519); *Stempel*, Treu und Glauben im Unionsprivatrecht, 2016, 108.

[864] Wenig ergiebig erscheint demgegenüber der Umstand, dass der Verbraucherschutz nach Art. 38 GRCh lediglich einen Chartagrundsatz darstellt, der Datenschutz hingegen nach Art. 8 GRCh ein Grundrecht. *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (690) wollen daraus einen Unterschied der einerseits datenschutzrechtlich und andererseits verbraucherrechtlich verbürgten Fairnessprinzipien ableiten. Allerdings liegt insofern ein Erst-Recht-Schluss näher: Wenn schon eine Norm des nach Art. 52 Abs. 5 GRCh ein deutlich schwächeres Schutzniveau bietenden Grundsatzes des Verbraucherschutzes verletzt ist, dann erst recht eine Norm des primärrechtlich stärker ausgestalteten Grundrechts auf Datenschutz. Letztlich wird man dieser primärrechtlichen Differenz jedoch keine entscheidende Bedeutung zumessen können, da die spezifisch-sekundärrechtlichen Argumente gegen einen derartigen Erst-Recht-Schluss sprechen.

[865] Siehe auch *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (133).

tität vorliegt,[866] sondern die DS-GVO bekanntlich, anders als die Klauselrichtlinie, auch den freien Datenverkehr zwischen den Mitgliedstaaten fördern möchte,[867] spricht auch die Berücksichtigung der mit den jeweiligen Instrumenten verfolgten Ziele lediglich für eine Indizwirkung der AGB-rechtlichen Wertung, nicht jedoch für einen strikten Durchgriff auf das Datenschutzrecht.

Ein Beispiel für die Übereinstimmung von AGB-rechtlicher und datenschutzrechtlicher Fairnesswertung können etwa weite Leistungspflichten sein, sofern diese nach § 307 Abs. 1 S. 1 BGB unwirksam sind. Denn diesen eignet typischerweise ein Überraschungs- und Verbergungselement hinsichtlich der begehrten datenschutzrechtlichen Rechtsfolgen, sodass eine Verletzung von Treu und Glauben durchaus naheliegend erscheint.

dd) Methodisches Ergebnis

In methodischer Hinsicht lassen sich daher Wechselwirkungen zwischen dem AGB-Recht und dem Datenschutzrecht in beiden Richtungen identifizieren. Dabei liegt es nahe, jeweils mit der spezifischeren Norm zu beginnen. So impliziert einerseits grundsätzlich die Verletzung spezifischer datenschutzrechtlicher Pflichten die AGB-rechtliche unangemessene Benachteiligung, sowohl im Bereich der Transparenzkontrolle als auch der Inhaltskontrolle im engeren Sinne. Diesen Schluss vom Datenschutzrecht auf das AGB-Recht hat die Rechtsprechung auch in der Vergangenheit immer wieder vollzogen.[868]

Geht es hingegen um eine substantielle Unangemessenheit im Sinne einer umfassenden Interessenabwägung, so sollte die Schlussrichtung aus methodischer Perspektive umgekehrt werden. Die substantielle Unangemessenheit im AGB-rechtlichen Sinne indiziert die Unrechtmäßigkeit der Datenverarbeitung nach der DS-GVO, sowohl mit Blick auf die datenschutzrechtliche Interessenabwägungsklausel nach Art. 6 Abs. 1 lit. f DS-GVO als auch auf den Grundsatz von Treu und Glauben nach Art. 5 Abs. 1 lit. a Var. 2 DS-GVO. Diese Schlussrichtung hat den methodischen Vorteil, dass mit dem hypothetischen Verhandlungsmechanismus der Klauselkontrolle ein Maßstab zur Verfügung steht, der, in gewissen Grenzen, präziser operationalisiert werden kann als die bislang noch äußerst vagen Vorgaben der DS-GVO. Insgesamt lässt sich damit eine Koordination und jedenfalls grundsätzlich auch ein Gleichklang zwischen Klauselkontrolle einerseits und DS-GVO andererseits erreichen, der zugleich die Eigengesetzlichkeiten der jeweiligen Rechtsgebiete zu respektieren vermag.

h) Zusammenfassung zur AGB-Kontrolle

Zusammenfassend lässt sich damit festhalten, dass die DS-GVO und das AGB-Recht von einer Wechselbezüglichkeit geprägt sind, die zugleich den jeweiligen

[866] Vgl. *Clifford/Graef/Valcke*, 20 German Law Journal 2019, 679 (693).
[867] Siehe oben, § 5 A.I.2.c)aa).
[868] Siehe die Nachweise in § 5, Fn. 616 sowie § 5, Fn. 713–715.

Rechtsgebieten Raum für eigenständige Wertungen belässt. Die §§ 305 ff. BGB sind demnach neben der DS-GVO ohne Weiteres anwendbar und haben eine eigenständige Bedeutung, die sich nicht im bloßen Nachvollzug datenschutzrechtlicher Vorgaben erschöpft. Das Datenschutzrecht ist insofern nicht alleiniger Prüfungsmaßstab der AGB-Kontrolle unter Geltung der DS-GVO. Der BGH wird seine diesbezügliche Rechtsprechung aufgeben müssen.

Schon an der Einbeziehungskontrolle nach § 305c Abs. 1 BGB scheitern Klauseln, welche eine Parteistellung Dritter etablieren sollen, die gegenüber dem Nutzer nicht klar außerhalb von AGB als solche benannt wurden. Die aus datenschutzrechtlicher Perspektive für die Anbieter wünschenswerte Einbeziehung von Drittanbietern kann daher nicht ausschließlich auf dem Weg über AGB erfolgen. Dagegen reicht ein etwaiger Überraschungseffekt hinsichtlich der datenschutzrechtlichen Legitimierungswirkung, die Art. 6 Abs. 1 lit. b DS-GVO vermittelt, nach hier vertretener Auffassung nicht aus, um eine Vertragsklausel als überraschend im Sinne von § 305c Abs. 1 BGB zu qualifizieren.

Im Rahmen der AGB-rechtlichen Transparenzkontrolle kommt es lediglich zu einem Nachvollzug der deutlich detaillierteren datenschutzrechtlichen Informationspflichten, soweit die Einwilligung betroffen ist. Keine Besonderheiten bestehen hingegen hinsichtlich der Transparenz von Vertragsklauseln, welche eine datenschutzrechtliche Erlaubnis nach Art. 6 Abs. 1 lit. b DS-GVO auslösen.

Die Inhaltskontrolle im engeren Sinne setzt hingegen voraus, dass die relevante Einwilligungserklärung oder Vertragsklausel nach § 307 Abs. 3 S. 1 BGB kontrollfähig ist. Bei der Einwilligung ist dies aufgrund ihrer rechtsgestaltenden Wirkung nach hier vertretener Auffassung immer der Fall. Aber auch Vertragsklauseln, welche eine datenbasierte Gegenleistung oder eine datenschutzrechtlich relevante Leistungsbeschreibung des Anbieters enthalten, sind in richtlinienkonformer, teleologischer Reduktion von § 307 Abs. 3 S. 1 BGB kontrollfähig. Denn hinsichtlich der datenbasierten Leistungen kommt es typischerweise gerade zu einem partiellen Versagen des Preismechanismus und zu rationaler Ignoranz auch von vertraglichen Hauptpflichten. Daher sind die rechtsökonomischen Prämissen, auf denen die Ausnahme der Hauptleistungspflichten und ihres Verhältnisses von der Klauselkontrolle aufruhen, gerade nicht erfüllt. Hinsichtlich der Angemessenheit des Preis-/Leistungsverhältnisses ist jedoch nach deutschem Zivilrecht systematisch § 138 Abs. 1 BGB mit der Fallgruppe des auffälligen Missverhältnisses vorrangig.

Maßstab der dergestalt eröffneten Inhaltskontrolle im engeren Sinne ist einerseits das Datenschutzrecht, andererseits aber auch der adaptierte *Aziz*-Test. Danach stellen Klauseln eine unangemessene Benachteiligung dar, wenn sie nicht das Ergebnis einer hypothetischen, individuellen Vertragsverhandlung des Verwenders mit einem Referenzakteur sein können. Dieser Referenzakteur ist grundsätzlich ein durchschnittlicher Nutzer mit mittelmäßig ausgeprägten Datenschutzpräferenzen; dem Anbieter bekannte stark ausgeprägte Daten-

schutzpräferenzen müssen jedoch ebenfalls Berücksichtigung finden. Auf diesem Weg kann der *Aziz*-Test moderat personalisiert werden. Allerdings kann eine unangemessene Benachteiligung nur angenommen werden, wenn hinreichend gesichert erscheint, dass der *Aziz*-Test fehlschlägt. Dies bedingt im Ergebnis eine zurückgenommene Dimension der, gegenüber dem Datenschutzrecht eigenständigen, AGB-rechtlichen Inhaltskontrolle.

Eine Unwirksamkeit infolge unangemessener Benachteiligung ergibt sich sodann in drei Fällen im Rahmen der hier behandelten datenbasierten Austauschprozesse. Erstens folgt sie aus einem Verstoß gegen datenschutzrechtliche Vorschriften, besonders bei der Einwilligung. Die Grundsätze der Datenverarbeitung nach der DS-GVO werden durch die AGB-Kontrolle nach hier vertretener Auffassung noch verschärft. Zweitens kann sich ausnahmsweise eine Unwirksamkeit aus einer isoliert exzessiven Pflicht zur Datenüberlassung ergeben, wenn der *Aziz*-Test mit hinreichender Konfidenz fehlschlägt. Diese Fallgruppe muss jedoch auf Extremfälle beschränkt werden. Drittens stellen weite Leistungspflichten eine unangemessene Benachteiligung dar, wenn sie mit der vertraglichen Hauptleistungspflicht des Anbieters nicht konnex sind und für den Nutzer gegenüber dem Marktstandard keinen Mehrwert bieten, aber datenschutzrechtliche Schutzvorkehrungen infolge der Substitution der Einwilligung durch die vertragserforderliche Datenverarbeitung unterlaufen. Die AGB-Kontrolle reproduziert dann, auf vertragsrechtlichem Wege, jene Schutzinstitute, die im datenschutzrechtlichen Bereich durch die weite Leistungspflicht ausgeschaltet wurden.

Rechtsfolge der Unwirksamkeit ist, in richtlinienkonformer Auslegung von § 306 BGB, dass bei Unwirksamkeit der Gegenleistungspflicht die Hauptleistungspflicht des Anbieters grundsätzlich entfällt. Eine Aufrechterhaltung kommt nur bei Vorleistung des Verbrauchers in Betracht. Auch die Unwirksamkeit der Einwilligung kann zur Folge haben, dass der Vertrag unwirksam wird. Denn hier entfaltet das Sanktionsinstrumentarium der DS-GVO ebenfalls hinreichende Abschreckungswirkung. Eine weite, inkonnexe Leistungspflicht entfällt hingegen immer ersatzlos.

In datenschutzrechtlicher Hinsicht bedingt die Unangemessenheit nach § 307 Abs. 1 S. 1 BGB, dass nicht nur der Erlaubnistatbestand von Art. 6 Abs. 1 lit. a oder b DS-GVO nicht einschlägig ist, sondern auch, jedenfalls grundsätzlich, die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO zugunsten der betroffenen Person ausfällt. Ferner indiziert die eigenständige Prüfung der Unangemessenheit nach dem AGB-Recht, dass der datenschutzrechtliche Fairnessgrundsatz verletzt ist. Eine abweichende Bewertung der datenschutzrechtlichen von der AGB-rechtlichen Fairness kann jedoch durch die Berücksichtigung von Drittinteressen oder die besondere Bedeutung einer Verarbeitung für den freien Datenverkehr zwischen den Mitgliedstaaten zustande kommen.

Insgesamt zeigt sich damit in methodischer Hinsicht eine Wechselbeziehung zwischen DS-GVO und Klauselrichtlinie, bei der Schlüsse in beide Rich-

tungen möglich sind. Methodisch vorzugswürdig ist dabei jeweils der Ausgang von der spezifischeren Norm: speziellen datenschutzrechtlichen Pflichten einerseits oder aber dem *Aziz*-Test als marktbezogener Operationalisierung der Schranken der Privatautonomie andererseits.

2. § 138 BGB

Die AGB-Kontrolle der §§ 305 ff. BGB wird, besonders hinsichtlich der dort radizierten Inhaltskontrolle, ergänzt durch die Grenzen, welche der privatautonomen Gestaltung von Rechtsverhältnissen in § 138 BGB gesetzt sind.[869] Mit Blick auf die im vorliegenden Kontext interessierenden datenbasierten Austauschverhältnisse sind hier zwei unterschiedliche Fallgruppen zu unterscheiden. Einerseits erfährt die Kontrolle des Äquivalenzverhältnisses aufgrund der bereits im Rahmen der AGB-Kontrolle diskutierten Gefahr des Marktversagens bei digitalen Austauschprozessen einen erheblichen Bedeutungsgewinn. Hier lässt sich fragen, inwieweit § 138 BGB Maßstäbe für eine „datenbasierte *laesio enormis*" zu entnehmen sind. Daneben kommen, wenngleich in der Praxis ungleich weniger bedeutsam, weitere Fallgruppen klassischer Sittenwidrigkeitstatbestände in Betracht, die ebenfalls hinsichtlich datenschutzrechtlich relevanter Klauseln einschlägig sein können.

In beiden Fällen ist zunächst zu fragen, inwiefern § 138 BGB neben der DS-GVO anwendbar ist (a)). Sodann ist der Tatbestand der Sittenwidrigkeit insbesondere mit Blick auf das wucherähnliche Geschäft in datenbasierten Austauschverhältnissen zu konkretisieren (b)), bevor Rechtsfolgen (c)) und Wechselwirkungen mit dem Datenschutzrecht beleuchtet werden (d)). Eine Zusammenfassung beschließt wiederum den Abschnitt (e)).

a) Anwendbarkeit neben der DS-GVO

Hinsichtlich der Anwendbarkeit von § 138 BGB neben der DS-GVO ist einmal mehr scharf zwischen die Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO legitimierenden Verträgen einerseits und der datenschutzrechtlichen Einwilligung nach Art. 4 Nr. 11 DS-GVO andererseits zu unterscheiden.

aa) Verträge

Die Anwendbarkeit von § 138 BGB auf Vertragsklauseln, die nach Art. 6 Abs. 1 lit. b DS-GVO eine Datenverarbeitung erlauben, steht außer Frage. Denn auch hier gilt das Credo, dass die DS-GVO keine eigenständigen Regelungen zur Bestimmung der Wirksamkeit derartiger Vertragsklauseln beinhaltet und insofern keinerlei Sperrwirkung für das nationale Vertragsrecht entfaltet.[870] Glei-

[869] Siehe nur *Lorenz*, Der Schutz vor dem unerwünschten Vertrag, 1997, 245 f.; *Fastrich*, Richterliche Inhaltskontrolle im Privatrecht, 1992, 215 ff.; *Becker*, Der unfaire Vertrag, 2003, 8.

[870] Siehe bereits oben, § 5, Fn. 582.

ches gilt für die DIDD-Richtlinie nach ihrem Art. 3 Abs. 10 sowie die Warenkauf-Richtlinie nach ihrem Art. 3 Abs. 6.

bb) Einwilligung

Die Möglichkeit der Anwendung von § 138 BGB auf eine datenschutzrechtliche Einwilligungserklärung hingegen steht durchaus infrage. Zwar scheitert sie nicht an der Rechtsnatur der Einwilligung, da § 138 BGB auf geschäftsähnliche Handlungen wie die datenschutzrechtliche Einwilligung analog anzuwenden ist.[871] In der Literatur zur Einwilligung außerhalb des Datenschutzrechts wird zudem bisweilen angenommen, dass die Einwilligung immanenten Schranken unterliegt, die sich nicht aus § 138 BGB, sondern vorrangig aus der Natur des betroffenen Rechts ergäben.[872] Dies wird man hingegen im Falle des Datenschutzrechts nicht annehmen können, da die Kriterien der Wirksamkeit der Einwilligung *insoweit* abschließend in der DS-GVO geregelt sind: Wenn eine Einwilligung alle Wirksamkeitsvoraussetzungen der DS-GVO erfüllt, steht der Anwendungsvorrang einer rechtlichen Wertung entgegen, wonach der Einwilligung *lediglich* wegen besonderer Betroffenheit des Datenschutzgrundrechts die Wirksamkeit versagt sein soll.[873]

In Frage stellen kann die Anwendbarkeit von § 138 BGB auf die datenschutzrechtliche Einwilligung daher nur der Anwendungsvorrang des Unionsrechts. Zum Teil wird hier in der Literatur in der Tat angenommen, dass die DS-GVO insofern einen vollständigen Anwendungsvorrang beanspruche, als eine sittenwidrige Einwilligung grundsätzlich bereits wegen Unfreiwilligkeit oder Uninformiertheit nach der DS-GVO unwirksam sei.[874] Indes kann dies nach hier vertretener Auffassung lediglich für § 138 Abs. 2 BGB gelten, da nur hier in der Tat die Freiwilligkeit infolge der dort genannten Umstände (Zwangslage etc.) aufgehoben ist.[875] Hinsichtlich der Anwendbarkeit von § 138 Abs. 1 BGB hingegen ist zwischen der Kontrolle des Äquivalenzverhältnisses

[871] Siehe bereits oben, § 6 A.I.1.a) und b); zur analogen Anwendung von § 138 BGB auf die medizinische Einwilligung BGH NJW 1976, 1790 (1790); für eine Anwendung von § 138 BGB auf die datenschutzrechtliche Einwilligung *Kohte*, AcP 185 (1985), 105 (135); dies erwägend auch *Kilian*, JZ 1977, 481 (484), für die arbeitsrechtliche Kontexte.

[872] Dazu umfassend *Ohly*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, 2002, 408 ff.; für eine Anwendung von § 138 BGB *Kohte*, AcP 185 (1985), 105 (131 ff.); siehe auch *Canaris*, AcP 184 (1984), 201 (232 ff.) zu sich unmittelbar aus Grundrechten ergebenden Grenzen der Privatautonomie, die gegenüber § 138 Abs. 1 BGB vorrangig seien.

[873] Anders noch zum BDSG aF *Kohte*, AcP 185 (1985), 105 (135), der eine Einwilligung bei völliger datenschutzrechtlicher Entäußerung für gem. § 138 BGB unwirksam hält. Hier wird jedoch nunmehr regelmäßig ein Verstoß gegen einen der Grundsätze der Datenverarbeitung vorliegen, etwa Art. 5 Abs. 1 lit. b oder c DS-GVO; wo nicht, ist eine Unwirksamkeit nicht angezeigt.

[874] *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 49.

[875] So auch *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 83.

einerseits und den weiteren Fallgruppen der Sittenwidrigkeit andererseits zu differenzieren.

(1) Preis-/Leistungs-Verhältnis: Datenbasierte *laesio enormis*

Die Kontrolle des Äquivalenzverhältnisses erfolgt im Rahmen von § 138 Abs. 1 BGB grundsätzlich außerhalb unionsrechtlicher Vorgaben. Zwar können unionsrechtliche Wertungen berücksichtigt werden, § 138 Abs. 1 BGB setzt jedoch nach tradierter Auffassung keine Richtlinie um.[876] Insofern wäre an sich die oben entwickelte zweistufige Prüfung anzuwenden,[877] die nach der Risikospezifizität und der Zielkompatibilität der jeweiligen nationalen Vorschrift fragt, um eine Vereinbarkeit mit dem unionalen Effektivitätsgrundsatz sicherzustellen. Im Bereich datenbasierter Austauschprozesse besteht hingegen die Besonderheit, dass, wie gesehen, eine Kontrolle des Äquivalenzverhältnisses nach hier vertretener Auffassung infolge der teleologischen Reduktion von Art. 4 Abs. 2 der Klauselrichtlinie in den durch die Klauselrichtlinie harmonisierten Bereich fällt und lediglich aus systematischen Gründen nicht im Rahmen von § 307 Abs. 1 S. 1 BGB, sondern von § 138 Abs. 1 BGB erfolgt.[878] Dies impliziert, dass § 138 Abs. 1 BGB in diesem Kontext unionsrechtlich aufgeladen wird. Zwar kann kein konkreter auf § 138 Abs. 1 BGB bezogener Umsetzungswille des deutschen Gesetzgebers festgestellt werden, da die Umsetzung der Klauselrichtlinie im BGB allein in den §§ 305 ff. BGB erfolgte und § 138 Abs. 1 BGB vor Erlass der Klauselrichtlinie verabschiedet wurde.[879] Dies ist jedoch nach zutreffender Auffassung kein Hinderungsgrund für eine richtlinienkonforme Auslegung, da sich deren Notwendigkeit bereits aus dem Unionsrecht[880] und dem deutschen Verfassungsrecht[881] ergibt und nach der Auffassung des EuGH das gesamte nationale Recht, nicht nur das zur Umsetzung erlassene, umfasst,[882] auch wenn es vor Erlass der Richtlinie in Kraft getreten

[876] *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 16.

[877] Siehe oben, § 5 A.I.2.b).

[878] Siehe oben, § 5 C.II.1.e)aa)(3)(b).

[879] *Suhr*, Richtlinienkonforme Auslegung im Privatrecht und nationale Auslegungsmethodik, 2011, 220; *W.-H. Roth/Jopen*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 263 (283 Rn. 40); *Canaris*, in: Festschrift Bydlinski, 2002, 47 (50 f.); die *Bundesregierung* scheint hingegen davon auszugehen, dass auch vor Erlass einer Richtlinienbestimmung erlassene nationale Normen nachträglich zu einer Umsetzungsnorm umqualifiziert werden können, siehe *Bundesregierung*, Questionnaire on the implementation of the Article 5(3) of the ePrivacy Directive, KommDok. COCOM11–20 vom 4.10.2011, 3 ff.

[880] Grundlagen sind Art. 288 Abs. 3 AEUV und Art. 4 Abs. 3 EUV; siehe nur *Roth/Jopen*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 263 (265 Rn. 3 ff.); *Canaris*, in: Festschrift Bydlinski, 2002, 47 (55 ff.); *Suhr*, Richtlinienkonforme Auslegung im Privatrecht und nationale Auslegungsmethodik, 2011, 220 ff.

[881] *Roth/Jopen*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 263 (282 Rn. 39).

[882] EuGH, Urt. v. 14.7.1994 – Rs. C-91/92 (*Faccini Dori*) – Rn. 26; Urt. v. 5.10.2004 – verb. Rs. C-397/01 bis C-403/01 (*Pfeiffer*) – Rn. 113–116; *Craig/de Búrca*, EU Law, 2015, 209 f.

ist.[883] Der konkrete Umsetzungswille des nationalen Gesetzgebers bezüglich einer Norm ist demgegenüber hinreichender, nicht jedoch notwendiger Grund für eine richtlinienkonforme Auslegung dieser Norm.[884]

Daher fällt die Frage des Verhältnisses von § 138 Abs. 1 BGB und DS-GVO nicht in den Bereich des Anwendungsvorrangs, sondern des sachintegrativen Wertungsausgleichs zwischen verschiedenen Normen unionsrechtlicher Provenienz, soweit die Äquivalenzkontrolle datenbasierter Gegenleistungen betroffen ist. Insofern wurde bereits festgestellt, dass die AGB-Kontrolle grundsätzlich neben der DS-GVO Anwendung findet. Es bleibt damit zu zeigen, dass auch für den Bereich der Äquivalenzkontrolle die DS-GVO keine abschließenden Regelungen bereithält. Vielmehr ist damit ein eigenständiges Risiko angesprochen, das im Rahmen der DS-GVO nicht adressiert wird.[885]

(a) Risikospezifizität gegenüber Art. 5 Abs. 1 lit. c DS-GVO

Zwar enthält Art. 5 Abs. 1 lit. c DS-GVO mit dem Grundsatz der Datenminimierung auch ein datenschutzrechtliches Exzessverbot, welches bereits nach der DSRL anerkannt war.[886] Dieses richtet sich jedoch lediglich auf den Zweck der Datenverarbeitung. Dieser steht zwar mit den Hauptleistungspflichten häufig in einem Zusammenhang. Dennoch findet über das Exzessverbot der DS-GVO keine eigenständige Überprüfung der Äquivalenz von Leistung und Gegenleistung im Rahmen eines Austauschverhältnisses statt. Dies gilt ohne Weiteres für die Datenverarbeitung legitimierende Vertragsklauseln, da diese von der DS-GVO ohnehin ausgeblendet werden. Aber auch hinsichtlich der Datenverarbeitung auf Grundlage einer Einwilligung erschöpft sich das Exzessverbot darin, festzustellen, ob der Umfang der Einwilligung mit dem der Datenverarbeitung inhärenten Zweck vereinbar ist.[887] Insbesondere wird dieser Grundsatz konkretisiert durch das Bestimmtheitsgebot der Einwilligung, wonach diese für bestimmte Zwecke erteilt werden muss. Anders als das Leistungsversprechen des Anbieters, dem der Nutzer zustimmen muss, kann der Zweck jedoch einseitig vom datenschutzrechtlich Verantwortlichen festgelegt werden. Er entspricht daher regelmäßig vor allem den Interessen des Verantwortlichen, wohingegen das Leistungsversprechen dem Nutzer zugutekommt. So mag der Zweck einer bestimmten Datenverarbeitung, die sich an die Überlassung von Daten als Gegenleistung anschließt, in der Schaltung von persona-

[883] EuGH, Urt. v. 13.11.1990 – Rs. C-106/89 (*Marleasing*) – Rn. 8; *Everling*, ZGR 1992, 376 (378 f.); *Roth/Jopen*, in: Riesenhuber (Hrsg.), Europäische Methodenlehre, 3. Aufl. 2015, 263 (288 Rn. 52); *Canaris*, in: Festschrift Bydlinski, 2002, 47 (73 f.); vgl. auch *Herresthal*, Rechtsfortbildung im europarechtlichen Bezugsrahmen, 2006, 319 ff.

[884] *Canaris*, in: Festschrift Bydlinski, 2002, 47 (51); *Gänswein*, Der Grundsatz unionsrechtskonformer Auslegung nationalen Rechts, 2009, 33; vgl. auch *Herresthal*, Rechtsfortbildung im europarechtlichen Bezugsrahmen, 2006, 319 f.

[885] Siehe auch *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (219).

[886] Siehe oben, Text bei § 4, Fn. 405.

[887] Siehe oben, § 4 A.III.2.b)ee).

lisierter Werbung liegen. Dieser Zweck ist jedoch von der typischen Hauptleistungspflicht des Anbieters, etwa der Eröffnung des Zugangs zu einem sozialen Netzwerk, klar zu trennen. Daher ist die Prüfung des Exzessverbots im Rahmen des Grundsatzes der Datenminimierung und auch der einwilligungsbezogene Bestimmtheitsgrundsatz auf gänzlich andere Kategorien bezogen als die Kontrolle des Äquivalenzverhältnisses nach §138 Abs. 1 BGB. Es ist daher denkbar, dass eine Einwilligung für bestimmte Zwecke erteilt wird, die vom Verantwortlichen festgelegt werden, wobei die Datenverarbeitung für diese Zwecke strikt erforderlich ist und daher den Zweckbindungsgrundsatz sowie den Grundsatz der Datenminimierung erfüllt, andererseits jedoch das Äquivalenzverhältnis zwischen Leistung und Gegenleistung nicht gewahrt ist. Dies stellt daher gegenüber den genannten Bestimmungen der DS-GVO ein eigenständiges Risiko dar.

(b) Risikospezifizität gegenüber Art. 5 Abs. 1 lit. a Var. 2 DS-GVO

Denkbar wäre allenfalls, eine Äquivalenzkontrolle auf Grundlage des Grundsatzes der Datenverarbeitung nach Treu und Glauben durchzuführen. Dies könnte auch Fälle von Sittenwidrigkeit, die sich auf eine Äquivalenzstörung gründen, umfassen. Auch hier erscheint es jedoch vorzugswürdig, zunächst auf die spezifischen Ausprägungen einer Äquivalenzkontrolle im nationalen Recht zurückzugreifen. Dies ist insofern einer Harmonisierungswirkung nicht abträglich, als sich diese nationalen Bestimmungen nach hier vertretener Auffassung als Umsetzungen der Klauselrichtlinie darstellen, da Art. 4 Abs. 2 der Klauselrichtlinie, wie ausgeführt, teleologisch reduziert werden muss. Daher steht letztlich in dieser Hinsicht auch der Rechtsweg zum EuGH offen. Dass jedoch die Klauselrichtlinie neben der DS-GVO Anwendung findet, wurde bereits ausgeführt. Die Einschätzung einer Klausel als sittenwidrig bei Verstoß gegen den Äquivalenzgrundsatz kann daher Auswirkungen auf den datenschutzrechtlichen Grundsatz von Treu und Glauben haben. Dieser bietet jedoch letztlich auch keine hinreichende Grundlage, um auf seiner Basis einen umfassenden „allgemeinen Teil" des Datenschutzprivatrechts auf unionaler Ebene auszuarbeiten. Dies wäre jedoch die Konsequenz, wenn die allgemeinen Grenzen der Privatautonomie der mitgliedstaatlichen Zivilgesetzbücher in den Fairnessgrundsatz hineingelesen würden. Der datenschutzrechtliche Grundsatz nimmt daher Wertungen zum Äquivalenzverhältnis auf, präjudiziert diese jedoch nicht.[888]

(2) Sonstige Sittenwidrigkeitstatbestände

Anders wiederum stellt sich in dogmatischer Hinsicht die Rechtslage dar, soweit andere Sittenwidrigkeitstatbestände als die des auffälligen Missverhält-

[888] Dazu genauer unten, §5 C.II.2.d).

nisses zwischen Leistung und Gegenleistung betroffen sind. Die Ausnutzung eines strukturellen Machtungleichgewichts ist, soweit man darin eine die Sittenwidrigkeit berührende Fallgruppe erkennen möchte,[889] vom Kriterium der Freiwilligkeit der Einwilligung nach Art. 4 Nr. 11 DS-GVO abschließend erfasst.[890] Andere Fallgruppen dürften regelmäßig von eher theoretischem Interesse sein. Denkbar ist etwa, dass ein Großvater die Verarbeitung seiner personenbezogenen Kontodaten durch seine Enkelin von der Bedingung abhängig macht, dass diese eine bestimmte Heirat nicht eingeht.[891]

Insoweit stellt sich § 138 BGB jedoch nicht als Umsetzung der Klauselrichtlinie, sondern als genuin nationale Bestimmung dar. Daher muss die Frage der Anwendbarkeit neben der DS-GVO nach der oben entwickelten zweistufigen Prüfung geklärt werden,[892] die Risikospezifizität und Zielkompatibilität verlangt. Das Risiko, dass durch eine Einwilligung gegen wie auch immer definierte gute Sitten verstoßen wird, ist in der DS-GVO nicht berücksichtigt worden. Auch hier käme allenfalls der Grundsatz der Datenverarbeitung nach Treu und Glauben in Betracht. Dieser bindet jedoch lediglich den datenschutzrechtlich Verantwortlichen (Art. 5 Abs. 2 DS-GVO), nicht aber den Einwilligenden oder denjenigen, der seine Daten unter Stellung einer sittenwidrigen Bedingung überlässt. Schon aus diesem Grunde können Fälle wie die sittenwidrige Heiratsklausel durch die DS-GVO nicht erfasst werden.

Auf der zweiten Stufe ist daher danach zu fragen, ob das Ziel der Regelung des § 138 BGB mit dem unionalen Datenschutzrecht, besonders mit der Harmonisierung der Wirksamkeitsvoraussetzungen der Einwilligung, kompatibel ist. Dies wird stark von der Interpretation des Begriffs der guten Sitten abhängen. Die dazu bestehenden Auffassungen können und müssen hier nicht im Einzelnen vertieft werden.[893] Sofern jedoch einzelne Rechtsordnungen die Sittenwidrigkeit als rechtlichen Transmissionsriemen für nicht anderweitig rechtlich fundierte, lediglich historisch tradierte Moralvorstellungen auffassen sollten,[894] dürfte dies nicht mehr mit dem auch auf Schaffung eines Binnenmarkts

---

[889] *Kohte*, AcP 185 (1985), 105 (134 f.); *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 85 ff.

[890] Siehe nur den 43. Erwägungsgrund der DS-GVO.

[891] Siehe zu der Parallelfrage der Sittenwidrigkeit einer derartigen Bedingung in einem Erbvertrag BVerfG NJW 2004, 2008; ferner OLG Saarbrücken, DNotZ 2015, 691; *Leipold*, in: MüKo, BGB, 7. Aufl. 2017, § 2074 Rn. 19 ff.; *Flume*, AT II, 4. Aufl. 1992, 369.

[892] Siehe oben, § 5 A.I.2.b).

[893] Zur Kontroverse um den Begriff im deutschen Recht siehe aus dem umfangreichen Schrifttum nur *Heinrich*, Formale Freiheit und materiale Gerechtigkeit, 2000, 369 ff.; *Eckert*, AcP 199 (1999), 337 (345 ff.); *Sack*, NJW 1985, 761; *Sack*, GRUR 1970, 493 (494 ff.); *Mayer-Maly*, AcP 194 (1994), 105 (174 f.); *Sack/Fischinger*, in: Staudinger, BGB, 2017, § 138 Rn. 62 ff.; *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 11 ff.; *Hefermehl*, in: Soergel, BGB, 13. Aufl. 1999, § 138 Rn. 2 ff.

[894] Dagegen treffend *Sack*, NJW 1985, 761 (767 f.); vorsichtig bejahend für in der Rechtsgemeinschaft auffindbare gemeinsame Wertungen *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 11; grundlegend zum Verhältnis von materialen Wertungen und General-

für Daten ausgerichteten unionalen Datenschutzrecht vereinbar sein. Wenn etwa eine Einwilligung, Daten zu Zwecken der außerehelichen Partnersuche oder des Matching von Sexualpartnern zu verarbeiten, an einer nationalen Sittenwidrigkeitsgrenze scheitern sollte,[895] so dürfte insofern der Anwendungsvorrang des Unionsrechts greifen. Denn der digitale unionale Binnenmarkt ist gerade auch auf die Möglichkeit der Datenübertragung in freier Selbstbestimmung ausgerichtet, die nicht durch rechtlich nicht eingehegte, lediglich überkommene Moralvorstellungen unterminiert werden sollte. Für das deutsche Recht allerdings ist eine solche Auslegung des § 138 BGB, im Bereich der Sexualmoral insbesondere seit Inkrafttreten des ProstG, richtigerweise ohnehin abzulehnen.[896]

Soweit jedoch Sittenwidrigkeit zum Beispiel als unzulässiger Eingriff in die individuelle Selbstbestimmung interpretiert wird,[897] wie im Falle der Heiratsklausel,[898] ist nicht ersichtlich, dass dies mit einem auf individuellen, privatautonomen Austauschverhältnissen basierenden Binnenmarkt inkompatibel wäre. Vielmehr stützt ein derartiger Ordnungsrahmen letztlich das Vertrauen in konsensuale Austauschprozesse und kann daher langfristig auch der Effizienz zugutekommen.[899]

Zudem ist auch der unionale Binnenmarkt, wie bereits angemerkt, nicht ausschließlich auf die Verwirklichung ökonomischer Effizienz ausgerichtet, sondern auch offen für rechtliche Ordnungsstrukturen, die einen Rahmen bereitstellen, um bestimmte Formen von missbilligtem Marktverhalten zu sanktionieren. Dies zeigen etwa die Klauselrichtlinie und die UGP-Richtlinie ganz deutlich. Im Bereich des Datenschutzprivatrechts kommt dies durch die Grundsätze der Datenverarbeitung – und hier insbesondere den Fairnessgrundsatz – in besonders prägnanter Weise zum Ausdruck. Daher ist die Anwendung von § 138 BGB mit den Zielen des unionalen Datenschutzrechts vereinbar, soweit dessen Inhalt nicht durch kontingente, tradierte Moralvorstellungen, sondern durch den Schutz individueller Selbstbestimmung getragen wird. Die Kriterien der zweistufigen Prüfung sind daher insoweit erfüllt.

---

klauseln *Auer*, Materialisierung, Flexibilisierung, Richterfreiheit, 2005, 42 ff., zu § 138 Abs. 1 BGB ebd., 116 ff.

[895] Siehe etwa die (mittlerweile freilich überholte) Entscheidung des BGH zur Sittenwidrigkeit des Verkaufs von Präservativen aus Warenautomaten in der Öffentlichkeit, BGH NJW 1959, 1092.

[896] Siehe nur *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 1, 57 ff.; *Sack*, NJW 1985, 761 (767 f.); *Wagner*, JZ 2017, 522 (524); *Sack/Fischinger*, in: Staudinger, BGB, 2017, § 138 Rn. 722 ff.; früh bereits *Rother*, AcP 172 (1972), 498 (502 ff.); vgl. auch *Ohly*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, 2002, 412.

[897] Zu Fallgruppen im deutschen Recht, siehe *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 68 ff.; vgl. auch *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, § 826 Rn. 19–21, freilich zu § 826 BGB.

[898] Siehe nochmals die Nachweise oben, § 5, Fn. 891.

[899] *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, § 826 Rn. 21.

b) Tatbestand der Sittenwidrigkeit: Wucherähnliches Geschäft

§ 138 Abs. 1 BGB ist demnach jedenfalls für die hier besonders interessierende Frage der Kontrolle des Äquivalenzverhältnisses neben der DS-GVO anwendbar. Auf diese dogmatisch wie auch praktisch besonders prägnante Problematik einer datenbasierten *laesio enormis* sollen sich die folgenden Ausführungen auch beschränken. Das römisch- und gemeinrechtliche Institut der *laesio enormis* sah eine objektiv-rechtliche[900] Kontrolle des Äquivalenzverhältnisses unter Verzicht auf subjektive Merkmale vor, nach welcher der Verkäufer zur Vertragsaufhebung berechtigt war, wenn der Kaufpreis den Grundstückswert um mehr als die Hälfte unterschritt.[901] Die *laesio enormis* wurde in der Folge auch zugunsten des Käufers angewandt sowie auf andere Vertragstypen erstreckt.[902] Das BGB freilich hat ihr grundsätzlich eine Absage erteilt.[903] Die Äquivalenzkontrolle nach dem BGB ist auf schwere Äquivalenzstörungen beschränkt[904] und erfordert grundsätzlich ein subjektives Element.[905] Der BGH nimmt in ständiger Rechtsprechung an, dass Rechtsgeschäfte wegen Sittenwidrigkeit unwirksam sind, wenn sie den Tatbestand des wucherähnlichen Geschäfts im Rahmen von § 138 Abs. 1 BGB erfüllen.[906] Dafür müssen zunächst Leistung und Gegenleistung in einem auffälligen Missverhältnis stehen.[907] Zudem muss nach der Rechtsprechung ein objektives oder ein subjektives Element hinzutreten.[908] Dieses subjektive Element kann insbesondere in einer verwerflichen Gesinnung bestehen, die bei einer bewussten Ausnutzung der wirtschaftlich schwächeren Position des Vertragspartners oder bei leichtfertigem Verschließen vor dieser Erkenntnis angenom-

[900] Zu einzelnen subjektiven Voraussetzungen seit dem Mittelalter, siehe *Becker*, Die Lehre von der laesio enormis in der Sicht der heutigen Wucherproblematik, 1993, 83 ff.

[901] *Becker*, Die Lehre von der laesio enormis in der Sicht der heutigen Wucherproblematik, 1993, 2, 10 ff.; *Zimmermann*, Richterliches Moderationsrecht oder Totalnichtigkeit?, 1979, 135 ff.; *Koch*, in: Festschrift Kanzleiter, 2010, 237 (237 ff.); *Mayer-Maly*, in: Festschrift Larenz, 1983, 395 (395 ff.); *Schäfer*, JuS 2009, 237 (238 f., 241 f.).

[902] *Becker*, Die Lehre von der laesio enormis in der Sicht der heutigen Wucherproblematik, 1993, 61 ff.; *Zimmermann*, Richterliches Moderationsrecht oder Totalnichtigkeit?, 1979, 138 f.; *Koch*, in: Festschrift Kanzleiter, 2010, 237 (239 f.).

[903] *Mugdan*, Die gesammten Materialien zum Bürgerlichen Gesetzbuch für das Deutsche Reich, Band 2, 1899, 178; Mot. II, 321; BGH NJW 1981, 1206; *Lorenz*, LMK 2012, 332201; *Flume*, ZIP 2001, 1621 (1622); *Zimmermann*, Richterliches Moderationsrecht oder Totalnichtigkeit?, 1979, 141; *Koch*, in: Festschrift Kanzleiter, 2010, 237 (244 f.); *Sack/Fischinger*, in: Staudinger, BGB, 2017, § 138 Rn. 138; *Schäfer*, JuS 2009, 237 (238); *Kessler*, BB 1981, 931 (932).

[904] *Metzger*, AcP 216 (2016), 817 (843 f.); *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 112; siehe auch *Rittner*, AcP 188 (1988), 101 (128).

[905] BGH NJW 1981, 1206.

[906] *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 113.

[907] BGH NJW-RR 2017, 1261 Rn. 10; BGH NJW-RR 2016, 692 Rn. 7; BGH NJW-RR 2011, 880 Rn. 13.

[908] BGH NJW-RR 2017, 1261 Rn. 10; BGH NJW-RR 2016, 692 Rn. 7; BGH NJW-RR 2011, 880 Rn. 13.

men wird.[909] Bei einem besonders groben Missverhältnis besteht ferner eine tatsächliche Vermutung, dass die subjektive Komponente des wucherähnlichen Geschäfts erfüllt ist,[910] wodurch sich die Rechtsprechung der objektivrechtlichen *laesio enormis* wieder annähert.[911]

Letztlich wird man jedoch bei der Kontrolle des Äquivalenzverhältnisses im Rahmen von datenbasierten Austauschverhältnissen auf eine subjektive Komponente in Form einer verwerflichen Gesinnung verzichten müssen. Denn Grund für die Äquivalenzkontrolle ist jedenfalls in diesen Fällen nicht eine besondere Verwerflichkeit des Handelns des Anbieters, sondern das auf rationaler Ignoranz und der Unklarheit des Preissignals fußende Marktversagen,[912] infolgedessen die Angemessenheit des Verhältnisses von Preis und Leistung nicht notwendig effizient durch das Marktgleichgewicht bestimmt wird.[913] Das subjektive Element der Sittenwidrigkeit soll beim wucherähnlichen Geschäft eine objektive Preiskontrolle durch die Gerichte verhindern,[914] wie sie im datenbasierten Austauschbereich jedoch, in Maßen, gerade angezeigt ist. Die Verzichtbarkeit des Kriteriums der verwerflichen Gesinnung, das ohnehin in Rechtsprechung und Literatur auf erheblichen Widerstand trifft,[915] zeigt sich denn auch darin, dass die Kontrolle des Äquivalenzverhältnisses funktional Ausfluss der durch die Klauselrichtlinie vorgezeichneten AGB-Kontrolle ist, die hier ausnahmsweise auch das Preis-/Leistungsverhältnis umfasst.[916] Der AGB-Kontrolle ist jedoch ein Verwerflichkeitskriterium fremd.[917] In richtlinienkonformer Auslegung muss dies daher auch für die Äquivalenzkontrolle datenbasierter Austauschprozesse im Rahmen von § 138 Abs. 1 BGB gelten.

---

[909] BGH NJW-RR 2016, 692 Rn. 7; BGH NJW-RR 2011, 880 Rn. 13; enger noch (verwerfliche Gesinnung unerlässlich) BGH NJW 2010, 363 Rn. 10.

[910] BGH NJW-RR 2016, 692 Rn. 7; BGH NJW-RR 2011, 880 Rn. 13; BGH NJW 2010, 363 Rn. 12; BGH NJW 2004, 2671 (2673); BGH NJW 2004, 3553 (3555); BGH NJW 2002, 3165 (3166).

[911] Für eine weitgehende Übereinstimmung *Flume*, ZIP 2001, 1621 (1622); Annäherung auch konstatiert bei *Schäfer*, JuS 2009, 237 (239); *Majer*, DNotZ 2013, 644 (648); *Fornasier*, Freier Markt und zwingendes Vertragsrecht, 2013, 135; die Differenzen betonend BGH NJW 2002, 3165 (3166); *Lorenz*, LMK 2012, 332201; *Mayer-Maly*, in: Festschrift Larenz, 1983, 395 (407); kritisch zu Tendenzen zur Rückkehr zur *laesio enormis Koziol*, AcP 188 (1988), 183 (185); *Koch*, in: Festschrift Kanzleiter, 2010, 237 (245 f.).

[912] Siehe oben, Text bei § 5, Fn. 686.

[913] Siehe bereits *Hacker*, ZfPW 2019, 148 (193).

[914] Deutlich BGH NJW 1981, 1206; *Koziol*, AcP 188 (1988), 183 (193).

[915] Gegen die Notwendigkeit einer verwerflichen Gesinnung BGH NJW 1985, 2405 (2406); OLG Stuttgart, NJW 1979, 2409 (2410); *Eckert*, AcP 199 (1999), 337 (350 f.); *Lindacher*, AcP 173 (1973), 124 (126); *Sack*, NJW 1985, 761 (765); *Flume*, AT II, 4. Aufl. 1992, 373; *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 117; *Sack/Fischinger*, in: Staudinger, BGB, 2017, § 138 Rn. 147; *Hefermehl*, in: Soergel, BGB, 13. Aufl. 1999, § 138 Rn. 31, 33; *Looschelders/Olzen*, in: Staudinger, BGB, 2015, § 242 Rn. 464; *Mayer-Maly*, in: Festschrift Larenz, 1983, 395 (408); *Hackl*, BB 1977, 1412 (1415); *Majer*, DNotZ 2013, 644 (649); siehe auch Mot. I, 211.

[916] Siehe oben, § 5 C.II.1.e)aa)(3)(b).

[917] Vgl. *Becker*, Der unfaire Vertrag, 2003, 10.

Dies impliziert zugleich, dass der *Aziz*-Test auch für die Kontrolle des Äquivalenzverhältnisses Geltung beanspruchen kann.[918] Der BGH geht bislang davon aus, dass das auffällige Missverhältnis unter Rekurs auf den Marktwert der jeweiligen Leistungen bestimmt werden kann. Überschreitet der Marktwert der einen Leistung den der anderen um etwa 100 %, so indiziert dies ein besonders grobes Missverhältnis.[919] Fällt die Differenz geringer aus, so kann ein auffälliges Missverhältnis vorliegen, wobei jedoch noch weitere Umstände hinzutreten müssen.[920] In der Tat wird man sagen können, dass eine Gegenleistung, die über dem Doppelten des Marktwerts der Leistung liegt, auch bei individuellen, fairen Vertragsverhandlungen mit einem informierten Nutzer mit großer Sicherheit nicht vereinbart worden wäre, sofern nicht besondere Umstände für eine Akzeptanz dieser Austauschbedingungen sprechen.[921] Bei einer geringeren Differenz nimmt die Konfidenz hinsichtlich des Fehlschlagens des *Aziz*-Tests ab, sodass in der Tat andere Umstände, die für den Anbieter erkennbar sind, hinzutreten müssen. Insofern lässt sich die Rechtsprechung des BGH mit den unionsrechtlichen Vorgaben durchaus in Einklang bringen.

Problematisch ist jedoch, dass sowohl hinsichtlich einer Einwilligung als auch hinsichtlich Vertragsklauseln der Marktwert von Leistung und Gegenleistung regelmäßig äußerst schwer zu bestimmen sein wird.[922] Schon aus diesem Grund ist hinsichtlich der Äquivalenzkontrolle Zurückhaltung angebracht.[923] Ein präziser *iustum pretium*[924] wird sich bei datenbasierter Zahlung noch schwerer als bei monetärem Entgelt festlegen lassen, da hier auch die Bewertung der Gegenleistung unsicher ist. Hinzu kommt, dass die genann-

---

[918] Zum *Aziz*-Test ausführlich oben, § 6 BII.1.e)bb)(3)(b).

[919] BGH NJW-RR 2017, 1261 Rn. 10; BGH NJW-RR 2016, 692 Rn. 7; BGH NJW 2004, 3553 (3554); für Grundstücksgeschäfte BGH NJW-RR 2011, 880 Rn. 16; BGH NJW 2010, 363 Rn. 12; für Darlehensveträgen (dort auffällliges Missverhältnis genannt, aber in der Sache wie ein besonders grobes Missverhältnis behandelt), wenn der effektive Vertragszins den marktüblichen Effektivzins relativ um etwa 100 % oder absolut um 12 Prozentpunkte überschreitet, BGH NJW 2017, 1018 Rn. 34; BGH NJW-RR 2012, 416 Rn. 10; BGH NJW 1988, 1659 (1660).

[920] BGH NJW-RR 2017, 1261 Rn. 10; *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 115.

[921] Die flexible Berücksichtigung der Umstände mahnen denn auch praktisch alle heutigen Autoren an, siehe etwa *Hackl*, BB 1977, 1412 (1413); *Bender*, NJW 1980, 1129 (1133 f.); *Majer*, DNotZ 2013, 644 (650 ff.); *Mayer-Maly*, in: Festschrift Larenz, 1983, 395 (407 f.); *Sack/Fischinger*, in: Staudinger, BGB, 2017, § 138 Rn. 309.

[922] *Hacker*, ZfPW 2019, 148 (193).

[923] So allgemein auch auch *Rittner*, AcP 188 (1988), 101 (128); *Canaris*, ZIP 1980, 709 (714); für datenbasierte Gegenleistungen *Metzger*, AcP 216 (2016), 817 (844) (Beschränkung auf „Extremfälle").

[924] Zur Schwierigkeit der Bestimmung, aus dem breiten Schrifttum, *Rittner*, AcP 188 (1988), 101 (128); *Sack/Fischinger*, in: Staudinger, BGB, 2017, § 138 Rn. 309; *Flume*, AT II, 4. Aufl. 1992, 389; zu Geschichte und Begriff *Becker*, Die Lehre von der laesio enormis in der Sicht der heutigen Wucherproblematik, 1993, 27 ff.; *Zimmermann*, The Law of Obligations, 1990, 255 ff.; *Koch*, in: Festschrift Kanzleiter, 2010, 237 (241); *Bartholomeyczik*, AcP 166 (1966), 30 (39 ff.).

ten Gründe für das Marktversagen eine wirksame Selbstbestimmung des Nutzers zwar erschweren, jedoch nicht gänzlich unmöglich machen. Auch der Respekt vor der privatautonomen Gestaltung von Rechtsverhältnissen gebietet es daher, die Äquivalenzkontrolle auf eine Datenexzesskontrolle zu beschränken, die greift, wenn die überlassenen oder durch die Einwilligung umfassten Daten zu der Leistung des Anbieters außerhalb jedes vernünftigen Verhältnisses liegen.[925] Dies muss im Einzelnen wiederum für die Einwilligung und den die Datenverarbeitung legitimierenden Vertrag getrennt operationalisiert werden.

aa) Einwilligung

Die betroffenen Personen haben infolge der in § 3 beschriebenen Typen von Marktversagen erhebliche Schwierigkeiten, eine rationale und informierte Entscheidung hinsichtlich der Abgabe der Einwilligungserklärung zu treffen. Dies legitimiert eine regulatorische Kontrolle der Einwilligung dahingehend, ob zwischen den von der Erklärung umfassten Daten und der Leistung des Anbieters ein auffälliges Missverhältnis besteht. Auf einer ersten Stufe kann hier der Versuch unternommen werden, den Marktwert der Leistung des Anbieters einerseits und der von der Einwilligung umfassten Daten andererseits zu bestimmen.[926] Dies wird jedoch regelmäßig lediglich approximativ möglich sein.

(1) Der unsichere Marktwert von Leistung und Gegenleistung

Hinsichtlich der Leistung des Anbieters kann, wie beim kartellrechtlichen Vergleichsmarktkonzept,[927] auf Preise zurückgegriffen werden, welche Wettbewerber des Anbieters verlangen.[928] Häufig wird es jedoch entweder an einem wirksamen Wettbewerb auf dem Markt fehlen, sodass die monetären Preise verzerrt sind,[929] oder die Wettbewerber verlangen ebenfalls keine monetäre, sondern lediglich eine datenbasierte Zahlung, so dass ohnehin kein monetärer Referenzwert vorliegt. Dieses Problem würde entschärft, wenn der Anbieter selbst eine datenschonende, monetär finanzierte Alternative anbieten würde oder müsste. Dies ist jedoch gegenwärtig in der Regel nicht der Fall.

Wie in § 3 eingehend beschrieben,[930] ist jedoch insbesondere die Bewertung der personenbezogenen Daten mit erheblicher Unsicherheit behaftet.[931] Die

[925] *Hacker*, ZfPW 2019, 148 (194).

[926] Zur Bedeutung des Martkwerts bei der Bestimmung des auffälligen Missverhältnisses *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 112.

[927] Dazu *Fuchs*, in: Immenga/Mestmäcker, Wettbewerbsrecht, 6. Aufl. 2019, Art. 102 AEUV Rn. 180 ff.; *Fuchs/Möschel*, in: Immenga/Mestmäcker, Wettbewerbsrecht, 5. Aufl. 2014, § 19 GWB Rn. 259 ff.

[928] Vgl. für Grundstücksgeschäfte BGH NJW 2004, 2671 (2672).

[929] *Fuchs/Möschel*, in: Immenga/Mestmäcker, Wettbewerbsrecht, 5. Aufl. 2014, § 19 GWB Rn. 270.

[930] § 3 B.II.1.d).

[931] Siehe insbesondere auch *OECD*, Exploring the Economics of Personal Data: A Sur-

verschiedenen, für eine Bewertung vorgeschlagenen ökonomischen Modelle differieren zum Teil stark in ihren Ergebnissen und können daher bestenfalls sehr grobe Annäherungen darstellen. Insgesamt wird es daher in den meisten Fällen äußerst schwierig sein, ein hinreichend gesichertes numerisches Verhältnis des Marktwerts von Leistung und Gegenleistung zu etablieren.

(2) Qualitative Abwägung

In dieser Situation muss auf qualitative Kriterien zurückgegriffen werden. Der BGH stellt hier eine Gesamtwürdigung an,[932] die insbesondere die für die jeweiligen Parteien relevanten Risiken berücksichtigt.[933] Nach hier vertretener Auffassung kann im Rahmen datenbasierter Geschäftsmodelle, bei denen Art. 4 Abs. 2 der Klauselrichtlinie teleologisch reduziert wird, methodisch vorrangig auf den *Aziz*-Test zurückgegriffen werden. Zu fragen ist also danach, ob in individuellen, fairen Verhandlungen mit einem Referenzakteur Leistung und Gegenleistung mit hinreichender Sicherheit so nicht vereinbart worden wären. Auch wenn dies letztlich eine Frage der jeweiligen speziellen Leistungsbestimmungen ist, so lassen sich einige allgemeine Richtlinien angeben und dadurch zwei Fallgruppen unterscheiden.[934]

(a) Bestimmbarer Marktwert der Anbieterleistung

Die erste Fallgruppe setzt voraus, dass der Marktwert der Anbieterleistung bestimmt oder klar bestimmbar ist. Dies kann der Fall sein, wenn das Vergleichsmarktkonzept hinreichend eindeutige Ergebnisse liefert. Besonders klar bestimmt ist die Anbieterleistung beim Rabattmodell. Sie entspricht hier der Höhe der monetären Rabattierung (sofern nicht noch weitere geldwerte Vorteile hinzutreten).

Von einem groben Missverhältnis kann dann ausgegangen werden, wenn Daten in einem Umfang und zu Zwecken überlassen werden, die auch unter Berücksichtigung der in § 3 dargestellten datenschutzrechtlichen Risiken zu dem Marktwert der Gegenleistung völlig außer Verhältnis stehen. Denn dann schlägt regelmäßig auch der *Aziz*-Test fehl. Zu berücksichtigen ist hier insbesondere, in welchem Umfang Nutzerdaten erhoben werden;[935] ob sensible Daten betroffen sind;[936] ob eine Datenweiterleitung ins EU-Ausland vorgenommen wird; inwiefern die Erhebung und Weiterverwendung der Daten transparent gestaltet oder verschleiert wird; und ob der Widerruf der Einwil-

vey of Methodologies for Measuring Monetary Value, 2013; *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen).

932 BGH NJW 1983, 2817 (2818).

933 BGH NJW-RR 2017, 1261 Rn. 13 f.; dem folgend *Hacker*, ZfPW 2019, 148 (194).

934 So auch *Hacker*, ZfPW 2019, 148 (194).

935 *Metzger*, AcP 216 (2016), 817 (843); vgl. auch KG ZD 2014, 412 (420).

936 Siehe zu den folgenden Kriterien auch *Hacker*, ZfPW 2019, 148 (194).

ligung in einfacher Weise möglich ist oder durch Transaktionskosten erschwert wird. Ein grobes Missverhältnis mag man annehmen, wenn für einen Rabatt in Höhe von wenigen Euro ein umfassendes Tracking der Lebensumstände inklusive Datenweiterleitung ins EU-Ausland vereinbart wird (zur Frage der Personalisierung des für den *Aziz*-Test relevanten Referenzakteurs sogleich, im übernächsten Abschnitt).

(b) Kein bestimmbarer Marktwert der Anbieterleistung

Ist hingegen die Leistung des Anbieters dem Marktwert nach nicht klar bestimmbar, so ist noch größere Zurückhaltung beim Verdikt der Sittenwidrigkeit angebracht. Angesichts der im Rahmen der AGB-Kontrolle und in § 3 diskutierten Formen des Marktversagens bei datenbasierten Austauschprozessen erscheint es jedoch auch aus ökonomischer Sicht nicht ratsam, eine über § 138 Abs. 1 BGB vermittelte Äquivalenzkontrolle gänzlich aufzugeben. Sinnvoll erscheint es hier, im Ansatz zwischen funktionell komplexen und funktionell begrenzten Produkten von Anbietern zu differenzieren.[937]

Bei funktionell komplexen Produkten – wie etwa sozialen Netzwerken oder anderen Plattformen, die eine Marktinfrastruktur bieten[938] – dürfte auch bei weitreichender Datenüberlassung in einer Einwilligungserklärung typischerweise nicht hinreichend sicher sein, dass der hypothetische Verhandlungstest negativ ausfallen würde. Denn der Verbraucher erhält, im Gegenzug zu seinen Daten, ein komplexes, mit erheblicher Funktionalität ausgestattetes Produkt. Es liegt nicht fern, dass die Nutzer gerade bei derartigen Produkten, die für Nutzer einen potenziell signifikanten Mehrwert bieten, von der Möglichkeit ihrer Erweiterung der Budgetrestriktionen durch die Verwendung von Daten als Zahlungsmittel Gebrauch machen wollen und in individuellen Verhandlungen hier auch weitreichende Datenüberlassungen akzeptieren würden, wenn dafür keine monetären Verpflichtungen eingegangen werden müssen.[939]

Ein auffälliges Missverhältnis wird jedoch in der Regel vorliegen, wenn die Einwilligung Daten deutlich über das funktional Erforderliche hinaus umfasst, das Produkt selbst jedoch funktionell stark begrenzt ist. Dies konturiert die zweite Fallgruppe der Sittenwidrigkeit der Einwilligung in diesem Kontext. Beispiele für funktionell beschränkte Produkte wären etwa eine Taschenlampen-App[940] oder eine App, die aus dem Fotoordner randomisiert Hinter-

[937] *Hacker*, ZfPW 2019, 148 (194).

[938] Dazu *Engert*, AcP 218 (2018) 304 (307 ff.).

[939] Diese Annahme kann allerdings durchaus empirisch widerlegt werden, wozu insbesondere Feldstudien geeignet wären; siehe aber auch Anhaltspunkte in der Vignette-Studie von *Rothmann/Buchner*, DuD 2018, 342 (345); zu deren begrenzter Aussagekraft aber noch unten, § 6 C.II.2.c)bb).

[940] Für eine Unwirksamkeit nach AGB-Recht *Rhoen*, 5(1) Internet Policy Review 2016, 1 (7), allerdings ohne Berücksichtigung der Problematik der Kontrollfähigkeit; ähnlich *Helberger/Zuiderveen Borgesius/Reyna*, 54 Common Market Law Review 2017, 1427 (1445) („unlawful according to the provisions of contract law").

grundbilder generiert.[941] Ferner kann eine funktionale Beschränkung auch dann angenommen werden, wenn das Produkt gerade infolge der (datenbasierten) Werbefinanzierung nur noch stark eingeschränkt brauchbar ist, etwa wenn ein Text aufgrund ständiger Werbeunterbrechung nicht mehr sinnvoll zusammenhängend gelesen werden kann.

In solchen Fällen ist regelmäßig die Schwelle evidenter Diskrepanz zwischen weitreichendem Datentransfer und Werthaltigkeit des Produkts überschritten, wenn in erheblichem Umfang funktional nicht notwendige Daten von der Einwilligung umfasst sind. Damit ist hinreichend sicher, dass der hypothetische Verhandlungstest, unter Zugrundelegung eines Referenzakteurs mit mittel ausgeprägten Datenschutzpräferenzen, fehlschlägt. Die Einwilligung ist dann wegen eines auffälligen Missverhältnisses zwischen der mit ihr bewirkten Gegenleistung und der Leistung des Anbieters sittenwidrig und unwirksam – unabhängig von der Frage des Kopplungsverbots nach Art. 7 Abs. 4 DS-GVO.[942]

(c) Die Rolle des Referenzakteurs – Maßvolle Personalisierung

Allerdings ist nicht zu verkennen, dass die Implementierung einer derartigen Datenexzesskontrolle nicht allen Nutzern gerecht wird. Insbesondere Akteure mit sehr niedrigen Datenschutzpräferenzen würden womöglich in individuellen Vertragsverhandlungen einer umfangreichen Datenerhebung und -analyse zustimmen, auch wenn sie dafür lediglich einen Rabatt in Höhe von wenigen Euro oder ein funktional begrenztes Produkt ohne monetäre Zahlung erhalten. Umgekehrt liegt die für Nutzer mit stark ausgeprägten Datenschutzpräferenzen akzeptable Grenze des Datentransfers deutlich niedriger. Daher stellt sich, wie auch im Rahmen der AGB-Kontrolle, wiederum die Frage nach der Personalisierung des *Aziz*-Tests durch eine Berücksichtigung subjektiver Eigenschaften des Vertragspartners.

Im Rahmen von § 138 Abs. 1 BGB ist das Äquivalenzverhältnis, und damit auch der Wert der Daten, grundsätzlich objektiv zu bestimmen.[943] Dies bietet zum einen Rechtssicherheit und schützt den Anbieter zum anderen vor unzumutbaren Nachforschungspflichten. Beide Gründe greifen jedoch dann nicht mehr, wenn der Anbieter positive Kenntnis von der abweichenden Bewertung durch den Nutzer hat. Dies ist etwa der Fall, wenn der Anbieter die Datenschutzpräferenzen der Nutzer aktiv ermittelt, sofern diese Analyse statistisch signifikante Ergebnisse liefert. Auch in der Rechtsprechung zu Kaufverträgen ist anerkannt, dass ein rein subjektiv-emotionales Affektionsinteresse des Erwerbers bei der Gesamtwürdigung der Sittenwidrigkeit berücksichtigt wer-

[941] *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen).

[942] Siehe dazu sogleich unter § 5C.II.2.d).

[943] BGH NJW-RR 2017, 1261 Rn. 10; BGH NJW-RR 2011, 880 Rn. 13; BGH NJW 2004, 3553 (3554); *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 113.

den kann.[944] Damit werden subjektive Präferenzen relevant gemacht, wenngleich diese sich beim Affektionsinteresse auf das angebotene Produkt und nicht, wie bei einer datenbasierten Zahlung, auf den Inhalt der Gegenleistung richten. Dies kann jedoch letztlich nicht entscheidend sein, da der Grund für die Berücksichtigung des Affektionsinteresses darin liegt, dass dem Erwerber die objektive Wertdifferenz gleichgültig ist.[945] Dies ist bei niedrigen Datenschutzpräferenzen regelmäßig der Fall. Wenn jedoch subjektive Präferenzen den Anbieter entlasten können, so müssen sie auch, bei positiver Kenntnis, zu einer stärkeren Belastung führen.

Wie im Rahmen der AGB-Kontrolle wird man daher in diesem Fall eine maßvolle Personalisierung der Abwägung vornehmen können.[946] Diese kann zugunsten, aber auch zulasten des Anbieters ausfallen. Man wird jedoch auch bei Nutzern mit bekanntermaßen stark ausgeprägten Datenschutzpräferenzen nicht vorschnell ein grobes Missverhältnis annehmen können. Denn gerade diesen Nutzern ist regelmäßig auch bewusst, dass sie bei monetär kostenloser Leistung mit ihren Daten zahlen.[947] Daher wird man auch bei ihnen nicht ohne Weiteres annehmen können, dass sie gerade infolge der Wertdifferenz zwischen ihren Daten und der angebotenen Leistung oder wegen üblicher datenschutzrechtlicher Risiken das Leistungspaket abgelehnt hätten.

Konsequenz der Personalisierung des *Aziz*-Tests ist, dass der Anbieter, will er eine maximal legitimierende Einwilligung erhalten, Sorge tragen muss, den Umfang der von der Einwilligung erfassten Daten den durch Datenanalyse ermittelten Datenschutzpräferenzen anzupassen. Probabilistische Fehlzuordnungen eines Nutzers zu einer Gruppe mit bestimmten Datenschutzpräferenzen gehen allerdings, bei einem insgesamt hinreichend belastbaren Analysemodell, nicht zulasten des Anbieters, da der *Aziz*-Test danach fragt, ob der Anbieter bei eigenem loyalem Verhalten *erwarten* durfte, dass der Nutzer zustimmt.[948]

Insgesamt wird der Anbieter durch diese personalisierte Äquivalenzkontrolle auch nicht über Gebühr belastet. Denn insofern dürfte es ausreichend sein, drei verschiedene Einwilligungserklärungen (für niedrig, mittel und stark ausgeprägte Datenschutzpräferenzen) zu erstellen; auch darauf kann der An-

---

[944] BGH NJW-RR 2003, 558 (559): Berücksichtigung des Affektions- und Spekulationsinteresses an einem Turnierpferd im Rahmen des subjektiven Tatbestands zugunsten des sittenwidrig Handelnden; BGH NJW 2000, 1254 (1255): Berücksichtigung des Affektionswertes bei der Ermittlung des für den Marktwert relevanten Marktes (Sammlermünzen); *Majer*, DNotZ 2013, 644 (645).

[945] BGH NJW 2007, 2841 (2842); siehe auch BGH NJW 2001, 1127 (1129).

[946] Siehe oben, § 5 C.II.1.e)bb)(3)(b)(bb).

[947] Vgl. *DIVSI*, Daten – Ware und Währung, 2014, 15; der konkrete Umfang der Datenerhebung ist den Nutzern jedoch häufig nicht bewusst, siehe *Rothmann/Buchner*, DuD 2018, 342 (345).

[948] EuGH, Urt. v. 14.3.2013 – Rs. C-415/11 (*Aziz*) – Rn. 69.

bieter verzichten, wenn er lediglich die am wenigsten weitreichende Erklärung verwendet. Vor allem jedoch greift die Personalisierung nur, wenn der Anbieter eine auf Datenschutzpräferenzen bezogene Datenanalyse betreibt. Davon ist jedoch nur auszugehen, wenn diese Analyse mit einem positiven Erwartungsnutzen für den Anbieter verbunden ist. Dann erscheint es jedoch sachgerecht, dass der Anbieter nicht lediglich einseitig von der Analyse profitieren kann, sondern deren Inhalt auch bei der Ausgestaltung des Rechtsverhältnisses mit dem Nutzer berücksichtigen muss. Einmal mehr gilt insoweit: *qui habet commoda ferre debet onera*.[949]

bb) Vertrag

In der Sache genauso wie die Einwilligung sind Vertragsklauseln zu beurteilen, die einerseits eine Leistung und andererseits eine datenbasierte Gegenleistung, sei es in Form der Abgabe einer Einwilligung oder der Datenüberlassung, festlegen. Sofern die Abgabe einer Einwilligung Gegenstand der Verpflichtung oder Bedingung ist, muss sich die Kontrolle am Inhalt der Einwilligung orientieren, sodass das soeben dazu Gesagte gilt. Sofern die Datenüberlassung selbst Gegenstand der Klausel ist, ist ebenfalls wiederum zwischen funktional begrenzten und funktional komplexen Produkten zu unterscheiden. Auch hinsichtlich der Vertragsbedingungen beschränkt sich die Äquivalenzkontrolle daher auf eine Datenexzesskontrolle.

cc) Ergebnis zum wucherähnlichen Geschäft

Damit implementiert § 138 Abs. 1 BGB eine Datenexzesskontrolle, die grundsätzlich auf Produkte mit niedrigem Marktwert oder funktional deutlich limitierte Produkte begrenzt ist. Damit wird eine maßvolle Äquivalenzkontrolle installiert, die angesichts der in § 3 diskutierten Formen von Marktversagen bei datenbasierten Austauschverhältnissen angezeigt erscheint. Der im Rahmen des *Aziz*-Tests relevante Referenzakteur kann bei positiver Kenntnis des Anbieters von den Datenschutzpräferenzen personalisiert werden. So lässt sich insgesamt ein schonender Ausgleich zwischen den, im Rahmen von § 138 Abs. 1 BGB regelmäßig zumindest im Wege der mittelbaren Drittwirkung[950] zu berücksichtigenden,[951] Grundrechtspositionen der Beteiligten (insbesondere dem Datenschutzgrundrecht, Art. 8 GRCh, einerseits und dem Recht auf unternehmerische Freiheit, Art. 16 GRCh, andererseits) erzielen.[952]

[949] Zu diesem Rechtssatz bereits oben, § 4, Fn. 250.
[950] Siehe genauer unten, Text bei und Nachweise in § 5, Fn. 1074 ff.
[951] *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 20.
[952] Vgl. auch *Metzger*, AcP 216 (2016), 817 (843).

c) Rechtsfolge

Die Rechtsfolge der Sittenwidrigkeit beschränkt sich nicht auf eine Gesamtnichtigkeit des Vertrags.[953] Vielmehr ist nach herrschender Meinung anerkannt, dass nach dem Sinn und Zweck der Vorschrift auch eine Beschränkung der Nichtigkeitsfolge in zeitlicher,[954] preislicher[955] oder persönlicher Hinsicht[956] zumindest in Betracht kommt.[957] Daher wird man im Ergebnis und auch in der Begründung wie bei § 306 BGB entscheiden können.[958]

Grundsätzlich ist daher bei Sittenwidrigkeit infolge eines auffälligen Missverhältnisses der gesamte Vertrag unwirksam, ein Wertersatzanspruch des Anbieters nach § 817 S. 2 BGB gesperrt. Gerade bei Sittenwidrigkeit einer Entgeltregelung ist nach der Rechtsprechung in der Regel von einer Gesamtnichtigkeit auszugehen.[959] Anders ist jedoch zu entscheiden, wenn der Nutzer signifikant vorgeleistet hat:[960] In diesem Fall bleibt der Vertrag in teleologischer Reduktion der Nichtigkeitsfolge des § 138 Abs. 1 BGB partiell wirksam, so dass der Nutzer in den Genuss einer seiner Vorleistung entsprechenden Leistung kommen kann.

Auch bei Unwirksamkeit der Einwilligung mag es wiederum über den Mechanismus der Geschäftsgrundlage zu einer Anpassung oder Kündigung des Vertrags kommen, da auch insoweit bei infolge der Unwirksamkeit der Einwilligung datenschutzrechtswidrigen Datenverarbeitungen die Sanktionen der DS-GVO greifen und eine darüberhinausgehende Anreizwirkung nicht notwendig ist.[961]

---

[953] So aber *Zimmermann*, Richterliches Moderationsrecht oder Totalnichtigkeit?, 1979, 81 ff.

[954] BGH NJW 1992, 2145 (2145 f.); BGH NJW 1972, 1459.

[955] Vgl. BGH NJW 1984, 722 (724) zum alten § 5 Abs. 1 WiStrG; siehe auch *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 161 zu Wohnraummietverhältnissen; *Sack/Fischinger*, in: Staudinger, BGB, 2017, § 138 Rn. 189.

[956] BGH NJW 1969, 1343; BGH FamRZ 1963, 287.

[957] *Sack/Fischinger*, in: Staudinger, BGB, 2017, § 138 Rn. 158 f., 323; *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 157 ff.; *Brambring*, NJW 2007, 865 (867 ff.); *H. Roth*, JZ 1989, 411 (412 f.); *Kohte*, NJW 1982, 2803 (2805); *Lindacher*, AcP 173 (1973), 124 (139 ff.); *Sandrock*, AcP 159 (1960), 481 (514 ff.).

[958] Siehe oben, § 5 C.II.1.f)cc).

[959] BGH NJW-RR 2006, 16 (18); BGH NJW 1965, 2147 (2148); zustimmend *Armbrüster*, in: MüKo, BGB, 8. Aufl. 2018, § 138 Rn. 161.

[960] Siehe auch *Helberger/Zuiderveen Borgesius/Reyna*, 54 Common Market Law Review 2017, 1427 (1449) (Reduzierung der Datenüberlassungspflicht auf erträgliches Maß); so ebenfalls *Hacker*, ZfPW 2019, 148 (195); dies kann dann angenommen werden, wenn die Sittenwidrigkeit lediglich durch einzelne, klar abgrenzbare Klauseln (z. B. Datenweiterleitung ins EU-Ausland) hervorgerufen wird und die Präventionsfunktion durch die Sanktionen der DS-GVO gewahrt wird; vgl. BGH NJW 1984, 722 (724).

[961] Siehe oben, Text bei § 5, Fn. 545 und 833.

d) Wechselwirkungen mit der DS-GVO

Auch hinsichtlich der Wechselwirkung mit der DS-GVO wird man wie bei der AGB-Kontrolle von Klauseln bzw. Einwilligungserklärungen entscheiden müssen, wenn die Sittenwidrigkeit auf dem Schutz der betroffenen Person beruht. So führt die Sittenwidrigkeit grundsätzlich dazu, dass nicht nur Art. 6 Abs. 1 lit. a bzw. b DS-GVO nicht greift, sondern auch die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO zugunsten der betroffenen Person ausfällt.[962] Die Kriterien, die bei der qualitativen Gesamtwürdigung zu berücksichtigen sind, decken sich zu großen Teilen mit jenen der datenschutzrechtlichen Interessenabwägungsklausel.[963]

Ferner ist nicht zu verkennen, dass regelmäßig neben § 138 Abs. 1 BGB auch der Tatbestand des Kopplungsverbots nach Art. 7 Abs. 4 DS-GVO erfüllt ist. Eine eigenständige Bedeutung erlangt die Äquivalenzkontrolle nach § 138 Abs. 1 BGB bei der Einwilligung jedoch dann, wenn, wie bei manchen Apps, marktbasierte Alternativen ohne Einwilligungserfordernis existieren und daher die Freiwilligkeit der Einwilligung nach hier vertretener Auffassung nicht am Kopplungsverbot scheitert.[964] Hinsichtlich die Datenverarbeitung legitimierender Verträge wiederum kompensiert § 138 Abs. 1 BGB, wie auch die AGB-Kontrolle bei weiten Leistungspflichten, den Mangel eines datenschutzrechtlichen Kopplungsverbots und anderer Schutzinstrumente in der DS-GVO. Ferner ist bei einer datenbasierten *laesio enormis* regelmäßig der Grundsatz der Datenverarbeitung nach Treu und Glauben verletzt. Auch hier gilt das im Rahmen der AGB-Kontrolle Ausgeführte entsprechend:[965] Die Sittenwidrigkeit indiziert die Verletzung von Art. 5 Abs. 1 lit. a Var. 2 DS-GVO, determiniert sie aber nicht abschließend. Daher kommt es letztlich auch bei § 138 Abs. 1 BGB zu einer Konvergenz von Datenschutzrecht und allgemeinem Vertragsrecht.

e) Zusammenfassung zu § 138 BGB

Die Sittenwidrigkeitskontrolle stellt sich bei datenbasierten Austauschverhältnissen vor allem als verlängerter Arm der AGB-Kontrolle dar und folgt daher inhaltlich wie auch in der Begründung deren Muster. Zunächst ist jedoch zu konstatieren, dass § 138 Abs. 2 BGB neben der DS-GVO nicht anwendbar ist. Hinsichtlich § 138 Abs. 1 BGB ist zu differenzieren. Die Äquivalenzkontrolle nach § 138 Abs. 1 BGB findet immer Anwendung. Andere Sittenwidrigkeitstatbestände können am Anwendungsvorrang der DS-GVO scheitern, wenn dadurch lediglich tradierte Moralvorstellungen nachvollzogen werden, was

962 *Hacker*, ZfPW 2019, 148 (195).
963 Siehe zu diesen Kriterien oben, § 4 C.I.2.c)bb).
964 Siehe oben, § 4 B.I.3.a)dd)(3)(c).
965 Siehe oben, § 5 C.II.1.g)cc).

aber nach deutschem Recht richtigerweise, insbesondere seit Inkrafttreten des ProstG, nicht mehr der Fall ist.

Die hier besonders interessierende Kontrolle des Äquivalenzverhältnisses kann als datenbasierte *laesio enormis* ausgestaltet werden. Dabei ist in subjektiver Hinsicht auf das Merkmal der verwerflichen Gesinnung zu verzichten, weil lediglich objektiv die Folgen von Marktversagen korrigiert werden müssen. Bei dem Verdikt der Sittenwidrigkeit ist jedoch starke Zurückhaltung angebracht. Die Sittenwidrigkeit ist auf eine Datenexzesskontrolle beschränkt, die greift, wenn die Datenüberlassung oder die von einer Einwilligung umfassten Daten zum Wert der Anbieterleistung völlig außer Verhältnis stehen. Zwei Fallgruppen kommen Betracht: einerseits ein sehr geringer, objektiv bestimmbarer Marktwert der Gegenleistung; und andererseits funktional stark beschränkte Produkte.

Die Rechtsfolgen und die Wechselwirkung mit der DS-GVO stellen sich wie bei der AGB-Kontrolle dar. Grundsätzlich ist der gesamte Vertrag unwirksam, es sei denn, der Nutzer hat signifikant vorgeleistet. Ferner fällt die datenschutzrechtliche Interessenabwägung in der Regel zugunsten der betroffenen Person aus; auch ist die Verletzung des Grundsatzes der Datenverarbeitung nach Treu und Glauben indiziert. Insbesondere bei Vertragsbedingungen kompensiert § 138 Abs. 1 BGB daher das Fehlen von spezifischen datenschutzrechtlichen Schutzvorschriften zur Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO.

3. § 242 BGB

Zuletzt ist denkbar, Einwilligungserklärungen oder Vertragsklauseln, die eine Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO ermöglichen sollen, nicht nur gemäß §§ 305 ff., 138 BGB, sondern auch nach § 242 BGB zu kontrollieren. Wie vielleicht keine andere Norm des deutschen Zivilrechts steht § 242 BGB für den Ausgleich von Vertragsfreiheit und Vertragsgerechtigkeit und damit für rechtsimmanente Grenzen der Privatautonomie.[966] Hinsichtlich der im Rahmen dieser Arbeit betrachteten datenbasierten Austauschprozesse kommen vor allem zwei Fallgruppen in Betracht. Zunächst ist eine spezifische Form der Inhaltskontrolle in § 242 BGB verortet. Dort hat bekanntlich auch die Inhaltskontrolle von AGB ihren Ausgang genommen.[967] Noch heute aber kennt die Rechtsprechung die erweiterte Inhaltskontrolle bestimmter Verträge nach der Generalklausel von Treu und Glauben (a)). Daneben ist denkbar, im Falle von Rechtsmissbrauch hinsichtlich der Ausübung einer datenschutzrechtlich relevanten Rechtsposition auf § 242 BGB zu rekurrieren (b)).

---

[966] Vgl. *Oechsler*, Gerechtigkeit im modernen Austauschvertrag, 1997, 199, 286 ff.; *Heinrich*, Formale Freiheit und materiale Gerechtigkeit, 2000, 392 ff., besonders 398; *Looschelders/Olzen*, in: Staudinger, BGB, 2015, § 242 Rn. 456; *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 526 f.

[967] *Canaris*, AcP 200 (2000), 273 (320); *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 532.

a) Anwendbarkeit der erweiterten Inhaltskontrolle: Dogmatik des BGB

§ 242 BGB installiert neben der AGB-Kontrolle nach §§ 305 ff. BGB und der Äquivalenzkontrolle nach § 138 Abs. 1 BGB eine weitere Form der Inhaltskontrolle von Verträgen. Das Verhältnis einer Inhaltskontrolle nach § 242 BGB zu den übrigen Schranken der Privatautonomie, insbesondere zu den bereits behandelten §§ 134, 138 BGB, ist jedoch umstritten.

Nach herrschender Meinung stellt ein Gesetzesverstoß oder ein Sittenverstoß grundsätzlich auch einen Verstoß gegen Treu und Glauben nach § 242 BGB dar.[968] Dies hat jedoch allenfalls für die Rechtsfolgen eines Gesetzes- oder Sittenverstoßes Relevanz,[969] die bereits behandelt wurden und für die im hiesigen Kontext die zusätzliche Verletzung von § 242 BGB keine abweichende Beurteilung erfordert. Zusätzliche Rahmenbedingungen für die privatautonome Gestaltung der digitalen Wirtschaft ergeben sich jedoch dann, wenn man § 242 BGB eine über die übrigen Grenzen der Privatautonomie hinausgehende Funktion bei der Inhaltskontrolle zubilligt. Teilweise wird § 242 BGB jedoch auf eine Rechtsausübungsschranke reduziert, während nach dieser Auffassung lediglich die §§ 134, 138 BGB (und, wie man hinzufügen muss, § 307 BGB) als Außenschranken die Wirksamkeit der Vertragsbedingungen selbst kontrollieren.[970] Demgegenüber vertritt jedoch die Rechtsprechung und ein erheblicher Teil der Literatur, dass auf Grundlage von § 242 BGB eine erweiterte Inhaltskontrolle geleistet werden kann.[971] Hier ist jedoch begrifflich zu differenzieren. Soweit damit eine Ausübungskontrolle angesprochen ist, etwa bei Eheverträgen zusätzlich zu § 138 Abs. 1 BGB,[972] ist dies eine Frage des Rechtsmissbrauchs im Einzelfall, der die Wirksamkeit der Klausel oder des Vertrags grundsätzlich nicht berührt (dazu unter b)).[973] § 242 BGB erlangt hingegen eigenständige Bedeutung als Wirksamkeitsschranke im Rahmen einer In-

[968] BAG NJW 1964, 1542 (1543); OLG Hamm, NJW 1981, 465 (466) (jeweils zum Sittenverstoß); *Looschelders/Olzen*, in: Staudinger, BGB, 2015, § 242 Rn. 362, 365; *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 127 f., 135; aA (Vorrang § 242 BGB vor § 138 BGB) *Becker*, Der unfaire Vertrag, 2003, 11.

[969] BGH NJW-RR 2008, 1050 Rn. 12; BGH NJW-RR 2008, 66 Rn. 18, 25 f.; BGH NJW 1983, 109 (110); BGH NJW 1981, 1439 (1440); BGH NJW 1970, 609 (610); *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 127 f.

[970] *Sutschet*, in: BeckOK, 51. Ed. 2019, § 242 Rn. 35; siehe auch *Looschelders/Olzen*, in: Staudinger, BGB, 2015, § 242 Rn. 366.

[971] *Heinrich*, Formale Freiheit und materiale Gerechtigkeit, 2000, 394, 398 f.; *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 135, 526 ff.; *Coester-Waltjen*, AcP 190 (1990), 1 (16), die allerdings nicht direkt auf § 242 BGB, sondern auf den übergeordneten Grundsatz von Treu und Glauben rekurrieren will.

[972] Die Rechtsprechung fügt hier der Wirksamkeitskontrolle nach § 138 Abs. 1 BGB in einem zweiten Schritt eine Ausübungskontrolle nach § 242 BGB hinzu, siehe nur BGH NJW 2009, 2124 Rn. 13, 15; BGH NJW 2008, 1080 Rn. 33; BGH NJW 2008, 3426 Rn. 10 f.; BGH NJW 2005, 2386 (2388); dazu auch *Becker*, Der unfaire Vertrag, 2003, 19 ff.

[973] BGH NJW 2013, 2742 Rn. 34; *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 529, 541; *Coester-Waltjen*, AcP 190 (1990), 1 (5); *Heinrich*, Formale Freiheit und materiale Gerechtigkeit, 2000, 394; siehe auch die Nachweise in § 5, Fn. 972; zur Möglichkeit der Un-

haltskontrolle, soweit eine Kontrolle nach §§ 305 ff., 138 BGB gar nicht stattfindet.[974] Allerdings sind auch hinsichtlich der insofern erweiterten Inhaltskontrolle grundsätzlich die Wertungen der §§ 134, 138, 307 BGB vorrangig.[975] Dies impliziert insbesondere, dass eine Inhaltskontrolle von Hauptleistungspflichten oder eine Äquivalenzkontrolle durch § 242 BGB grundsätzlich ausscheiden muss, da die § 307 Abs. 3 S. 1 BGB zu Grunde liegenden Erwägungen auch insofern gelten.[976] Insoweit fungiert daher lediglich § 138 BGB als Grenze.[977]

Zwar ist § 307 Abs. 3 S. 1 BGB nach hier vertretener Auffassung für datenbasierte Austauschprozesse im oben genannten Umfang teleologisch zu reduzieren.[978] Nichtsdestoweniger ist nicht ersichtlich, dass im Rahmen von § 242 BGB bei der Inhaltskontrolle Umstände zu berücksichtigen wären, die im Rahmen von § 307 BGB oder § 138 BGB nicht zum Tragen kommen könnten.[979] Auch im Verbraucherrecht besitzt die Inhaltskontrolle nach § 242 BGB anerkanntermaßen keine eigenständige Bedeutung neben den §§ 305 ff. BGB.[980] Daher scheidet eine erweiterte Inhaltskontrolle von Einwilligungserklärungen und Datenverarbeitungsklauseln bereits nach der Dogmatik des deutschen Zivilrechts aus. Sie wird allein durch die §§ 305 ff., 138 Abs. 1 BGB geleistet.

b) Anwendbarkeit bei Rechtsmissbrauch und als Ausübungskontrolle: Anwendungsvorrang der DS-GVO?

§ 242 BGB ist mithin im hier untersuchten Kontext nicht als weiterer Maßstab der Inhaltskontrolle von Belang. Relevanz kann die Norm jedoch erlangen, wenn ein Rechtsmissbrauch in Rede steht. Damit ist, im Gegensatz zur Inhaltskontrolle, die Ausübungskontrolle angesprochen, über die einzelfallbezogen die Geltendmachung einer im Übrigen wirksam eingeräumten Rechtsposition beschränkt werden kann.[981] Hier ist wiederum zwischen Einwilligungserklärungen einerseits und Vertragsbedingungen andererseits zu unterscheiden.

---

wirksamkeit einer rechtsmissbräuchlich erlangten Vereinbarung *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 80.

[974] *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 532 f.

[975] *Looschelders/Olzen*, in: Staudinger, BGB, 2015, § 242 Rn. 366; *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 127.

[976] *Looschelders/Olzen*, in: Staudinger, BGB, 2015, § 242 Rn. 472 f.

[977] *Looschelders/Olzen*, in: Staudinger, BGB, 2015, § 242 Rn. 473.

[978] Siehe oben, § 5 C.II.1.e)aa)(3)(a)(bb).

[979] Anders liegt es hinsichtlich der in § 242 BGB verwurzelten Ausübungskontrolle, siehe *Looschelders/Olzen*, in: Staudinger, BGB, 2015, § 242 Rn. 483; *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 128; dazu sogleich, unter b).

[980] *Looschelders/Olzen*, in: Staudinger, BGB, 2015, § 242 Rn. 482.

[981] Siehe bereits die Nachweise in § 5, Fn. 973.

aa) Einwilligung

Zunächst ist denkbar, dass die Erlangung einer Einwilligungserklärung (z. B. bei unredlichem Erwerb[982]) oder die Berufung auf diese (z. B. bei Verwirkung[983]) rechtsmissbräuchlich ist. Dabei würde es sich jedoch um ein treuwidriges Verhalten des datenschutzrechtlich Verantwortlichen handeln. Insofern ist zu klären, inwieweit der datenschutzrechtliche Grundsatz von Treu und Glauben nach Art. 5 Abs. 1 lit. a Var. 2 DS-GVO, an den der Verantwortliche nach Art. 5 Abs. 2 DS-GVO gebunden ist, Anwendungsvorrang vor § 242 BGB beansprucht. Davon geht ein Teil der Literatur in der Tat aus.[984] Dies erscheint jedoch bereits deshalb fraglich, weil sich der datenschutzrechtliche Grundsatz seinem Wortlaut zufolge nur auf die Verarbeitung selbst bezieht, nicht jedoch auf eine Einwilligungserklärung, welche die Datenverarbeitung legitimieren soll.[985] Nun könnte man argumentieren, dem Grundsatz nach Art. 5 Abs. 1 lit. a Var. 2 DS-GVO komme, schon wegen seiner primärrechtlichen Verankerung in Art. 8 Abs. 2 S. 1 GRCh, eine umfassende Bedeutung für die DS-GVO zu, die sich nicht in einer engen Fokussierung auf die Verarbeitung selbst erschöpfen könne.[986] Nach hier vertretener Auffassung wird man dennoch zwischen der Datenverarbeitung einerseits (für die allein Art. 5 Abs. 1 lit. a Var. 2 DS-GVO gilt) und der dieser zugrunde liegenden Einwilligungserklärung andererseits differenzieren müssen.

Hinsichtlich der Erlangung oder Berufung auf die Einwilligungserklärung selbst gilt demnach der datenschutzrechtliche Grundsatz von Treu und Glauben nicht. Denn dies hätte andernfalls zur Folge, dass bereits die rechtsmissbräuchliche Berufung auf die Einwilligung eine Verletzung von Art. 5 Abs. 1 lit. a Var. 2 DS-GVO konstituieren und die Sanktionen nach Art. 83 Abs. 5 lit. a DS-GVO auslösen würde, ohne dass es überhaupt zu einer Datenverarbeitung gekommen wäre. Dies erscheint jedoch mit dem Wortlaut von Art. 5 Abs. 1 lit. a Var. 2 DS-GVO und auch dem Sanktionszweck von Art. 83 DS-GVO nicht mehr vereinbar.

---

[982] Siehe dazu etwa *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 256 ff.; *Sutschet*, in: BeckOK, 51. Ed. 2019, § 242 Rn. 58 ff.

[983] Siehe dazu etwa *Heinrich*, Formale Freiheit und materiale Gerechtigkeit, 2000, 410 ff.; *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 369 ff.; *Sutschet*, in: BeckOK, 51. Ed. 2019, § 242 Rn. 137 ff.

[984] *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 83.

[985] Vgl. *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 45, 47; *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 17 (jeweils Fairness/Treuwidrigkeit „der Verarbeitung").

[986] Grundsätzlich für eine umfassende Bedeutung des Grundsatzes der Datenverarbeitung von Treu und Glauben *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130; für eine Erstreckung des Datenschutzrechts *de lege ferenda* auf *chilling*-Effekte, die ohne eigentliche Datenverarbeitung auftreten, auch *Hallinan*, 5 European Data Protection Law Review 2019, 293.

Auch in teleologischer Hinsicht ist eine analoge Anwendung von Art. 5 Abs. 1 lit. a Var. 2 DS-GVO auf die Einwilligung nicht geboten. Denn es besteht schon keine Regelungslücke: Das Unionsrecht kennt nach zutreffender Ansicht eine eigene Kategorie des Rechtsmissbrauchs, die sich aus dem allgemeinen, unionsrechtlichen Grundsatz von Treu und Glauben[987] ergibt[988] und die Berufung auf spezifische, unionsrechtlich konstituierte Rechtspositionen („Rechte […] auf Grundlage des Gemeinschaftsrechts“[989]) verhindert. Den Rechtsmissbrauch hat der EuGH in einer Reihe von Urteilen immer wieder als immanente Schranke von unionsrechtlichen Rechtspositionen herangezogen.[990] Insofern erscheint es gerechtfertigt, auch hinsichtlich der aus einer Einwilligungserklärung resultierenden Rechtsposition den unionsrechtlichen Einwand des Rechtsmissbrauchs zuzulassen. Immerhin sind die Wirksamkeitsvoraussetzungen der Einwilligung jedenfalls grundsätzlich in der DS-GVO festgehalten, so dass man von einem unionsrechtlich konstituierten Recht auszugehen hat. Dies hat ferner den Vorzug, dass insofern eine Harmonisierung der Voraussetzungen, unter denen der Einwilligung wegen Rechtsmissbrauchs die Legitimierungswirkung versagt bleibt, erreicht werden kann. Denn insofern ist der Rückgriff auf § 242 BGB, soweit danach andere Ergebnisse erzielt würden, durch den Anwendungsvorrang des Unionsrechts begrenzt.

---

[987] Grundlegend, wenngleich sibyllinisch, EuGH, Urt. v. 3.9.2009 – Rs. C-489/07 (*Messner*) – Rn. 26; zu diesem Grundsatz umfassend und seine Existenz bejahend *Stempel*, Treu und Glauben im Unionsprivatrecht, 2016, besonders 268 ff., 310 f.; bejahend ferner *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 398, 401; *Wulfers*, GPR 2006, 106 (109); *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, 348 f.; *Faust*, JuS 2009, 1049 (1052); ebenso, für den Grundsatz des Rechtsmissbrauchs, *Schmidt-Kessel*, Jahrbuch junger Zivilrechtswissenschaftler 2000, 61 (79 f.); zweifelnd noch *Stempel*, ZEuP 2010, 925 (933 f.); einen unionsrechtlichen Grundsatz von Treu und Glauben ablehnend *Stürner*, in: Schulte-Nölke et al. (Hrsg.), Der Entwurf für ein optionales europäisches Kaufrecht, 2012, 47 (81 f.); *Hesselink*, in: Leczykiewicz/Weatherill (Hrsg.), The Involvement of EU Law in Private Law Relationships, 2013, 131 (171); *Hahn*, jurisPR-SteuerR 15/2006 Anm. 1, unter B.2.; kritisch auch *Miller*, The Emergence of EU Contract Law: Exploring Europeanization, 2011, 43 f.; ablehnend hinsichtlich der Missbrauchsdoktrin generell, auch im nationalen Recht, *Gambaro*, 4 European Review of Private Law 1995, 561.

[988] *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 399; siehe auch *Schmidt-Kessel*, Jahrbuch junger Zivilrechtswissenschaftler 2000, 61 (79 f.).

[989] EuGH, Urt. v. 12.3.1996 – Rs. C-441/93 (*Pafitis*) – Rn. 69; siehe auch EuGH, Urt. v. 12.5.1998 – Rs. C-367/96 (*Kefalas*) – Rn. 20; Urt. v. 23.3.2000 – Rs. C-373/97 (*Diamantis*) – Rn. 33 (Berufung „auf Gemeinschaftsrecht“).

[990] Zum allgemeinen Gesellschaftsrecht EuGH, Urt. v. 12.3.1996 – Rs. C-441/93 (*Pafitis*) – Rn. 69; Urt. v. 12.5.1998 – Rs. C-367/96 (*Kefalas*) – Rn. 20; Urt. v. 23.3.2000 – Rs. C-373/97 (*Diamantis*) – Rn. 33; zur Diensleistungsfreiheit EuGH, Urt. v. 3.12.1974 – Rs. 33/74 (*Van Binsbergen*) – Rn. 13; Urt. v. 5.10.1994 – Rs. C-23/93 (*TV10*) – Rn. 21; zur Niederlassungsfreiheit EuGH, Urt. 9.3.1999 – Rs. C-212/97 (*Centros*) – Rn. 24; zum freien Warenverkehr EuGH, Urt. v. 10.1.1985 – Rs. 229/83 (*Leclerc u. a.*) – Rn. 27; zur Arbeitnehmerfreizügigkeit EuGH, Urt. v. 21.6.1988 – Rs. 39/86 (*Lair*) – Rn. 43; zur Lohnfortzahlung EuGH, Urt. v. 2.5.1996 – Rs. C-206/94 (*Paletta*) – Rn. 24.

In der Rechtssache *Kefalas* hatte der EuGH zwar den Rückgriff auf das nationale Verbot des Rechtsmissbrauchs im harmonisierten Bereich zugelassen, dies jedoch nur deshalb, weil das Unionsrecht gleichfalls diesen Grundsatz kennt.[991] Der EuGH machte ferner in einer Reihe von Rechtssachen klare Vorgaben, welche Auslegung des nationalen Rechtsmissbrauchsverbots mit dem unionsrechtlichen Effektivitätsgrundsatz nicht mehr im Einklang stünde.[992] Der Rekurs auf den Effektivitätsgrundsatz ist jedoch nur bei einer indirekten Kollision erforderlich,[993] was nahelegt, dass der EuGH davon ausgeht, dass das nationale Verbot des Rechtsmissbrauchs über den unionsrechtlichen Grundsatz von Treu und Glauben hinausgehen kann; wäre dies von vornherein ausgeschlossen, der unionsrechtliche Grundsatz also abschließend, läge eine direkte Kollision vor, so dass es für den Anwendungsvorrang auf den Effektivitätsgrundsatz gar nicht ankäme. Dies legt die Schlussfolgerung nahe: Im harmonisierten Bereich, und damit auch hinsichtlich der Einwilligungserklärung nach Art. 4 Nr. 11 DS-GVO, kann § 242 BGB zwar über die unionsrechtlichen Grenzen von Treu und Glauben hinausreichen, muss jedoch am Effektivitätsgrundsatz gemessen werden.[994] Diese doppelten Grenzen zu konturieren, obliegt letztlich dem EuGH, weshalb eine harmonisierungsfeindliche Rechtszersplitterung zwischen den Mitgliedstaaten nicht zu befürchten steht.[995]

bb) Vertrag

Anders zu beurteilen sind Vertragsklauseln, die eine Legitimierungswirkung nach Art. 6 Abs. 1 lit. b DS-GVO entfalten sollen. Bei rechtsmissbräuchlicher Erlangung oder Ausübung der vertraglich konstituierten Rechtsposition gilt unumschränkt § 242 BGB. Der datenschutzrechtliche Grundsatz der Datenverarbeitung nach Treu und Glauben, Art. 5 Abs. 1 lit. a Var. 2 DS-GVO, erfasst diese Fälle gerade nicht. Andernfalls würde wie bei der Einwilligung die Unstimmigkeit entstehen, dass eine reine Berufung auf Art. 6 Abs. 1 lit. b DS-GVO, unabhängig von einer tatsächlich durchgeführten Datenverarbeitung, datenschutzrechtswidrig wäre. Zudem wäre unklar, inwiefern die Verletzung von Art. 5 Abs. 1 lit. a Var. 2 DS-GVO eine im Rahmen des Vertragsverhältnis-

---

[991] EuGH, Urt. v. 12.5.1998 – Rs. C-367/96 (*Kefalas*) – Rn. 20 f.; dazu ausführlich *Schmidt-Kessel*, Jahrbuch junger Zivilrechtswissenschaftler 2000, 61.

[992] EuGH, Urt. v. 12.3.1996 – Rs. C-441/93 (*Pafitis*) – Rn. 68–70; Urt. v. 12.5.1998 – Rs. C-367/96 (*Kefalas*) – Rn. 23 ff.; Urt. 9.3.1999 – Rs. C-212/97 (*Centros*) – Rn. 27; Urt. v. 23.3.2000 – Rs. C-373/97 (*Diamantis*) – Rn. 34 ff.; eine positive Konturierung des Grundsatzes anmahnend *Fleischer*, JZ 2003, 865 (874).

[993] Siehe oben, § 5 A.I.2.

[994] Ebenso *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 411 f.; ähnlich auch *Fleischer*, JZ 2003, 865 (873 f.).

[995] *Fleischer*, JZ 2003, 865 (873 f.).

ses zu berücksichtigende, zivilrechtliche Einwendung begründen sollte. Dies ist dogmatisch bei § 242 BGB allgemein anerkannt.[996]

Auch das unionsrechtliche allgemeine Verbot des Rechtsmissbrauchs ist jedoch, anders als bei der Einwilligung, nicht einschlägig, da die Wirksamkeit und Durchsetzbarkeit der vertraglichen Verpflichtung gerade nicht unionsrechtlich konstituiert, sondern allein dem nationalen Recht überantwortet ist. Dafür spricht insbesondere, dass nach Art. 6 Abs. 1 lit. b DS-GVO relevante Vertragsklauseln in der DS-GVO keinerlei über die genannte Bestimmung hinausgehende Regelung erfahren haben.[997] Der unionsrechtliche Grundsatz von Treu und Glauben fordert jedoch die missbräuchliche Berufung „auf Gemeinschaftsrecht".[998] Sofern sich der Verantwortliche auf die Wirksamkeit und Durchsetzbarkeit des Vertrags beruft, ist mithin gerade kein Recht auf Grundlage des Gemeinschaftsrechts betroffen, sondern eine sich allein aus nationalem Recht ergebende Rechtsposition. Anders verhielte es sich, wenn die Berufung gerade auf die Legitimierungswirkung des Art. 6 Abs. 1 lit. b DS-GVO als treuwidrig anzusehen wäre.

Wie bereits gesehen, kann daher die betroffene Person wegen der Widerrufsmöglichkeit nach Art. 7 Abs. 3 DS-GVO die *dolo agit*-Einrede gemäß § 242 BGB[999] erheben, wenn der Verantwortliche die Abgabe einer datenschutzrechtlichen Einwilligungserklärung oder die Überlassung von Daten fordert, deren Verarbeitung lediglich durch eine Einwilligungserklärung erlaubt werden könnte.[1000] Der unionsrechtliche Grundsatz von Treu und Glauben hingegen wäre verletzt, wenn der Verantwortliche vor Vertragsschluss zugesichert hätte, sich hinsichtlich einer Klausel gerade nicht auf Art. 6 Abs. 1 lit. b DS-GVO zu berufen (*venire contra factum proprium*[1001]).[1002]

c) Wechselwirkungen mit der DS-GVO

Die Verletzung des unionsrechtlichen Grundsatzes von Treu und Glauben, hinsichtlich der Einwilligung oder der Legitimierungswirkung von Art. 6 Abs. 1

[996] Siehe nur *Sutschet*, in: BeckOK, 51. Ed. 2019, § 242 Rn. 150; *Schubert*, in: MüKo, BGB, 8. Aufl. 2019, § 242 Rn. 80.

[997] *Indenhuck/Britz*, BB 2019, 1091 (1093).

[998] Siehe oben, § 5, Fn. 989.

[999] Zur *dolo agit*-Einrede allgemein *Looschelders/Olzen*, in: Staudinger, BGB, 2015, § 242 Rn. 279 ff.; *Wacker*, JA 1982, 477.

[1000] Siehe oben, Text bei § 4, Fn. 685 f.

[1001] Zur Anerkennung des Grundsatzes im Unionsrecht EuGH, Urt. v. 12.7.1962 – Rs. 14/61 (*Hoogovens*) – Rn. 7; EuG, Urt. v. 25.3.1999 – Rs. T-102/96 (*Gencor*) – Rn. 65; Erwähnung auch in EuGH, Urt. v. 22.3.1990 – Rs. C-347/87 (*Triveneta Zuccheri*) – Rn. 14; *Riesenhuber*, System und Prinzipien des Europäischen Vertragsrechts, 2003, 399; vorsichtig allerdings hinsichtlich einer Übertragung ins Unionsprivatrecht *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, 350.

[1002] Zur Vertrauensverletzung, auf Grundlage vorangegangener Absprachen oder Verhaltensweisen, als Verletzung von Art. 5 Abs. 1 lit. a Var. 2 DS-GVO *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 47.

lit. b DS-GVO, indiziert zugleich die Verletzung des datenschutzrechtlichen Grundsatzes von Treu und Glauben nach Art. 5 Abs. 1 lit. a Var. 2 DS-GVO, wenn es tatsächlich zu einer Datenverarbeitung auf Grundlage der Einwilligung oder Vertragsklausel kommt. Denn insofern sind grundsätzlich dieselben Kriterien ausschlaggebend.

Dies bedeutet jedoch umgekehrt nicht, dass die Umstände, die im vertraglichen Bereich zu einer Verletzung von § 242 BGB führen, unionsrechtlich irrelevant wären. Einerseits führt die Berufung auf die Einwendung nach § 242 BGB dazu, dass die Datenverarbeitung nicht mehr auf Art. 6 Abs. 1 lit. b DS-GVO gestützt werden kann. Denn auch wenn einer Leistungspflicht nur die Durchsetzbarkeit fehlt, ist die Datenverarbeitung nicht mehr zur Vertragserfüllung erforderlich. Dies ist insbesondere dann relevant, wenn man entgegen der hier vertretenen Auffassung annimmt, dass Nutzerpflichten die Legitimierungswirkung von Art. 6 Abs. 1 lit. b DS-GVO herbeiführen können.[1003] Andererseits müssen die zur Verletzung von § 242 BGB führenden Umstände bei der Frage berücksichtigt werden, ob eine Verletzung auch des datenschutzrechtlichen Grundsatzes von Treu und Glauben vorliegt, sofern eine Datenverarbeitung tatsächlich durchgeführt wird. Allerdings spielt die spezifische Einordnung dieser Handlungen als rechtsmissbräuchlich nach nationalem Recht dafür keine Rolle, da andernfalls der unionsrechtlich autonom zu bestimmende Begriff von Treu und Glauben nach Art. 5 Abs. 1 lit. a Var. 2 DS-GVO von der Auslegung nationalen Rechts abhängig wäre.[1004] Nichtsdestoweniger dürfte, wegen Identität des Argumentationshaushalts, regelmäßig bei einer Verletzung von § 242 BGB auch zugleich ein Verstoß gegen den datenschutzrechtlichen Grundsatz von Treu und Glauben vorliegen, sofern die Datenverarbeitung auf der nach deutschem Verständnis treuwidrigen erlangten oder ausgeübten Rechtsposition gründet.

Differenziert sind hingegen die Folgen des Rechtsmissbrauchs für die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO zu beurteilen. Zwar stellt die Missbräuchlichkeit einen abwägungsrelevanten Faktor dar. Nichtsdestoweniger kann die Interessenabwägung zugunsten des Verantwortlichen ausfallen, wenn der Missbrauch lediglich in den Umständen der Erlangung einer Einwilligung oder einer Vertragsbedingung begründet ist. Denn die Interessenlage hinsichtlich der Datenverarbeitung kann von diesen treuwidrigen Versuchen des Erreichens eines vermeintlich sichereren Erlaubnistatbestands unabhängig sein.[1005]

[1003] Siehe oben, § 4 B.II.2.b)bb)(2).

[1004] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 46; *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 DS-GVO Rn. 13.

[1005] Zum Streit der Möglichkeit der Berufung auf Art. 6 Abs. 1 lit. f DS-GVO neben einer unwirksamen oder widerrufenen Einwilligung oben, § 4 B.I.3.b)bb)(1).

d) Zusammenfassung zu § 242 BGB

Zusammenfassend lässt sich daher festhalten, dass hinsichtlich der Inhaltskontrolle von Einwilligungserklärungen und von solchen Vertragsklauseln, auf die eine Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO gestützt werden soll, die §§ 305 ff., 138 Abs. 1 BGB Vorrang vor § 242 BGB haben. Eine eigenständige Bedeutung kann § 242 BGB daher im hier untersuchten Kontext ohnehin nur im Bereich des Rechtsmissbrauchs, im Rahmen der Ausübungskontrolle, zukommen.

Hinsichtlich eines rechtsmissbräuchlichen Erwerbs der oder einer rechtsmissbräuchlichen Berufung auf die Einwilligung ist zwar der datenschutzrechtliche Grundsatz von Treu und Glauben, Art. 5 Abs. 1 lit. a Var. 2 DS-GVO, nicht einschlägig. Allerdings greift in der Regel der allgemeine unionsrechtliche Grundsatz von Treu und Glauben in Gestalt des Verbots von Rechtsmissbrauch. Sofern § 242 BGB über diesen Grundsatz im Einzelfall hinausgehen sollte, ist die Anwendung der Norm am Effektivitätsgrundsatz des Unionsrechts zu messen.

Steht hingegen Rechtsmissbrauch hinsichtlich einer Vertragsbedingung, auf welche die Datenverarbeitung gestützt werden soll, in Rede, so sind weder der datenschutzrechtliche noch der allgemeine unionsrechtliche Grundsatz von Treu und Glauben anwendbar. Wirksamkeit und Durchsetzbarkeit eines vertraglichen Anspruches werden durch die DS-GVO oder andere unionsrechtliche Instrumente im hier interessierenden Kontext gerade nicht geregelt. Daher kann § 242 BGB insoweit voll zur Entfaltung gebracht werden, ohne dass der Anwendungsvorrang des Unionsrechts berührt wäre. Lediglich dann, wenn sich die Missbräuchlichkeit gerade auf die Legitimationswirkung des Vertrags nach Art. 6 Abs. 1 lit. b DS-GVO bezieht, ist wiederum primär der unionsrechtliche allgemeine Grundsatz einschlägig.

Der Rechtsmissbrauch hat jeweils zur Folge, dass die Datenverarbeitung nicht nach Art. 6 Abs. 1 lit. a bzw. b DS-GVO erlaubt ist. Ferner ist regelmäßig der datenschutzrechtliche Grundsatz von Treu und Glauben nach Art. 5 Abs. 1 lit. a Var. 2 DS-GVO verletzt, wenn die Datenverarbeitung auf die von der Missbräuchlichkeit erfasste Einwilligungserklärung oder Vertragsklausel gestützt wird. Hingegen fällt die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO nicht notwendig zugunsten der betroffenen Person aus: Die Abwägung ist bei missbräuchlichem Erwerb der Rechtsposition von dem Verdikt des Rechtsmissbrauchs weitestgehend unabhängig.

III. Haftung

Schließlich wirft auch die Haftung des datenschutzrechtlich Verantwortlichen sowohl im vertraglichen wie auch im außervertraglichen Bereich Fragen der Koordination von Datenschutzrecht und allgemeinem Zivilrecht auf.

Dabei ist zunächst zu erörtern, ob eine zivilrechtliche Haftung nach Maßgabe des nationalen Haftungsrechts neben der unionalen Anspruchsgrundlage in Art. 82 Abs. 1 DS-GVO überhaupt in Betracht kommt (1.). Da dies jedenfalls im Grundsatz, wenn auch mit erheblichen Einschränkungen, bejaht werden kann, muss das Verhältnis zwischen Art. 82 Abs. 1 DS-GVO und § 280 Abs. 1 BGB geklärt werden für Fälle, in denen nach dem soeben Erörterten ein wirksamer Vertrag zwischen betroffener Person und datenschutzrechtlich Verantwortlichem zustande kommt (2.).

Ferner können außervertragliche Ansprüche neben vertragliche treten. Sie sind aber insbesondere dann von Relevanz, wenn eine privatautonom getroffene Regelung zwischen der betroffenen Person und dem datenschutzrechtlich Verantwortlichen nicht zu Stande kommt oder unwirksam ist. Dies ist vor allem zu gewärtigen, wenn die Einbeziehung von Drittanbietern oder Drittnutzern von IoT-Geräten bereits am Abschlusstatbestand scheitert (§ 5 B.III.) oder aber einer rechtsgeschäftlichen Regelung nach Maßgabe der soeben erörterten Grenzen der Privatautonomie (§ 5 C.I.-II.) die Wirksamkeit zu versagen ist. In diesen Fällen kommen zunächst Ansprüche aus *culpa in contrahendo* sowie bereicherungsrechtliche Ansprüche in Betracht (3.). Besonders bedeutsam sind dann ferner deliktische Ansprüche der betroffenen Person gegen den datenschutzrechtlich Verantwortlichen wegen der Verletzung datenschutzrechtlich relevanter Pflichten (4.). Nach der Rechtsprechung des EuGH sind nationale Regelungen zur außervertraglichen Haftung zwar von den oben dargestellten, unionsrechtlich induzierten Folgen der AGB-rechtlichen Unwirksamkeit unabhängig.[1006] Problematisch ist jedoch wiederum das Verhältnis zur DS-GVO, sofern datenschutzrechtlich relevante Konstellationen vorliegen.

1. Anwendbarkeit zivilrechtlicher Haftungsnormen neben der DS-GVO

Mit Geltungsbeginn der DS-GVO ist erstmals eine Anspruchsgrundlage für die Verletzung datenschutzrechtlicher Pflichten unmittelbar im Unionsrecht verortet worden. Nach Art. 82 Abs. 1 DS-GVO hat jede Person, der wegen eines Verstoßes gegen die DS-GVO ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Diese werden jedoch nach Abs. 3 von der Haftung befreit, wenn sie nachweisen, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich sind.[1007] Dieser unionsrechtliche Anspruch tritt nunmehr an die Stelle von §§ 7 f. BDSG

[1006] EuGH, Urt. v. 7.11.2019 – verb. Rs. C-349/18 bis C-351/18 (*NMBS*) – Rn. 73.

[1007] Zur umstrittenen, praktisch aber wenig relevanten dogmatischen Einordnung von Art. 82 Abs. 3 DS-GVO als tatbestandliche Verschuldensvermutung (so *Spindler*, DB 2016, 937 [947]; *Quaas*, in: BeckOK Datenschutzrecht, 29. Ed. 2019, Art. 82 DS-GVO Rn. 17; *Jacquemain*, RDV 2017, 227 [230]) oder als rechtsvernichtende Einwendung (so *Wybitul*, ZD 2016, 253 [253 f.]; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 6) siehe *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019,

aF.[1008] Schon seinem Wortlaut nach geht er verhältnismäßig weit: Er verlangt keinen Verschuldensnachweis des Anspruchstellers. Ferner umfasst er materielle und – anders als noch die Anspruchsgrundlage gegen private Verarbeiter nach § 7 BDSG aF[1009] – auch immaterielle Schäden. Mehrere Schuldner haften gem. Art. 82 Abs. 4 DS-GVO gesamtschuldnerisch und können nach Art. 82 Abs. 5 DS-GVO Binnenregress nehmen.

Die Existenz von Art. 82 DS-GVO wirft die Frage auf, inwieweit eine Haftung für datenschutzrechtliche Verstöße nach Maßgabe nationaler Anspruchsgrundlagen überhaupt noch notwendig und, vor allem, zulässig ist. Die Antwort ist, wie auch bei sonstigen Fragen des Vorrangs des Unionsrechts, für jede nationale Norm separat zu suchen.

Zunächst lässt sich eine Differenzierung vor die Klammer ziehen: jene der Unterscheidung zwischen einer Störerhaftung einerseits und der Haftung für eigene Rechtsverletzungen andererseits. Hinsichtlich einer Störerhaftung wegen eines nicht täterschaftlichen Beitrags zu einer Datenschutzrechtsverletzung wurde bereits ausgeführt, dass der Anwendungsvorrang der DS-GVO einer solchen Rechtsfigur entgegensteht.[1010]

Mit Blick auf nationale Normen zur Haftung für eigene Rechtsverletzungen jedoch muss differenziert werden. Unstreitig dürfte im Ausgangspunkt sein, dass ergänzende Regelungen des BGB, etwa zu Verjährung und Übertragbarkeit des Anspruchs, in den Grenzen des Äquivalenz- und Effektivitätsgrundsatzes, Anwendung finden, wenn sie in der DS-GVO keine Regelung erfahren haben.[1011] Auch das Mitverschulden fällt nach umstrittener, aber zutreffender Ansicht darunter.[1012]

Art. 82 DS-GVO Rn. 6; *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 12.

[1008] Zum alten Recht überblicksartig *Gola/Piltz*, RDV 2015, 279 (279 ff.).

[1009] BGH NJW 2017, 800 Rn. 12 ff.

[1010] Siehe oben, § 4 A.III.1.c).

[1011] EuGH, Urt. v. 25.11.2010 – Rs. C-429/09 (*Fuß*) – Rn. 93 (zum Rückgriff auf unionsrechtliche nicht geregelte Aspekte eines Schadensersatzanspruchs); ferner EuGH, Urt. v. 22.11.2012 – Rs. C-139/11 (*Moré*) – Rn. 33 (zum Rückgriff auf nationales Verjährungsrecht hinsichtlich der Ansprüche aus der Fluggastrechteverordnung); zu diesem Urteil kritisch allerdings *Basedow*, ZEuP 2014, 402 (405 ff.); zur DS-GVO speziell *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 9; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 19; *Quaas*, in: BeckOK Datenschutzrecht, 29. Ed. 2019, Art. 82 DS-GVO Rn. 5; *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 82 DS-GVO Rn. 38; *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 65 f.; *Spindler/Horváth*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 82 DS-GVO Rn. 3; *Neun/Lubitzsch*, BB 2017, 2563 (2569); *Sackmann*, ZIP 2017, 2450 (2451); *Paal*, MMR 2020, 14 (19).

[1012] *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 9; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 19; *Quaas*, in: BeckOK Datenschutzrecht, 29. Ed. 2019, Art. 82 DS-GVO Rn. 28, 31; *Nemitz*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 82 Rn. 15; *Spindler/Horváth*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 82 DS-GVO Rn. 3; *Wybitul/Neu/Strauch*, ZD 2018, 202 (207); aA *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl.

Die Anspruchskonkurrenz von Art. 82 DS-GVO mit nationalen Schadensersatzvorschriften bei eigener Rechtsverletzung ist hingegen umstritten. Teilweise wird Art. 82 DS-GVO eine Sperrwirkung gegenüber allen deliktischen Ansprüchen unterstellt.[1013] *Svantesson* vertritt demgegenüber, dass nur unter außerordentlichen Umständen („in the extreme circumstances") das Haftungsregime der DS-GVO, mit der Trennung zwischen passivlegitimierten datenschutzrechtlich Verantwortlichen und nicht passivlegitimierten datenschutzrechtlich Nicht-Verantwortlichen, durch andere Haftungsnormen überwunden werden kann.[1014] Damit ist der Anwendungsvorrang der DS-GVO im Ansatz richtig erfasst; die Freigabe anderer unionaler oder nationaler Schadensersatzansprüche unter außerordentlichen Umständen ist jedoch zugleich zu vage und zu pauschal, um zu überzeugen.

Vielmehr kann ein entscheidender Hinweis dem 146. Erwägungsgrund der DS-GVO entnommen werden. Dieser beschäftigt sich mit dem Schadensersatzanspruch nach Art. 82 DS-GVO und lautet in seinem dritten und vierten Satz:

„Der Begriff des Schadens sollte im Lichte der Rechtsprechung des Gerichtshofs weit auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht. Dies gilt unbeschadet von Schadenersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten."

Der vierte Satz dieses Erwägungsgrunds kann jedoch nicht so verstanden werden, dass Ansprüche nach nationalem Recht schlechterdings nicht berührt werden.[1015] Denn erstens müssen Schadensersatzansprüche, um nach dem vierten Satz des 146. Erwägungsgrunds unberührt zu bleiben, an die Verletzung *anderer* Vorschriften als solcher der DS-GVO anknüpfen. Zweitens ist auch für diese Ansprüche nicht klar, ob die vom vierten Satz proklamierte Unabhängigkeit nicht lediglich für den im dritten Satz angesprochenen weiten Schadensbegriff gilt. Das legt das Demonstrativpronomen „Dies" nahe, das allerdings grammatikalisch auch auf die gesamten, in den Sätzen 1–3 des 146. Erwägungsgrunds enthaltenen Erwägungen zu Art. 82 DS-GVO bezogen werden kann. Auch der Vergleich mit der englischen („This") und französischen („Cela") Sprachfassung bringt insofern keine Klarheit. Allerdings sprechen für den Bezug von Satz 4 des 146. Erwägungsgrunds lediglich auf Satz 3 die großen Unsicherhei-

2018, Art. 82 DS-GVO Rn. 59; *Sackmann*, ZIP 2017, 2450 (2453); *Kreße*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 82 Rn. 20 (nur bei Mitverschulden i. H. v. 100 %).

[1013] *Kreße*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 82 Rn. 27.

[1014] *Svantesson*, 34 Computer Law and Security Review 2018, 25 (33).

[1015] So aber *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 67; *Spindler/Horváth*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 82 DS-GVO Rn. 4 f.; *Moos/Schefzig*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 82 DS-GVO Rn. 101; *Kohn*, ZD 2019, 498 (499); *Neun/Lubitzsch*, BB 2017, 2563 (2569); *Sackmann*, ZIP 2017, 2450 (2451); wohl auch *Thon*, RabelsZ 84 (2020), 24 (29).

ten, die mit der Bestimmung des Schadensbegriffs im Schnittbereich von nationalem und unionalem Haftungsrecht im Zuge des Gesetzgebungsprozesses der DS-GVO verbunden waren.[1016] Satz 4 soll daher wohl lediglich eine Kontamination der Schadensbegriffe anderer Normen als der DS-GVO durch das in Satz 3 ausgesprochene, weite Verständnis verhindern.[1017]

Der hinter dem vierten Satz stehende Gedanke jedoch, dass eine eigenständige Bedeutung weiterer unionsrechtlicher oder nationaler Anspruchsgrundlagen nur in Betracht kommt, sofern *andere* Normen als jene der DS-GVO verletzt sind, leuchtet unmittelbar ein. Dies entspricht – als materielle Andersartigkeit verstanden – gerade dem Kriterium der Risikospezifizität. Daher muss nach hier vertretener Auffassung die Zulässigkeit der Haftung für eigene Rechtsverletzungen nach nationalem Recht durch die oben entwickelte zweistufige Prüfung geklärt werden,[1018] um eine Verletzung des unionsrechtlichen Effektivitätsgrundsatzes auszuschließen.[1019] Fehlt es an einer Risikospezifizität, kann Art. 82 DS-GVO gar eine *lex specialis* darstellen.

Dies ist in der Tat zumeist der Fall, kann jedoch nur für jede Haftungsnorm einzeln beurteilt werden, was Gegenstand der folgenden Ausführungen ist. Vorab sollte lediglich noch betont werden, dass Art. 82 DS-GVO ganz offensichtlich nur im Rahmen seines Anwendungsbereichs eine *lex specialis* darstellen kann. Dieser umfasst nach herrschender[1020] und zutreffender Meinung jedoch, wie die DS-GVO ganz allgemein (vgl. Art. 1 Abs. 1 DS-GVO), nicht Ansprüche von juristischen, sondern nur von natürlichen Personen. Hinsichtlich des Haftungsregimes zum Schutz juristischer Personen kann und muss daher vollumfänglich auf mitgliedstaatliches Recht zurückgegriffen werden.[1021]

2. Vertragliche Haftung

Sofern nach Maßgabe des in den letzten Abschnitten Erörterten zwischen der betroffenen Person und dem Verantwortlichen ein wirksamer Vertrag zustande kommt (§ 5 B.III., C.I.-II.), ergibt sich zwangsläufig die Folgefrage, ob das datenschutzrechtliche Pflichtenregime der DS-GVO zugleich Inhalt von vertraglichen Nebenpflichten aus § 241 Abs. 2 BGB ist. Diese auch vertragliche Verortung datenschutzrechtlich radizierter Pflichten ist zwar in Anbetracht des

---

[1016] Rat der Europäischen Union, Interinstitutional File: 2012/0011 (COD), Dokument 7084/15 vom 16.3.2015, 48 Fn. 131.

[1017] Vgl. *Heinze*, Schadensersatz im Unionsprivatrecht, 2017, 580 f. mit Fn. 302.

[1018] Siehe oben, § 5 A.I.2.b).

[1019] Ebenfalls für eine differenzierte Bewertung anhand des Effektivitätsgrundsatzes *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 19 f.

[1020] *Paal*, MMR 2020, 14 (14); *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 82 DS-GVO Rn. 8; *Kohn*, ZD 2019, 498 (502); *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 10; *Dieckmann*, r+s 2018, 345 (346); wohl auch *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 13, 15.

[1021] *Paal*, MMR 2020, 14 (14); *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 82 DS-GVO Rn. 8.

Regelungsgehalts von Art. 82 DS-GVO von reduzierter Bedeutung. Eine vertragliche Haftung bietet hinsichtlich ihrer Verschuldensvermutung nach § 280 Abs. 1 S. 2 BGB keinen Vorteil gegenüber Art. 82 Abs. 3 DS-GVO. Sie ist jedoch Ausgangspunkt für eine Diskussion der Möglichkeit der Zurechnung über § 278 BGB, die insbesondere deshalb relevant erscheint, weil das Datenschutzrecht selbst keine eigene Zurechnungsnorm kennt. Dafür muss jedoch zunächst geklärt werden, ob Pflichten der DS-GVO überhaupt als vertragliche Nebenpflichten angesehen werden können.

a) Wesentliche Pflichten der DS-GVO als vertragliche Nebenpflichten nach § 241 Abs. 2 BGB

Ein Teil der Literatur möchte alle Pflichten aus der DS-GVO zugleich als Nebenpflichten nach § 241 Abs. 2 BGB qualifizieren.[1022] Dem wird man in dieser Allgemeinheit jedoch nicht zustimmen können.

aa) Rechtslage im Bereich der Anlageberatung

Vielmehr lohnt ein Blick auf die aus der kapitalmarktrechtlichen Anlageberatung bekannte Problematik der Ausstrahlung des aufsichtsrechtlichen Pflichtenregimes auf zivilrechtliche Nebenpflichten des Beratungsvertrags zwischen einem Anleger und der Bank.[1023] Der BGH hat in einer wegweisenden Entscheidung aus dem Jahr 2014 zu versteckten Innenprovisionen festgehalten, dass wesentliche Pflichten des von ihm im Übrigen als öffentlich-rechtlich qualifizierten Regelungsregimes der Wohlverhaltenspflichten (nunmehr §§ 63 ff. WpHG) bei Auslegung des Beratungsvertrags nach §§ 133, 157 BGB vertragliche Nebenpflichten darstellen:

„Der *Senat* hält es jedoch für angezeigt, den nunmehr im Bereich des – aufsichtsrechtlichen – Kapitalanlagerechts nahezu flächendeckend vom Gesetzgeber verwirklichten Transparenzgedanken hinsichtlich der Zuwendungen Dritter auch bei der Bestimmung des Inhalts des Beratungsvertrags zu berücksichtigen, weil der Anleger nunmehr für die Bank erkennbar eine entsprechende Aufklärung im Rahmen des Beratungsvertrags erwarten kann (§§ 133, 157 BGB)."[1024] „Der Anleger kann zwar nicht erwarten, dass sich die beratende Bank im gesamten Umfang ihrer öffentlich-rechtlichen Pflichten ohne Weiteres auch im individuellen Schuldverhältnis gegenüber dem jeweiligen Anleger verpflichten will. Er kann aber voraussetzen, dass die beratende Bank die tragenden Grundprinzipien des Aufsichtsrechts beachtet."[1025]

[1022] *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 21; *Forst*, AuR 2010, 106 (107) für das BDSG aF für den Arbeitsvertrag; vgl. insofern auch LAG Hamburg NZA 1992, 509 (511); ferner für das BDSG aF *Wind*, RDV 1991, 16 (17); *Niedermeier/Schröcker*, RDV 2002, 217 (219).

[1023] Dazu etwa *Assmann*, in: Festschrift Schneider, 2011, 37; *Hacker*, Verhaltensökonomik und Normativität, 2017, 842 ff.

[1024] BGH NJW 2014, 2947 Rn. 36.

[1025] BGH NJW 2014, 2947 Rn. 37.

In der Literatur wurde die Begründung des BGH zum Teil dahingehend kritisiert, der Rekurs auf die flächendeckende Verwirklichung eines Regelungsgedankens sei vage und beliebig.[1026] Man wird jedoch die eigentliche, dogmatische Begründung in den Passagen suchen müssen, die sich auf die von der Gegenseite erkennbare Erwartungshaltung des Anlegers beziehen, die nach §§ 133, 157 BGB maßgeblich zu berücksichtigen ist.[1027] Die flächendeckende Verwirklichung eines bestimmten Rechtsprinzips dürfte dabei lediglich eine von mehreren Möglichkeiten konstituieren, aus denen sich eine derartige Erwartungshaltung erkennbarer Weise ergeben kann.[1028] Diese Maßstäbe wiederum lassen sich auf die datenschutzrechtliche Problematik übertragen.

bb) Übertragung auf datenschutzrechtliche Sachverhalte

Wie auch bei der Bankberatung spricht hinsichtlich solcher Verträge, die auf eine Verarbeitung von Daten ausgerichtet sind, bei denen diese jedoch nicht die vertragliche Hauptpflicht ausmacht,[1029] eine umfassende Interessenabwägung nach §§ 133, 157 BGB dafür, im Wege der Vertragsauslegung die Übernahme der wesentlichen Pflichten der DS-GVO als vertragliche Nebenpflichten im Sinne von § 241 Abs. 2 BGB anzuerkennen. Dogmatisch betrachtet liegt die Einordnung als Nebenpflicht nach § 241 Abs. 2 BGB näher als die als Nebenleistungspflicht nach § 241 Abs. 1 BGB, da durch die Nichteinhaltung datenschutzrechtlicher Vorgaben typischerweise eher das Integritätsinteresse und nicht das Äquivalenzinteresse betroffen ist.[1030] Angesichts der unmittelbaren Haftung des Verantwortlichen aus Art. 82 DS-GVO erschiene auch ein Fristsetzungserfordernis nach § 281 Abs. 1 BGB, sofern man diesen neben Art. 82 DS-GVO überhaupt für anwendbar hält,[1031] nicht als systemkonform.[1032]

Klärungsbedürftig ist weiterhin der Umfang der vertraglichen Nebenpflicht. Zwar hat der Verantwortliche ein legitimes Interesse daran, nicht alle noch so detaillierten datenschutzrechtlichen Pflichten zum Gegenstand auch vertraglicher Gewährleistung zu machen. Hinsichtlich der tragenden Konzepte und Pflichten der DS-GVO kann die betroffene Person jedoch, gerade in den drei hier in Rede stehenden Leitfällen, regelmäßig erwarten, dass das Datenschutzrecht insoweit auch im Rahmen von Vertragsverhältnissen Beachtung findet. In der Tat zeigen auch alle empirischen Erhebungen, dass die datenschutzrechts-

[1026] *Balzer/Lang*, BKR 2014, 377 (379 f.); kritisch auch *Omlor*, LMK 2014, 361191; *Zoller*, BB 2014, 1805; *Heun-Rehn/Lang/Ruf*, NJW 2014, 2909 (2912); die Ableitung von Nebenpflichten aus dem Aufsichtsrecht fordernd jedoch bereits *Krüger*, NJW 2013, 1845 (1847).

[1027] So auch *Zahrte*, in: MüKo, HGB, 4. Aufl. 2019, Band 6, M. Anlageberatung Rn. 109.

[1028] Ähnlich auch *Buck-Heeb*, WM 2014, 1601 (1605).

[1029] Dazu *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 22.

[1030] Siehe zu diesem Abgrenzungskriterium nur *Bachmann*, in: MüKo, BGB, 8. Aufl. 2019, § 241 Rn. 62; anders stellt sich dies, wie angemerkt, bei einem Vertrag dar, bei dem die Datenverarbeitung Hauptpflicht ist.

[1031] Siehe dazu unten, § 5 C.III.2.c).

[1032] Vgl. nochmals *Bachmann*, in: MüKo, BGB, 8. Aufl. 2019, § 241 Rn. 64.

konforme Verarbeitung ein signifikantes Desiderat von Kunden ist.[1033] Diese Erwartungshaltung ist für den Verantwortlichen regelmäßig auch erkennbar.

Damit erhebt sich sogleich die Frage, welche Regeln der DS-GVO als hinreichend gewichtig angesehen werden können, um Gegenstand einer vertraglichen Nebenpflicht zu sein. Hier wird man sich von der DS-GVO-internen Hierarchie leiten lassen können, die in der unterschiedlichen Sanktionierung verschiedener Pflichten in Art. 83 Abs. 4 und 5 DS-GVO zum Ausdruck kommt. Daher erscheint es naheliegend, nur die in Art. 83 Abs. 5 DS-GVO genannten, am schärfsten sanktionierten Pflichten als zentral anzusehen. Dies umfasst insbesondere die Grundsätze für die Verarbeitung gemäß Art. 5, 6, 7 und 9 sowie die Rechte der betroffenen Person gemäß Art. 12–22 DS-GVO. Allerdings wird man die in Art. 83 Abs. 5 DS-GVO ebenfalls genannten Bedingungen der Einwilligung nicht zu den im Wege der Vertragsauslegung als Nebenpflichten des Vertrags qualifizierbaren Teilen der DS-GVO rechnen können. Denn wie oben ausführlich dargelegt wurde, muss zwischen der Einwilligung einerseits und dem Vertrag andererseits dogmatisch streng unterschieden werden.[1034] Der Nutzer kann daher nicht erwarten, dass die Verletzung von einwilligungsspezifischen Pflichten zugleich eine *Vertrags*verletzung des Anbieters darstellt.

Insgesamt stellen damit also die wesentlichen Pflichten der DS-GVO auch vertragliche Nebenpflichten dar. Dies wird insbesondere dann relevant, wenn man in der Datenverarbeitung mit einem Teil der Literatur keine Sonderrechtsbeziehung im Sinne von § 278 S. 1 BGB erblickt. Diese Fragen sind Gegenstand des nächsten Abschnitts.

b) Die Anwendbarkeit von § 278 BGB im Rahmen der Datenverarbeitung

Können demnach zumindest die wesentlichen Pflichten der Datenverarbeitung nach der DS-GVO zugleich typischerweise als vertragliche Nebenpflichten qualifiziert werden, so stellt sich insbesondere die Frage, inwiefern der Verantwortliche für die Verletzung dieser Pflichten durch Erfüllungsgehilfen gemäß § 278 BGB haftet.

aa) Tatbestandsvoraussetzungen

Die Tatbestandsvoraussetzungen von § 278 BGB sind dabei erfüllt. Dies gilt jedoch nach hier vertretener Auffassung unabhängig davon, ob DS-GVO-Pflichten als vertragliche Nebenpflichten behandelt werden. Denn für die Anwendbarkeit von § 278 BGB genügt auch die Existenz eines gesetzlichen, sogar öffentlich-rechtlichen[1035] Schuldverhältnisses, aus dem sich spezifische, über die allgemeinen deliktischen Verkehrspflichten hinausgehende Obligationen

[1033] Siehe oben, § 3 B.II.2.a).
[1034] Siehe oben, § 4 B.I.2.
[1035] BGH NJW 2006, 1121 (1123); *Grundmann*, in: MüKo, 8. Aufl. 2019, § 278 Rn. 19.

ergeben.[1036] Ein solches Sonderrechtsverhältnis besteht zwischen dem datenschutzrechtlich Verantwortlichen und der betroffenen Person regelmäßig – auch wenn dies in der Literatur bislang, soweit ersichtlich, kaum thematisiert und überwiegend abgelehnt wird[1037] – infolge des Umstands der Datenverarbeitung selbst: Damit gehen *spezifische* Pflichten des Verantwortlichen gegenüber der betroffenen Person einher, etwa hinsichtlich der Einhaltung der datenschutzrechtlichen Grundsätze nach Art. 5 Abs. 1 DS-GVO, hinsichtlich der Informationspflichten nach Art. 12 ff. DS-GVO sowie der weiteren Betroffenenrechte. Insbesondere muss man bei der Auslegung berücksichtigen, dass es angemessen scheint, dass der datenschutzrechtlich Verantwortliche jedenfalls hinsichtlich der Pflichten der DS-GVO für das Personalrisiko strikt nach § 278 S. 1 BGB haftet: Denn er alleine kann dieses Risiko durch Compliance-Maßnahmen beherrschen.[1038] Nach Maßgabe des deutschen Rechts haftet daher der Verantwortliche nach § 278 S. 1 BGB strikt für alle datenschutzrechtlichen Pflichtverletzungen seiner Erfüllungsgehilfen.[1039]

bb) Kein Anwendungsvorrang der DS-GVO

Allerdings konfligiert die Anwendung von § 278 BGB auf das Rechtsverhältnis zwischen datenschutzrechtlich Verantwortlichem und betroffener Person womöglich mit dem Anwendungsvorrang der DS-GVO. Zwar kennt die DS-GVO selbst keine spezifische Zurechnungsnorm. Allerdings existiert mit den Regeln zur Auftragsverarbeitung ein besonderes Regime, das die Pflichten und auch die Haftung von Personen beschreibt, an welche der Verantwortliche bestimmte Tätigkeiten im Rahmen der Datenverarbeitung delegiert. Auftragsverarbeiter ist nach der unbefriedigenden Legaldefinition in Art. 4 Nr. 8 DS-GVO jede „natürliche oder juristische Person, Behörde, Einrichtung oder

[1036] Siehe nur *Grundmann*, in: MüKo, 8. Aufl. 2019, § 278 Rn. 15; *Caspers*, in: Staudinger, BGB, 2014, § 278 Rn. 10 f.

[1037] Zur Rechtslage vor Geltungsbeginn der DS-GVO *Forst*, AuR 2010, 106 (108) (deliktische Qualität des § 7 BDSG aF schließe Anwendung von § 278 BGB aus); in dieser Richtung lassen sich auch die Ausführungen des OLG Köln, MMR 2015, 204 (208) verstehen, wonach kein Sonderrechtsverhältnis besteht zwischen dem Betreiber einer Suchmaschine und einer Person, deren bürgerlicher Name im Rahmen der Autocomplete-Funktion ergänzt wird. Allerdings mögen hier die besonderen, persönlichkeitsrechtlichen Prüfpflichten die Ablehnung eines Sonderrechtsverhältnisses motiviert haben; für eine deliktische Qualifikation des Art. 82 Abs. 1 DS-GVO und gegen die allgemeine Annahme eines Sonderrechtsverhältnisses auch *Sackmann*, ZIP 2017, 2450 (2451); für ein Sonderrechtsverhältnis zwischen betroffener Person und „der die Daten faktisch kontrollierenden Partei" nunmehr aber auch *Datenethikkommission*, Gutachten der Datenethikkommission, 2019, 147.

[1038] Zur Beherrschung des Personalrisikos als Geltungsgrund von § 278 BGB siehe BGH NJW 1960, 669 (671); *Grundmann*, in: MüKo, 8. Aufl. 2019, § 278 Rn. 3; *Hacker*, RW 9 (2018), 243 (254); *Schmidt*, AcP 166 (1966), 1 (24); vgl. auch *Spiro*, Die Haftung für Erfüllungsgehilfen, 1984, 52–54.

[1039] So im Ergebnis auch *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 24; *Forst*, AuR 2010, 106 (109).

andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet".[1040] Er wird mithin mit Willen und im Interesse des Verantwortlichen von diesem in die Verarbeitung eingebunden.[1041] Grundsätzlich muss die Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter gemäß Art. 28 Abs. 1 lit. a DS-GVO auch ein Weisungsrecht des Verantwortlichen umfassen.[1042] Die zentrale Norm der Auftragsdatenverarbeitung, Art. 28 DS-GVO, enthält jedoch gerade keine Grundlage für eine *Zurechnung* vom Auftragsverarbeiter zum Verantwortlichen. Das Schweigen der DS-GVO kann jedoch letztlich nicht als beredtes Schweigen gedeutet werden, das einen Rückgriff auf § 278 BGB ausschließt. Denn auch datenschutzrechtlich sprechen die besseren Argumente für eine strikte Haftung des Verantwortlichen für seine Erfüllungsgehilfen, inklusive der Auftragsverarbeiter.[1043]

So spricht bereits die Tatsache, dass Auftragsverarbeiter nach Art. 29 DS-GVO grundsätzlich nur auf Weisung des datenschutzrechtlich Verantwortlichen Daten verarbeiten dürfen, für eine Zurechnung von Pflichtverletzung und Verschulden des Auftragsverarbeiters zum Verantwortlichen. Denn dieser, und nur dieser, kann durch die Auswahl des Auftragsverarbeiters und mittels des Weisungsrechts das in der Einschaltung des Gehilfen liegende Personalrisiko beherrschen.[1044] Ferner zeigt auch die Regelung in Art. 82 Abs. 4 DS-GVO, dass der betroffenen Person kein Vorgehen gegen eine unbestimmte Anzahl von nachrangigen Verarbeitern zugemutet werden, sondern diese den Schaden *in toto* beim Verantwortlichen reklamieren können soll.[1045] Nur dies entspricht einer letztlich wirksamen und effektiven privatrechtlichen Durchsetzung des

[1040] Dazu ausführlich *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP 169, 2010, 30 ff.

[1041] *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP 169, 2010, 31.

[1042] Siehe *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 8 DS-GVO Rn. 7; *Artikel-29-Datenschutzgruppe*, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP 169, 2010, 31.

[1043] So auch im Ergebnis *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 55; *Nemitz*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 82 Rn. 20; *Spindler*, DB 2016, 937 (947); *Wybitul/Haß/Albrecht*, NJW 2018, 113 (116); *Wybitul/Neu/Strauch*, ZD 2018, 202 (204) (jeweils Haftung für Mitarbeiter und Auftragsverarbeiter); *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 82 Rn. 15 (Haftung für Mitarbeiter und Dritte); *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 19 (Haftung für Mitarbeiter), zudem *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 24 (Anwendung von § 278 BGB); *Ingold*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 11 f.; *Spoerr*, in: BeckOK Datenschutzrecht, 29. Ed. 2019, Art. 29 DS-GVO Rn. 20 (jeweils Haftung für Auftragsverarbeiter); ebenso wohl *Piltz*, K&R 2017, 85 (90).

[1044] Siehe die Nachweise oben, in § 5, Fn. 1038.

[1045] Vgl. *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 55; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 82 Rn. 15; *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 82 DS-GVO Rn. 24.

Schadensersatzanspruches (sechster Satz des 146. Erwägungsgrunds),[1046] da die Aufgabenverteilung zwischen Verantwortlichem und Auftragsverarbeiter für die betroffene Person häufig von außen kaum erkennbar ist. Anders als die Vereinbarung zwischen gemeinsam Verantwortlichen nach Art. 26 Abs. 1 und 2 DS-GVO muss die Vereinbarung zwischen Verantwortlichem und Auftragsverarbeiter der betroffenen Person nicht zur Verfügung gestellt werden (Art. 26 Abs. 2 S. 2 DS-GVO *e contrario*). Allein der Verantwortliche tritt daher nach außen gegenüber der betroffenen Person auf und sollte dementsprechend auch haften:[1047] Er ist der „single point of entry"[1048], wenngleich sich die betroffene Person, sofern sie hinreichende Kenntnisse über die Umstände besitzt, nach ihrer Wahl auch nach Art. 82 Abs. 1 und Abs. 2 S. 2 DS-GVO direkt an den Auftragsverarbeiter wenden kann.[1049] Der Verantwortliche kann auf Grundlage der Vereinbarung mit dem Auftragsverarbeiter sowie nach Art. 82 Abs. 5 DS-GVO sodann bei diesem Regress nehmen.

Die Zurechnung des Personalrisikos hinsichtlich vom Verantwortlichen beauftragter Gehilfen ist daher in der DS-GVO zwar nicht explizit adressiert. Die Anwendung von §278 BGB innerhalb des Schuldverhältnisses zwischen datenschutzrechtlich Verantwortlichem und betroffener Person entspricht jedoch dem Sinn und Zweck des Regelungsgefüges der DS-GVO zum Auftragsverarbeiter und steht daher mit dem Anwendungsvorrang des Unionsrechts im Einklang.

c) Zur Anwendbarkeit von §280 Abs. 1 BGB

Die vorstehenden Erwägungen lassen erkennen, dass die Frage, ob §280 Abs. 1 BGB eine Anspruchsgrundlage darstellt für die Verletzung vertraglicher Nebenpflichten gemäß §241 Abs. 2 BGB, die unmittelbar aus der DS-GVO abgeleitet werden, oder ob §280 Abs. 1 BGB von Art. 82 Abs. 1 DS-GVO verdrängt wird, rein akademischer Natur ist. Denn in der Praxis ist regelmäßig der letztgenannte Anspruch für den Geschädigten vorteilhafter.[1050] Nicht nur muss sich, wie im Rahmen von §280 Abs. 1 S. 2 BGB, der Verantwortliche hinsichtlich seines Verschuldens selbst entlasten (Art. 82 Abs. 3 DS-GVO) und ist §278 BGB nach dem soeben Gesagten vollumfänglich anwendbar. Vielmehr

[1046] *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 55; *Nemitz*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 82 Rn. 20; *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 82 DS-GVO Rn. 24.

[1047] *Spindler*, DB 2016, 937 (947).

[1048] Rat der Europäischen Union, Interinstitutional File: 2012/0011 (COD), Dokument 9083/15 vom 27.5.2015, 2.

[1049] Rat der Europäischen Union, Interinstitutional File: 2012/0011 (COD), Dokument 9083/15 vom 27.5.2015, 2.

[1050] *Nemitz*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 82 Rn. 7.

kann auch ein immaterieller Schaden, der gerade bei datenschutzrechtlichen Pflichtverletzungen erhebliche Relevanz besitzt, ohne die Restriktionen des § 253 BGB oder die Begrenzung auf schwerwiegende Persönlichkeitsrechtsverletzungen[1051] geltend gemacht werden.[1052]

Nichtsdestoweniger geht die herrschende Meinung davon aus, dass § 280 Abs. 1 BGB zu Art. 82 Abs. 1 DS-GVO in Anspruchskonkurrenz steht.[1053] Nach hier vertretener Auffassung jedoch stellt letztere Anspruchsgrundlage eine *lex specialis* auch zur vertraglichen Haftung nach § 280 Abs. 1 BGB dar, soweit es um die Verletzung vertraglicher Nebenpflichten geht, die unmittelbar aus der DS-GVO gewonnen werden.[1054] Denn Art. 82 Abs. 1 DS-GVO verwirklicht, wie soeben gesehen, eine Haftung aus einem datenschutzrechtlichen Sonderrechtsverhältnis, sodass nicht argumentiert werden kann, die vertragliche Haftung stünde auch sonst zu einer deliktischen Haftung regelmäßig in Anspruchskonkurrenz.[1055] Das haftungsrechtliche Sonderregime der DS-GVO ist, soweit es lediglich um die Verletzung von Pflichten aus der DS-GVO selbst geht, auf eine Ergänzung durch nationales Haftungsrecht hinsichtlich einer Anspruchsgrundlage nicht angewiesen und deckt alle Fälle genuin datenschutzrechtlicher Pflichtverletzungen selbst ab. Daher würde die Anwendung von § 280 Abs. 1 S. 2 BGB nicht auf einer anderen Norm im Sinne des vierten Satzes des 146. Erwägungsgrunds der DS-GVO beruhen.[1056] Insbesondere ist nicht auszuschließen, dass in Einzelfällen die Auslegungen von Art. 82 Abs. 3 DS-GVO einerseits und § 280 Abs. 1 S. 2 BGB andererseits divergieren und womöglich die Haftung nach § 280 Abs. 1 BGB weiter gehen könnte. Hier gebietet jedoch der abschließende Charakter von Art. 82 DS-GVO für Verletzungen der DS-GVO[1057] dessen Vorrang.

[1051] Dazu noch unten, Text bei § 5, Fn. 1174.

[1052] *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 13; *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 18.

[1053] *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 20 f.; *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 67; *Kreße*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 82 Rn. 27; *Quaas*, in: BeckOK Datenschutzrecht, 29. Ed. 2019, Art. 82 DS-GVO Rn. 11; *Moos/Schefzig*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 82 DS-GVO Rn. 104; wohl auch *Nemitz*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 82 Rn. 7; ferner *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 20, aber mit der Grenze des Effektivitätsgrundsatzes; siehe auch für das BDSG aF die Nachweise in § 5, Fn. 1022.

[1054] Wie hier *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 82 DS-GVO Rn. 32.

[1055] Allgemein zur Anspruchskonkurrenz zwischen vertraglicher und deliktischer Haftung *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, Vor 823 Rn. 78, 82 ff.; eingehend *Schlechtriem*, Vertragsordnung und außervertragliche Haftung, 27 ff.

[1056] Siehe oben, § 5 C.III.1.

[1057] Siehe nochmals oben, § 5 C.III.1.

d) Zusammenfassung zu vertraglichen Nebenpflichten

Die Auslegung eines auf eine Datenverarbeitung abzielenden Vertrags zwischen einem datenschutzrechtlich Verantwortlichen und einer betroffenen Person nach §§ 133, 157 BGB fordert zwar nur, wesentliche Pflichten der DS-GVO zugleich als vertragliche Nebenpflichten nach § 241 Abs. 2 BGB anzusehen. Dies umfasst die Pflichten nach Art. 83 Abs. 5 DS-GVO mit Ausnahme der Regeln zur Einwilligung.

Nichtsdestoweniger ist hinsichtlich *aller* datenschutzrechtlichen Pflichten eine Zurechnung von Pflichtverletzung und Verschulden nach § 278 BGB möglich. Denn die Datenverarbeitung begründet nach hier vertretener Auffassung grundsätzlich ein Sonderrechtsverhältnis, sodass es auf die vertragliche Radizierung der Pflichten nicht entscheidend ankommt. Die Anwendung von § 278 BGB widerspricht auch nicht dem Anwendungsvorrang des Unionsrechts, da auch datenschutzrechtlich die besseren Gründe für eine strikte Haftung des Verantwortlichen für seine Erfüllungsgehilfen, inklusive der Auftragsverarbeiter, sprechen. Daneben bedarf es einer Haftung aus § 280 Abs. 1 BGB wegen Verletzung einer unmittelbar aus der DS-GVO abgeleiteten Nebenpflicht gemäß § 241 Abs. 2 BGB nicht; sie wird von Art. 82 Abs. 1 DS-GVO als *lex specialis* verdrängt.

3. Haftung aus culpa in contrahendo *und Bereicherungsrecht*

Mögliche vertragsähnliche und bereicherungsrechtliche Ansprüche zwischen einem datenschutzrechtlich Verantwortlichen und einer betroffenen Person können hier nicht umfassend erörtert werden.[1058] Sie waren, soweit sie für die hier behandelten Leitfälle relevant sind, bereits verschiedentlich Gegenstand der Analyse, sodass an dieser Stelle eine Zusammenfassung des bislang Erarbeiteten genügen kann.

Eine Haftung aus *culpa in contrahendo* kommt nach der Rechtsprechung im hier verhandelten Kontext insbesondere dann in Betracht, wenn der Verantwortliche die Verwendung unwirksamer Vertragsbedingungen zu vertreten hat.[1059] Der Anspruch ist dann auf das negative Interesse gerichtet, sodass im Vertrauen auf die Wirksamkeit der Regelung durch den Nutzer getätigte Aufwendungen ersetzt werden können.[1060] Der Vertragspartner kann jedoch zum Schutze der negativen Privatautonomie der Anbieter nicht so gestellt werden, als sei eine wirksame Klausel vereinbart worden.[1061] Anerkannt ist diese

[1058] Zu einer Geschäftsführung ohne Auftrag bei Leistungen zur Erfüllung einer unwirksamen Vertragsklausel, siehe BGH NJW 2009, 2590 (2591 ff.).

[1059] *Emmerich*, in: MüKo, BGB, 8. Aufl. 2019, § 311 Rn. 183; *Sutschet*, in: BeckOK, 51. Ed. 2019, § 311 Rn. 70; siehe auch oben, Text bei § 5, Fn. 846.

[1060] BGH NJW 2009, 2590.

[1061] BGH NZM 2011, 478 Rn. 2; *Graf von Westphalen*, NJW 2012, 2243 (2244); *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 306 Rn. 49.

Variante der *culpa in contrahendo* für die AGB-rechtliche Unwirksamkeit[1062] ebenso wie für jene nach § 138 BGB.[1063] Darin kann jeweils eine Verletzung vorvertraglicher Rücksichtnahmepflichten liegen.[1064] Zudem sind die wesentlichen datenschutzrechtlichen Pflichten auch im vorvertraglichen Bereich als Nebenpflichten nach § 241 Abs. 2 BGB zu qualifizieren, sodass ihre Verletzung grundsätzlich einen Anspruch aus *culpa in contrahendo* auslösen könnte,[1065] der aber wiederum von Art. 82 Abs. 1 DS-GVO als *lex specialis* verdrängt wird.[1066] Insofern lässt sich die obige Argumentation zu vertraglichen Nebenpflichten übertragen.[1067]

Hinsichtlich einer bereicherungsrechtlichen Rückabwicklung einer bereits vollzogenen, aber nicht wirksam zustande gekommenen datenbasierten Austauschbeziehung wurden die maßgeblichen Wertungskriterien ebenfalls bereits entwickelt.[1068] Demnach scheitert ein Wertersatzanspruch des Anbieters gem. §§ 812 Abs. 1 S. 1, 818 Abs. 2 BGB wegen in der Vergangenheit liegender Nutzung des Produkts durch den Nutzer entweder an § 817 S. 2 BGB oder am Effektivitätsgrundsatz des Unionsrechts. Ein bereicherungsrechtlicher Anspruch des Nutzers auf Herausgabe der überlassenen Daten tritt hingegen in Anspruchskonkurrenz zu den datenschutzrechtlichen Abwicklungsansprüchen nach Art. 17 Abs. 1 und Art. 20 Abs. 1 DS-GVO.

4. Deliktische Haftung

Das Deliktsrecht schließlich stellt nicht nur, aber insbesondere auch dann einen rechtlichen Rahmen für das Rechtsverhältnis zwischen betroffener Person und datenschutzrechtlich Verantwortlichem bereit, wenn zwischen beiden kein Vertragsverhältnis besteht. Dies ermöglicht insbesondere die Erfassung von Drittkonstellationen, welche den Kern der drei Leitfälle des zweiten Teils ausmachen. Die obigen Ausführungen haben gezeigt, dass eine vertragliche Bindung hier häufig scheitert, sofern sie nicht ausdrücklich vereinbart wird.[1069] Im Zentrum des Interesses steht dann das Verhältnis deliktischer Schadensersatzansprüche aus den §§ 823 ff. BGB zu dem unionsrechtlichen Schadensersatzanspruch nach Art. 82 DS-GVO. Ferner kommen auch Unterlassungs- und

[1062] BGH NJW 2009, 2590; BGH NJW 1988, 197 (198); BGH NJW 1984, 2816 (2817); OLG Köln NJW-RR 1995, 1333 (1334); *Graf von Westphalen*, NJW 2012, 2243 (2244); *Basedow*, in: MüKo, BGB, 8. Aufl. 2019, § 306 Rn. 49.

[1063] BGH NJW 1987, 639.

[1064] BGH NJW 2009, 2590; BGH NJW 1987, 639 (640).

[1065] *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 23; allgemein für Anspruchskonkurrenz *Kreße*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 82 Rn. 27.

[1066] Vgl. auch *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 82 DS-GVO Rn. 32.

[1067] Siehe oben, § 5 C.III.2.c).

[1068] Siehe oben, § 5 C.I.1.c)aa) und § 5 C.I.1.c)bb)(2)(b).

[1069] Siehe inbesondere § 5 B., aber auch § 6 B.I.-II.

Beseitigungsansprüche analog § 1004 Abs. 1 BGB[1070] bzw. nach Art. 17 DS-GVO[1071] in Betracht, die hier jedoch nicht im Einzelnen untersucht werden können.[1072] Vielmehr liegt der Fokus auf den spezifischen Wechselwirkungen zwischen dem Regime der DS-GVO und § 823 Abs. 1 BGB (a)), § 823 Abs. 2 BGB (b)), § 824 BGB (c)), § 826 BGB (d)) und § 831 BGB (e)). Eine Zusammenfassung rundet die Ausführungen ab (f)).

a) § 823 Abs. 1 BGB i. V. m. sonstigen, datenschutzbezogenen Rechten

Eine Haftung von datenschutzrechtlich Verantwortlichen aus der Zentralnorm des deutschen deliktischen Schadensersatzrechts, § 823 Abs. 1 BGB, kommt grundsätzlich in mehrfacher Hinsicht in Betracht. Zu untersuchen ist hier insbesondere, welche datenschutzrechtlich aufgeladenen Rechtspositionen als sonstige Rechte im Sinne der Norm gelten können.

aa) Das unionale Datenschutzgrundrecht

Nicht undenkbar wäre es zunächst, § 823 Abs. 1 BGB in Verbindung mit dem unionsrechtlichen Datenschutzgrundrecht aus Art. 8 GRCh zur Anwendung zu bringen.[1073] Letzteres gilt nach neuerer EuGH-Rechtsprechung[1074] wohl

---

[1070] OLG Hamburg, NJW-RR 2011, 1611; OLG Hamm, NJW 1996, 131 (jeweils zum BDSG aF); zur DS-GVO *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 20; *Quaas*, in: BeckOK Datenschutzrecht, 29. Ed. 2019, Art. 82 DS-GVO Rn. 12; *Spindler/Horváth*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 82 DS-GVO Rn. 5; *Bamberger*, in: BeckOK BGB, 51. Ed. 2019, § 12 Rn. 231; *Forst*, AuR 2010, 106 (111).

[1071] LG Frankfurt a. M. ZD 2019, 410 Rn. 30 ff.

[1072] Hierzu nun umfassend *C. Becker*, Das Recht auf Vergessenwerden, 2019, 147 ff.; *Ausloos*, The Right to Erasure in EU Data Protection Law, 2020; zur Rechtslage vor Geltungsbeginn der DS-GVO auch *Neunhoeffer*, Das Presseprivileg im Datenschutzrecht, 2005, 172 ff.

[1073] Vgl. etwa *Bamberger*, in: BeckOK BGB, 51. Ed. 2019, § 12 Rn. 124; *Jacquemain*, RDV 2017, 227 (231) (nach DS-GVO unzulässige Datenverarbeitung als Verstoß gegen das Datenschutzgrundrecht).

[1074] Der EuGH hat in seiner jüngeren Rechtsprechung zumindest einigen Chartagrundrechten (Art. 21 Abs. 1 und Art. 31 Abs. 2 GRCh) bereits unmittelbare Horizontalwirkung zugebilligt, siehe EuGH, Urt. v. 17.4.2018 – Rs. C-414/16 (*Egenberger*) – Rn. 76; Urt. v. 11.9.2018 – Rs. C-68/17 (*IR*) – Rn. 69; Urt. v. 6.11.2018 – verb. Rs. C-569/16 und C-570/16 (*Bauer und Willmeroth*) – Rn. 89 f., 92; EuGH, Urt. v. 22.1.2019 – Rs. C-193/17 (*Cresco Investigation*) – Rn. 79 f.; zuvor bereits GA *Tizzano*, Schlussanträge v. 30.6.2005 – Rs. C-144/04 (*Mangold*) – Rn. 84; in diese Richtung auch EuGH, Urt. v. 8.4.1976 – Rs. 43/75 (*Defrenne*) – Rn. 38/39; zustimmend etwa *Ciacchi*, 5 European Journal of Comparative Law and Governance 2018, 207; *dies.*, 15 European Review of Contract Law 2018, 84 (86 f.); *Jacobs*, RdA 2018, 263 (267); *Sagan*, EuZW 2018, 381 (387); *Wienbracke*, NZA-RR 2018, 349 (350); *Mörsdorf*, JZ 2019, 1066 (1071 f.) mit der zutreffenden Einschränkung der Eröffnung des Anwendungsbereichs des jeweiligen Grundrechts durch die Durchführung von Unionsrecht; allgemein für eine horizontale Direktwirkung *Unseld*, Zur Bedeutung der Horizontalwirkung von EU-Grundrechten, 2019, 225 ff., 233 f.; kritisch zu den EuGH-Urteilen *Classen*, EuR 2018, 752 (763 f.); *Kainer*, NZA 2018, 894 (898 f.); *Classen*, JZ 2019, 1057 (1063 f.); *Fornasier*, GPR

auch unmittelbar zwischen Privaten,[1075] wie dies im Übrigen zwar nicht beim deutschen Recht auf informationelle Selbstbestimmung,[1076] wohl aber auch beim österreichischen Datenschutzgrundrecht der Fall ist.[1077] Das Bundesverfassungsgericht geht zwar in der Rechtssache *Recht auf Vergessen II*, im Rahmen seiner nunmehr beanspruchten Kompetenz zur Prüfung von Unionsrecht auch am Maßstab der Unionsgrundrechte,[1078] von einer privatrechtlichen Wirkung des Datenschutzgrundrechts lediglich „ähnlich" der mittelbaren Drittwirkung aus.[1079] Es unterlässt dabei jedoch jegliche Auseinandersetzung mit der entgegenstehenden Rechtsprechung des EuGH, die in der Sache eindeutig erscheint.

Das unionale Datenschutzgrundrecht ist, genauso wie Art. 21 Abs. 1 GRCh und Art. 31 Abs. 2 GRCh, für die der EuGH bereits eine unmittelbare Horizontalwirkung angenommen hat,[1080] einerseits durch hinreichend bestimmte[1081] und inhaltlich unbedingte[1082] primärrechtliche Bestimmungen und ins-

2019, 141 (146 f.); *Sittard/Esser*, jm 2019, 284 (287); früh bereits in dieser Richtung *Metzger*, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, 2009, 352; *Fornasier*, 23 European Review of Private Law 2015, 29 (32 ff.); tendenziell eine unmittelbare Adressierung Privater durch EU-Grundrechte ablehnend auch *Starke*, EU-Grundrechte und Vertragsrecht, 2016, 176 f., 202 ff.; ähnlich *Riesenhuber*, EU-Vertragsrecht, 2013, 30; *Franzen*, Privatrechtsangleichung durch die Europäische Gemeinschaft, 1999, 252; *Preis*, NZA 2006, 401 (402).

[1075] Kritisch *Kainer*, NZA 2018, 894 (899), der diese Wirkung auf Art. 21 Abs. 1 GRCh beschränken möchte.

[1076] Die herrschende Meinung in Deutschland möchte dem Recht auf informationelle Selbstbestimmung lediglich mittelbare Drittwirkung zuerkennen, siehe nur BVerfG GRUR 2020, 74 Rn. 86 – Recht auf Vergessen I; *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 47 f.; *Di Fabio*, in: Maunz/Dürig, GG, 86. EL Januar 2019, Art. 2 Rn. 191; für eine staatsgleiche Grundrechtsbindung Privater durch Datenschutzgrundrechte bei essenziellen Infrastrukturleistungen *Roßnagel*, NJW 2019, 1 (4); allgemein zur lediglich mittelbaren Drittwirkung und zur situativen Ausstrahlung auf Private BVerfG NJW 2018, 1667 Rn. 31 ff. – Stadionverbot; dazu und zu einer möglichen Übertragung auf große Onlineunternehmen f. *Michl*, JZ 2018, 911 (918); *Raue*, JZ 2018, 961 (965 f.); *Grünberger/Washington*, JZ 2019, 1104 (1105); *Hellgardt*, JZ 2018, 901 (Grenze zur unmittelbaren Drittwirkung überschritten); siehe auch, zu einer möglichen Grundrechtsbindung von Facebook, BVerfG NJW 2019, 1935 Rn. 15; nunmehr im Kontext des Datenschutzgrundrechts nochmals angesprochen von BVerfG GRUR 2020, 74 Rn. 88 – Recht auf Vergessen I.

[1077] *Ennöckl*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, 2014, 210 ff.

[1078] BVerfG GRUR 2020, 88 Rn. 50 – Recht auf Vergessen II; dazu *Kühling*, NJW 2020, 275 (277).

[1079] BVerfG GRUR 2020, 88 Rn. 97 – Recht auf Vergessen II; ebenso *Streinz/W. Michl*, EuZW 2011, 384 (387).

[1080] Siehe oben, § 5, Fn. 1074.

[1081] Diese hinreichende Bestimmtheit lässt sich zwar, gerade für spezifische Ableitungen, mit beachtlichen Argumenten für Art. 21 Abs. 1 GRCh bezweifeln, siehe GA *Bobek*, Schlussanträge v. 25.7.2018 – Rs. C-193/17 (*Cresco Investigation*) – Rn. 131–138; *Piepenbrock*, GPR 2019, 93 (95); wenn man allerdings den Maßstab des EuGH, der *Bobek* gerade nicht folgte, anlegt, so ist Art. 8 GRCh ebenfalls sicherlich hinreichend bestimmt bzw., in der Diktion des EuGH, zwingend, siehe EuGH, Urt. v. 22.1.2019 – Rs. C-193/17 (*Cresco Investigation*) – Rn. 76.

besondere das Grundrecht in Art. 8 GRCh garantiert und andererseits auf eine Regelung von Rechtsverhältnissen gerade auch zwischen Privaten angelegt.[1083] Der Gerichtshof beruft sich zur Begründung der unmittelbaren Adressierung Privater durch Unionsgrundrechte auf die äquivalente Rechtsprechung zu den Grundfreiheiten.[1084] In der Rechtssache *Angonese* führte er als ein entscheidendes Argument denn auch gerade an, dass die Überwindung von Hindernissen für die Geltung der Grundfreiheiten durch die Bindung der öffentlichen Gewalt nicht durch private Regelwerke zunichte gemacht werden darf.[1085] Genau diese Gefahr der Wiederaufrichtung von Einschränkungen der effektiven Gewährleistung von Primärrecht besteht jedoch gleichermaßen im Datenschutzrecht: Hier sind im Rahmen der digitalen Wirtschaft besonders private Abreden für die Ausgestaltung des Schutzes der Privatsphäre und die effektive Reichweite des Datenschutzes maßgeblich. Aus diesem Grund differenziert die DS-GVO jedenfalls grundsätzlich auch nicht zwischen öffentlichen und privaten Verarbeitern.[1086] Daher erscheint nach der insoweit maßgeblichen Rechtsprechung des EuGH eine horizontale Direktwirkung von Art. 8 Abs. 1 GRCh fast zwingend.

Daraus ließe sich eine privatrechtliche Zuweisungs- wie auch eine Ausschlussfunktion gegenüber jedermann konstruieren,[1087] mit einem Abwägungsvorbehalt (vgl. Art. 6 Abs. 1 lit. f DS-GVO) wie bei anderen Rahmenrechten auch.[1088] Insofern ist jedoch, wie dargestellt, Art. 82 DS-GVO *lex specialis*, soweit es um Verstöße geht, die zugleich Verletzungen der DS-GVO darstellen. Denn diesbezüglich ist gerade keine andere Rechtsvorschrift des Unionsrechts, wie es der vierte Satz des 146. Erwägungsgrunds der DS-GVO voraussetzt,[1089] betroffen. Sofern das unionale Datenschutzgrundrecht verletzt wird, ohne dass die DS-GVO einschlägig ist (etwa beim Datenschutzgrundrecht von

[1082] Dies könnte man allenfalls für Art. 16 Abs. 1 AEUV in Ansehung der Kompetenzvorschrift des Art. 16 Abs. 2 AEUV bezweifeln. Allerdings ist Art. 16 Abs. 1 AEUV, anders als Art. 27 GRCh, für seine Operationalität nicht logisch zwingend auf eine Ausfüllung durch Sekundärrecht angewiesen; dies legt auch die Rechtsprechung zum Recht auf informationelle Selbstbestimmung nahe, das ja neben dem BDSG durchaus auch einen eigenständigen Gehalt hat.

[1083] Vgl. *Kainer*, NZA 2018, 894 (898 f.).

[1084] EuGH, Urt. v. 17.4.2018 – Rs. C-414/16 (*Egenberger*) – Rn. 77.

[1085] EuGH, Urt. v. 6.6.2000 – Rs. C-281/98 (*Angonese*) – Rn. 32.

[1086] Vgl. nur *Lynskey*, The Foundations of EU Data Protection Law, 2015, 15 ff.

[1087] Zu diesen Voraussetzungen für nach § 823 Abs. 1 BGB absolut geschützte Rechtspositionen statt vieler BGH NJW 2012, 2034 Rn. 23; *Jansen*, Die Struktur des Haftungsrechts, 2003, 469 ff.; *Zech*, Information als Schutzgegenstand, 2012, 64 ff., besonders 73; *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, § 823 Rn. 162 f.; konkret zu personenbezogenen Daten *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 228 ff.; *Zech*, Information als Schutzgegenstand, 2012, 215–217; einen Zuweisungsgehalt ablehnend *Härting*, CR 2016, 646 (648); zur Multirelationalität personenbezogener Daten bereits oben, § 3 A.III.

[1088] Vgl. *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 229; *Zech*, Information als Schutzgegenstand, 2012, 219.

[1089] Siehe oben, § 5 C.III.1.

juristischen Personen[1090]), erscheint es hingegen näher liegend und schon aufgrund der Harmonisierungswirkung vorzugswürdig, Art. 82 DS-GVO analog anzuwenden, statt auf § 823 Abs. 1 BGB zu rekurrieren.[1091] Eine Berücksichtigung des unionalen Datenschutzgrundrechts im Rahmen von § 823 Abs. 1 BGB ist daher letztlich abzulehnen.

bb) Das deutsche allgemeine Persönlichkeitsrecht im weiteren Sinne

Deutlich stärker und kontrovers diskutiert wird demgegenüber, inwiefern neben Art. 82 DS-GVO ein Anspruch aus § 823 Abs. 1 BGB in Verbindung mit dem allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) bestehen kann. Dieses hatte bekanntlich ursprünglich der BGH bereits aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gerade auch für den Verkehr unter Privaten entwickelt[1092] und in der Folge als sonstiges Recht im Rahmen von § 823 Abs. 1 BGB anerkannt.[1093]

Auch hier sind die Anwendungsvoraussetzungen neben Art. 82 DS-GVO bislang noch nicht hinreichend geklärt. Zum Teil wird pauschal von einer Anspruchskonkurrenz ausgegangen,[1094] von anderen hingegen ein Rückgriff auf § 823 Abs. 1 BGB rundweg abgelehnt.[1095] Die Anspruchskonkurrenz von datenschutzrechtlichem Schadensersatzanspruch und § 823 Abs. 1 BGB wegen Verletzung des allgemeinen Persönlichkeitsrechts entsprach der ganz herrschenden Meinung zu § 7 BDSG aF. Damals urteilte das BAG: „Soweit das BDSG eingreift, stellt die Schadensersatzregelung in § 7 BDSG keine ausschließliche Regelung dar, sie verdrängt den auf § 823 I BGB gestützten Anspruch auf Geldentschädigung wegen einer schweren Persönlichkeitsrechtsverletzung nicht."[1096] Nach hier vertretener Auffassung wird man unter Geltung

---

[1090] EuGH, Urt. v. 9.11.2010 – Rs. C-92/09 und C-93/09 (*Schecke*) – Rn. 52 f.; dazu oben, Text bei § 4, Fn. 193.

[1091] Gegen die Anerkennung eines absolut geschützten Rechts i. S. v. § 823 Abs. 1 BGB an eigenen persönlichen Daten über das BDSG aF hinaus auch *Zech*, Information als Schutzgegenstand, 2012, 217–220; siehe auch BGH NJW 2009, 2888 Rn. 30: „Allerdings hat der Einzelne keine absolute, uneingeschränkte Herrschaft über ‚seine' Daten; denn er entfaltet seine Persönlichkeit innerhalb der sozialen Gemeinschaft. In dieser stellt die Information, auch soweit sie personenbezogen ist, einen Teil der sozialen Realität dar, der nicht ausschließlich dem Betroffenen allein zugeordnet werden kann."

[1092] BGH NJW 1954, 1404 (1405).

[1093] BGH NJW 1957, 1146 (1147); BGH NJW 1958, 1344.

[1094] *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 25; *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 82 DS-GVO Rn. 32; *Quaas*, in: BeckOK Datenschutzrecht, 29. Ed. 2019, Art. 82 DS-GVO Rn. 11; *Moos/Schefzig*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 82 DS-GVO Rn. 103; siehe die allerdings unverständliche Formulierung bei *Jacquemain*, RDV 2017, 227 (232), wonach Art. 82 Abs. 1 DS-GVO *lex specialis* zu deutschem Deliktsrecht sein, dieses aber nicht verdrängen soll.

[1095] *Kreße*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 82 Rn. 27.

[1096] BAG NJW 2015, 2749 (2750); siehe aber sogleich die abweichende Verhältnisbestimmung des BGH, Text bei § 5, Fn. 1159.

der DS-GVO jedoch stärker als bisher, und auch stärker als es bislang die Literatur tut, zwischen verschiedenen Teilaspekten des allgemeinen Persönlichkeitsrechts differenzieren müssen.

(1) Recht auf informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung, gespeist aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, beinhaltet die Befugnis des Einzelnen, grundsätzlich selbst über die Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten zu bestimmen.[1097] Es stellt eine eigenständige Ausprägung des allgemeinen Persönlichkeitsrechts dar[1098] und zielt letztlich, zumindest mittelbar, auf die Freiheit von Verhalten und die freie Entfaltung der Persönlichkeit.[1099] Nach der Rechtsprechung des Bundesverfassungsgerichts entfaltet es „als objektive Norm seinen Rechtsgehalt auch im Privatrecht und strahlt in dieser Eigenschaft auf die Auslegung und Anwendung privatrechtlicher Vorschriften aus."[1100]

(a) Art. 82 DS-GVO als *lex specialis* im Allgemeinen

Ansprüche gestützt auf § 823 Abs. 1 in Verbindung mit dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG wurden vor Geltungsbeginn der DS-GVO regelmäßig und unproblematisch als möglich angesehen.[1101] Sie scheiden im Kontext der DS-GVO jedoch nach hier vertretener Auffassung aus.[1102] Denn soweit die DS-GVO gemäß Art. 51 Abs. 1 S. 1 GRCh durchgeführt wird, sind nach der Solange II-Rechtsprechung des Bundesverfassungsgerichts[1103] die Grundrechte des Grundgesetzes kein Prü-

[1097] Grundlegend BVErfG NJW 1984, 419 (422); ferner BVerfG NJW 1991, 2411; OLG Düsseldorf, Urt. v. 21.8.2015, BeckRS 2016, 3782, Rn. 22; umfassend *Albers*, Informationelle Selbstbestimmung, 2005; ferner *Jarass*, NJW 1989, 857 (858 f.); *Kühling/Sackmann*, JURA 2018, 364 (365 ff.); *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, 31 ff.

[1098] BVErfG NJW 1984, 419 (421 f.); BVerfG NJW 1991, 2411; BVerfG GRUR 2020, 74 Rn. 84 – Recht auf Vergessen I; OLG Düsseldorf, Urt. v. 21.8.2015, BeckRS 2016, 3782, Rn. 22; *Jarass*, NJW 1989, 857 (858 f.); *Di Fabio*, in: Maunz/Dürig, GG, 86. EL Januar 2019, Art. 2 Rn. 171.

[1099] Siehe oben, § 3, Fn. 138.

[1100] BVerfG NJW 1991, 2411; *Di Fabio*, in: Maunz/Dürig, GG, 86. EL Januar 2019, Art. 2 Rn. 191; *Schantz*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 174; *Wente*, NJW 1984, 1446 (1446 f.); *Ehmann*, AcP 188 (1988), 230 (379) (jeweils mittelbare Drittwirkung); weitergehend *Trute*, JZ 1998, 822 (8256) (vollständige Angleichung öffentlich-rechtlicher und privatrechtlicher Gewährleistung); *Linnenkohl et al.*, BB 1988, 57 (59 ff.) (unmittelbare Drittwirkung); wohl ebenso *Simitis*, NJW 1984, 398 (400).

[1101] Siehe nur BGH GRUR 2015, 92 Rn. 15; BGH NJW 1991, 1532 (1533); OLG Köln ZUM 2008, 869 (874).

[1102] Gegen ein umfassendes privatrechtliches Recht auf informationelle Selbstbestimmung auch *Zech*, Information als Schutzgegenstand, 2012, 227–229; ein solches als Recht an den eigenen Daten bejahend *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 229.

[1103] BVerfG NJW 1987, 577 (582) – Solange II; BVErfG NJW 2000, 3124 (3125) – Ba-

fungsmaßstab für sekundäres Gemeinschaftsrecht.[1104] Dies impliziert zwar nicht, dass das nationale Recht auf informationelle Selbstbestimmung notwendig im Wege eines Anwendungsvorrangs durch das unionale Datenschutzgrundrecht verdrängt würde; soweit der Gewährleistungsgehalt identisch ist, besteht dafür kein Grund.[1105] Doch könnte der Schutz durch § 823 Abs. 1 BGB in Verbindung mit dem Recht auf informationelle Selbstbestimmung dann nicht über den durch Art. 82 DS-GVO gewährten hinausgehen,[1106] da die Risiken für die informationelle Selbstbestimmung grundsätzlich gerade abschließend in der DS-GVO adressiert werden.[1107] Insofern stellt sich Art. 82 DS-GVO schlicht als *lex specialis* dar.

(b) Der Bereich der Öffnungsklauseln

Nach nicht unumstrittener, aber wohl herrschender Ansicht kann allerdings parallel zu den Unionsgrundrechten auf das nationale Grundrecht auf informationelle Selbstbestimmung insoweit zurückgegriffen werden, als der nationale Gesetzgeber ihm überlassene legislative Spielräume innerhalb des Regelungsplans der DS-GVO, wie die Öffnungsklauseln, nutzt.[1108] Dieser

---

nanenmarktordnung; BVErfG NVwZ 2007, 937 (938); BVerfG GRUR 2020, 88 Rn. 89 f. – Recht auf Vergessen II.

[1104] Siehe auch, zur Auslegung der Bestimmungen der DSRL und des sie umsetzenden nationalen Rechts im Lichte der Chartagrundrechte, BVerfG GRUR 2020, 88 Rn. 95 – Recht auf Vergessen II. Inhaltsgleiche nationale Vorschriften sind hingegen bei unionsrechtlichen Verordnungen grundsätzlich mit Art. 288 Abs. 3 AEUV nicht vereinbar, wenn dadurch Unsicherheit über Rechtsnatur und Inkrafttreten der Verordnung entstehen und die unmittelbare Geltung der Verordnung aufs Spiel gesetzt würde, siehe EuGH, Urt. v. 7.2.1973 – Rs. 39/72 (*Kommission/Italien*) – Rn. 17; Urt. v. 28.3.1983 – Rs. 272/83 (*Kommission/Italien*) – Rn. 26 f.

[1105] Zur Möglichkeit der parallelen Anwendung von Unionsgrundrechten und nationalen Grundrechten im nicht vollständig unionsrechtlich determinierten Bereich des Fachrechts sogleich; vgl. auch die Ausführungen des Bundesverfassungsgerichts in BVerfG GRUR 2020, 88 Rn. 89 – Recht auf Vergessen II, wo betont wird, dass die Solange II-Rechtsprechung nur bedeutet, dass das Grundgesetz (unter gewissen Vorbehalten) nicht mehr als *Prüfungsmaßstab* für unionsrechtlich determinierte Recht herangezogen wird.

[1106] Vgl. *Ludwigs/Sikora*, JuS 2017, 385 (391) (Anwendungsvorrang von unionalem Datenschutzgrundrecht vor deutschem Recht auf informationelle Selbstbestimmung bei paralleler Anwendung in multipolaren Verhältnissen); ebenso *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 292; *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, 31; *Kühling/Sackmann*, JURA 2018, 364 (377); so nunmehr auch BVerfG GRUR 2020, 74 Rn. 63 ff. – Recht auf Vergessen I; siehe auch *Schantz*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 194.

[1107] Siehe den 10. Erwägungsgrund der DS-GVO; zu einer analogen Anwendung von Art. 82 DS-GVO auf von der DS-GVO nicht erfasste Bereiche des unionalen Datenschutzgrundrechts bereits oben, Text bei § 5, Fn. 1091.

[1108] Umfassend *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 283 ff., besonders 291 ff. zur parallelen Geltung von GG und GRCh, und 353 ff.; siehe ferner *Schantz*, in: Schantz/Wolff, Das neue Datenschutzrecht, 2017, Rn. 194; *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, 31; *Kühling/Sackmann*, JURA 2018, 364 (376); zur Bindung an das Grundgesetz bei der Ausfüllung von Umsetzungsspielräumen BVerfG NJW 2005, 2289

Auffassung hat sich auch das Bundesverfassungsgericht mit der Entscheidung in der Rechtssache *Recht auf Vergessen I* angeschlossen.[1109] Danach können im nicht vollständig unionsrechtlich determiniertem Bereich das Fachrechts (z. B. bei journalistischen Tätigkeiten, die unter Art. 85 DS-GVO fallen) sowohl Unionsgrundrechte als auch Grundrechte des Grundgesetzes Anwendung finden.[1110] Erstere können dabei jedoch nach dem Gericht den Gewährleistungsgehalt letzterer grundsätzlich nicht einschränken,[1111] wenngleich auch die Grundrechte des Grundgesetzes im Lichte der Charta ausgelegt werden müssen, sofern diese parallel anwendbar ist.[1112]

Für das Haftungsrecht legt diese Rechtsprechung für den Bereich der Öffnungsklauseln zunächst eine parallele Anwendung von Art. 82 DS-GVO (als mittelbare Verbürgung des Unionsgrundrechts) und § 823 Abs. 1 BGB i. V. m. dem Recht auf informationelle Selbstbestimmung (als Ausfluss grundgesetzlichen Schutzes) nahe. Dies hält jedoch näherer Betrachtung nicht stand. Denn der Schadensersatzanspruch nach Art. 82 Abs. 1 DS-GVO erfasst ausweislich des fünften Satzes des 146. Erwägungsgrunds der DS-GVO gerade auch die Verletzung von „Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen" der DS-GVO.[1113] Daher ist Art. 82 Abs. 1 DS-GVO auch insofern als *lex specialis* zu § 823 Abs. 1 BGB i. V. m. dem Recht auf informationelle Selbstbestimmung anzusehen. Denn es liegen insoweit gerade keine „anderen Vorschriften" im Sinne des vierten Satzes des 146. Erwägungsgrunds der DS-GVO vor.[1114] Auch die abgedeckten Risiken sind identisch.

Art. 82 DS-GVO sanktioniert daher nicht nur eine Verletzung der DS-GVO selbst, sondern – und hier ist der fünfte Satz des 146. Erwägungsgrunds der DS-GVO ganz explizit – auch eine Verletzung von etwaig darüber hinausgehenden Bestimmungen des durch Öffnungsklauseln ermöglichten nationa-

(2291); BVerfG NJW 2011, 3428 Rn. 88; aus unionsrechtlicher Perspektive räumt diese Möglichkeit ein EuGH, Urt. v. 26.2.2013 – Rs. C-617/10 (*Åkerberg Fransson*) – Rn. 29; Urt. v. 26.2.2013 – Rs. C-399/11 (*Melloni*) – Rn. 60; schon von vornherein scheidet eine parallele Anwendung nationaler Grundrechte aus bei der Konkretisierung autonom auszulegender unbestimmter Rechtsbegriffe der DS-GVO, etwa der Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO, siehe nur *Marsch*, Das europäische Datenschutzgrundrecht, 2018, 354 f.; *Ziegenhorn/von Heckel*, NVwZ 2016, 1585 (1586).

[1109] BVerfG GRUR 2020, 74 Rn. 43 f. – Recht auf Vergessen I.

[1110] BVerfG GRUR 2020, 74 Rn. 43 f. – Recht auf Vergessen I.

[1111] BVerfG GRUR 2020, 74 Rn. 44 – Recht auf Vergessen I.

[1112] BVerfG GRUR 2020, 74 Rn. 60 – Recht auf Vergessen I.

[1113] Dieser lautet: „Zu einer Verarbeitung, die mit der vorliegenden Verordnung nicht im Einklang steht, zählt auch eine Verarbeitung, die nicht mit den nach Maßgabe der vorliegenden Verordnung erlassenen delegierten Rechtsakten und Durchführungsrechtsakten und Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang steht." Dass sich dies auf Art. 82 DS-GVO bezieht, zeigt der erste Satz des 146. Erwägungsgrunds: „Der Verantwortliche oder der Auftragsverarbeiter sollte Schäden, die einer Person aufgrund einer Verarbeitung entstehen, die mit dieser Verordnung nicht im Einklang steht, ersetzen."

[1114] Siehe oben, § 5 C.III.1.

len Rechts[1115] – wie etwa des Rechts auf informationelle Selbstbestimmung im Bereich von Art. 85 DS-GVO.[1116] Dieser Durchgriff durch die Ebenen des Mehrebenensystems ist zwar methodisch gewöhnungsbedürftig, aber in der genannten Passage der DS-GVO klar und deutlich angelegt.

Art. 82 DS-GVO fungiert damit im Bereich der Öffnungsklauseln strukturäquivalent zu § 823 Abs. 2 BGB. Ein Anspruch setzt zunächst die Verletzung einer anderen, in diesem Fall mitgliedstaatlichen, Rechtsnorm voraus. Deren Feststellung obliegt primär den mitgliedstaatlichen Gerichten, auch wenn sich hinsichtlich des Einflusses der Öffnungsklauseln im Einzelfall Entscheidungsbefugnisse des EuGH ergeben können. Die Verletzung der mitgliedstaatlichen Norm löst sodann einen Schadensersatzanspruch nach Art. 82 DS-GVO aus, sofern dessen weitere Voraussetzungen erfüllt sind. Zweifelsfragen hinsichtlich dieser weiteren Tatbestandselemente[1117] müssen im Wege des Vorabentscheidungsverfahrens nach Art. 267 AEUV geklärt werden.[1118] Es steht daher zu vermuten, dass das Recht auf informationelle Selbstbestimmung bei methodisch stringenter Vorgehensweise der Gerichte im privatrechtlichen Bereich erheblich an Bedeutung verlieren wird – sofern der EuGH der hier vorgeschlagenen Interpretation folgt.

(2) Recht auf Gewährleistung der Integrität und Vertraulichkeit von informationstechnischen Systemen

Ganz parallel liegen die Dinge für das Grundrecht auf die Gewährleistung der Integrität und Vertraulichkeit von informationstechnischen Systemen, das vom Bundesverfassungsgericht als weiterer Ausfluss des allgemeinen Persön-

[1115] Siehe nur *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 14.

[1116] So auch *Laue*, in: Laue/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl. 2019, § 11 Rn. 3 („nationale Vorschriften im Zusammenhang mit der Datenschutz-Grundverordnung erlassen"); möglicherweise auch *Becker*, in: Plath, DSGVO/BDSG, 3. Aufl. 2018, Art. 82 DSGVO Rn. 3 („alle Verstöße gegen materielles Datenschutzrecht"); aA *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 24 mit dem Argument, dass mitgliedstaatliche Normen nach Art. 85 DS-GVO die DS-GVO nicht präzisieren; dies ist letztlich Auslegungs- und Wertungsfrage; tendenziell wie *Bergt* auch *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 9.

[1117] Zu denken ist dabei etwa an die Frage, ob Art. 82 Abs. 3 DS-GVO oder ein etwaiges Tatbestandsmerkmal einer mitgliedstaatlichen Norm die maßgebliche Verschuldensregelung darstellen soll. Hier wird es, in Anbetracht des Wortlauts des fünften Satzes des 146. Erwägungsgrunds der DS-GVO („nicht […] im Einklang steht"), darauf ankommen, ob der EuGH für die Verletzung mitgliedstaatlichen Rechts auch das Vorliegen von Verschulden – sofern grundsätzlich national erforderlich – verlangt oder, was angesichts der Regelung in Art. 82 Abs. 3 DS-GVO näher liegt, eine objektive Rechtsverletzung genügen lässt.

[1118] Vgl. auch, zum ähnlichen Problem der parallelen Anwendung von nationalen und Unionsgrundrechten, die Ausführungen zu Art. 267 Abs. 2 und 3 AEUV in BVerfG GRUR 2020, 74 Rn. 72 f. – Recht auf Vergessen I.

lichkeitsrechts entwickelt wurde.[1119] Es „schützt vor Eingriffen in informationstechnische Systeme, soweit der Schutz nicht durch andere Grundrechte […] sowie durch das Recht auf informationelle Selbstbestimmung gewährleistet ist."[1120] Anlass für die Anerkennung war die Erkenntnis, dass vernetzte IT-Systeme einerseits in zunehmendem Umfang Daten speichern, deren Auslesung „weitreichende Rückschlüsse auf die Persönlichkeit des Nutzers bis hin zu einer Profilbildung" ermöglicht,[1121] und andererseits die Vernetzung zu einer technischen Vulnerabilität des Systems führt, gegen die der Nutzer typischerweise machtlos ist.[1122] Das IT-Grundrecht schützt nach dem Bundesverfassungsgericht allerdings lediglich Systeme, „die allein oder in ihren technischen Vernetzungen personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten."[1123] Ob es seiner Anerkennung neben dem Recht auf informationelle Selbstbestimmung bedurfte, darf mit Fug und Recht bezweifelt werden.[1124] Es kann nichtsdestoweniger grundsätzlich, ebenso wie die anderen Ausprägungen des allgemeinen Persönlichkeitsrechts, als sonstiges Recht im Rahmen von § 823 Abs. 1 BGB privatrechtliche Ansprüche auslösen.[1125]

Mit dem unerwünschten Zugriff auf besonders interpretationsmächtige Daten, die auf Endgeräten lagern, adressiert das IT-Grundrecht jedoch genau jene Risiken, die auch den Regelungen der ePrivacy-Richtlinie zugrunde lagen und durch die Nutzer vor einem Zugriff auf Daten, die auf ihren Endgerät gespeichert sind, geschützt werden sollen.[1126] Wie gesehen, wurden deren Normen jedoch weitestgehend, insbesondere hinsichtlich der Einwilligung, bis zum Geltungsbeginn einer möglichen ePrivacy-Verordnung durch die DS-GVO abgelöst.[1127] Ihre Verletzung ist daher durch Art. 82 DS-GVO abgedeckt.[1128] Insoweit gelten daher die Ausführungen zum Recht auf informationelle Selbstbestimmung entsprechend: Art. 82 DS-GVO ist auch insoweit *lex specialis*.

[1119] BVerfG NJW 2008, 822 Rn. 166 ff.; siehe nur *Kühling/Sackmann*, JURA 2018, 364 (370 ff.); *Kühling/Klar/Sackmann*, Datenschutzrecht, 4. Aufl. 2018, 49 ff.

[1120] BVerfG NJW 2008, 822 Rn. 167.

[1121] BVerfG NJW 2008, 822 Rn. 178.

[1122] BVerfG NJW 2008, 822 Rn. 180.

[1123] BVerfG NJW 2008, 822 Rn. 203.

[1124] *Kühling/Sackmann*, JURA 2018, 364 (371).

[1125] Vgl. LG Hamburg, Urt. v. 3.12.2010, BeckRS 2010, 144267 (abgelehnt mangels Schutzbereichsbetroffenheit); ebenso LG Düsseldorf, Urt. v. 9.4.2013, BeckRS 2013, 9039; Anerkennung bei *Roßnagel/Schnabel*, NJW 2008, 3534 (3536); *Bartsch*, CR 2008, 613 (615 f.); *Hoffmann*, CR 2010, 514 (518); *Stieper*, AfP 2010, 217 (221 f.); *Zech*, Information als Schutzgegenstand, 2012, 387.

[1126] Siehe den 65. und 66. Erwägungsgrund der revidierten ePrivacy-Richtlinie; ferner oben, § 4 B.I.4.a)aa).

[1127] Siehe oben, § 4 B.I.4.b).

[1128] Für nicht personenbezogene Daten gilt insofern Art. 82 Abs. 1 DS-GVO analog, siehe oben, Text bei § 4, Fn. 858.

(3) Allgemeines Persönlichkeitsrecht

In Betracht kommt demnach allenfalls eine Verletzung des allgemeinen Persönlichkeitsrechts, soweit es einen Gehalt jenseits des Rechts auf informationelle Selbstbestimmung und des Rechts auf die Gewährleistung der Integrität und Vertraulichkeit von IT-Systemen aufweist.[1129] Das allgemeine Persönlichkeitsrecht gewährt dem Einzelnen einen umfassenden „räumlich und thematisch bestimmten Bereich, der grundsätzlich frei von unerwünschter Einsichtnahme bleiben soll."[1130] Nach der zum BDSG aF vorherrschenden Meinung sollte die Verletzung datenschutzrechtlicher Pflichten in der Regel zu einer Verletzung des allgemeinen Persönlichkeitsrechts und damit auch zu einem Anspruch aus § 823 Abs. 1 BGB führen.[1131] Das Datenschutzrecht war damit, jedenfalls in haftungsrechtlicher Sicht, integraler Bestandteil des allgemeinen Persönlichkeitsrechts. Unklar und umstritten ist hingegen, wie sich dieses Verhältnis im Bereich der deliktischen Haftung nach Geltungsbeginn der DS-GVO darstellt.

(a) Vorrang von § 823 Abs. 1 BGB i. V. m. dem allgemeinen Persönlichkeitsrecht nach dem Bundesverfassungsgericht?

Speziell für das Verhältnis der grundgesetzlichen Rechtspositionen des allgemeinen Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht nunmehr in der bereits genannten Rechtssache *Recht auf Vergessen I* eine wegweisende Abgrenzung vorgenommen.[1132] Im Fall selbst ging es um in einem Onlinearchiv bereitgehaltene Artikel des Nachrichtenmagazins *Der Spiegel* über einen spektakulären, jedoch bereits 1982 verübten Mord. Das Gericht judizierte, dass der verfassungsrechtliche Maßstab für den Schutz gegenüber Gefährdungen durch die Verbreitung personenbezogener Informationen im öffentlichen Raum primär durch die äußerungsrechtlichen Ausprägungen des allgemeinen Persönlichkeitsrechts, und nicht durch das Recht auf informationelle Selbstbestimmung, gewährleistet wird.[1133] Diese Differenzierung wurde zuvor bereits in der Literatur vertreten.[1134] Grund für diese Abgrenzung ist nach dem Bundesverfas-

[1129] BVerfG GRUR 2020, 74 Rn. 79 ff. – Recht auf Vergessen I; dazu sogleich näher.

[1130] BVerfG NJW 2008, 822 Rn. 197.

[1131] *Forst*, AuR 2010, 106 (109 f.) *Wind*, RDV 1991, 16 (17); *Niedermeier/Schröcker*, RDV 2002, 217 (220) (jeweils: BDSG-Verletzung regelmäßig zugleich Verletzung des allgemeinen Persönlichkeitsrechts); BGH NJW 1984, 436; BGH NJW 1984, 1886 (1887): „Jede durch das Bundesdatenschutzgesetz nicht gedeckte Übermittlung personenbezogener Daten stellt eine Verletzung [des allgemeinen Persönlichkeitsrechts] dar"; stärker differenzierend und eine Abwägung im Einzelfall fordernd *Ehmann*, AcP 188 (1988), 230 (267, 270 f.); *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 300; *Jacquemain*, RDV 2017, 227 (234); umgekehrt zur Begrenzung des allgemeinen Persönlichkeitsrechts durch das Datenschutzrecht treffend *Klement*, JZ 2017, 161 (162).

[1132] BVerfG GRUR 2020, 74 Rn. 79 ff. – Recht auf Vergessen I.

[1133] BVerfG GRUR 2020, 74 Leitsatz 2a) und Rn. 90–92 – Recht auf Vergessen I.

[1134] *Kamp*, Personenbewertungsportale, 2011, 130 f.; *C. Becker*, Das Recht auf Verges-

sungsgericht der Umstand, dass vorrangig das allgemeine Persönlichkeitsrecht Schutz gegen die öffentliche *Kommunikation* eines Sachverhalts gewährt, während das Recht auf informationelle Selbstbestimmung die Preisgabe personenbezogener Daten und ihre intransparente Nutzung erfasst.[1135]

Wollte man diesen verfassungsrechtlichen Maßstab der deliktsrechtlichen Beurteilung zugrunde legen, so müssten äußerungsrechtliche Fälle, auch wenn sie mit einer Verarbeitung personenbezogener Daten einhergehen, weiterhin und primär über § 823 Abs. 1 BGB in Verbindung mit dem (nationalen) allgemeinen Persönlichkeitsrecht gelöst werden.[1136] Allenfalls parallel dazu könnte sich ein Anspruch aus Art. 82 DS-GVO ergeben.

(b) Vorrang von Art. 82 DS-GVO nach dem Unionsrecht

Letztlich wird über das haftungsrechtliche Verhältnis von allgemeinem Persönlichkeitsrecht und Art. 82 DS-GVO der EuGH zu entscheiden haben. Der vom Bundesverfassungsgericht in der Entscheidung *Recht auf Vergessen I* artikulierte Abgrenzungsmaßstab kann jedoch jedenfalls für das deliktsrechtliche Haftungsregime aus drei Gründen nicht überzeugen.

(aa) Untrennbarkeit von Datenschutzrecht und Äußerungsrecht im datenverarbeitenden Bereich

Erstens begegnet die Abgrenzung zwischen dem Recht auf informationelle Selbstbestimmung und dem äußerungsrechtlichen Teil des allgemeinen Persönlichkeitsrechts grundlegenden Bedenken.[1137] Denn die Kommunikation personenbezogener Informationen im öffentlichen Raum kann bei Zuhilfenahme von IT-Infrastrukturen gerade nicht als von der Verarbeitung personenbezogener Daten getrennt gedacht werden. Dies zeigt gerade auch der vom Bundesverfassungsgericht entschiedene Fall: Die Veröffentlichung von Informationen über Straftaten ist nachgerade paradigmatisch eine datenschutzrechtliche Fragestellung, jedenfalls nach dem Verständnis der DS-GVO, in der diese Konstellation sogar eine Sonderregelung in Art. 10 erfahren hat. Es scheint daher kaum möglich, die öffentliche Kommunikation von personenbezogenen Daten, wenn diese mit deren informationstechnischer Verarbeitung einhergeht, als analytisch von der Verarbeitung getrennt zu betrachten.

Dies wäre allenfalls denkbar, wenn man das Datenschutzrecht lediglich als Schutz vor der Preisgabe und Nutzung einzelner Daten ohne Berücksichtigung des kommunikativen Zusammenhangs betrachten würde. Dem Bundesverfas-

---

senwerden, 2019, 124, 147; siehe auch *Peifer*, GRUR 2020, 34 (36); vgl. auch *Peifer/Kamp*, ZUM 2009, 185 (186 f.).

[1135] BVerfG GRUR 2020, 74 Rn. 80, 90–92 – Recht auf Vergessen I; zustimmend *Klass*, ZUM 2020, 265 (269, 275).

[1136] *Peifer*, GRUR 2020, 34 (36).

[1137] Kritisch hinsichtlich einer solchen Aufspaltung auch *Peifer*, GRUR 2020, 34 (36).

sungsgericht mag ein derartiges Verständnis für das Recht auf informationelle Selbstbestimmung vorschweben.[1138] Richtigerweise wird man jedoch davon ausgehen müssen, dass jedenfalls das unionale Datenschutzrecht ein derartig enges Verständnis seines Schutzgegenstands hinter sich gelassen hat.[1139] Dies liegt nicht zuletzt daran, dass der EuGH Art. 7 und 8 GRCh typischerweise gemeinsam prüft.[1140] Auch der EGMR geht im Übrigen von einem einheitlichen in Art. 8 EMRK verbürgten Grundrecht aus, das sowohl Persönlichkeitsschutz als auch Datenschutz umfasst.[1141] Anders als im deutschen Recht, wo neben bzw. (logisch betrachtet) über dem Recht auf informationelle Selbstbestimmung das allgemeine Persönlichkeitsrecht auch deliktsrechtlichen Schutz vermittelt, mangelt es ferner im Unionsrecht an einer sekundärrechtlichen Haftung für äußerungsrechtliche Verletzungen außerhalb der DS-GVO. Auch dies dürfte der Tendenz, persönlichkeitsrechtliche Aspekte in die DS-GVO einzubeziehen, Vorschub leisten.

Jedenfalls auf unionsrechtlicher Ebene stellt der Grad der Öffentlichkeit einer Kommunikation von personenbezogenen Daten daher einen überaus relevanten Abwägungsgesichtspunkt für die Zulässigkeit der Datenverarbeitung dar, wie gleich noch zu zeigen ist (sogleich unter [cc]). Auch die Verbreitung von personenbezogenen Informationen im öffentlichen Raum ist daher klassisches Terrain des unionalen Datenschutzrechts, wie schon der bereits thematisierte[1142] Fall *Lindqvist* zeigt,[1143] der als einer der ersten Fälle überhaupt zur DSRL vom EuGH entschieden wurde und die Veröffentlichung von Informationen über die Mitarbeiter einer schwedischen Kirchengemeinde im Internet durch eine Kirchenmitarbeiterin zum Thema hatte.[1144] Das unionale Datenschutzrecht lässt sich daher schlechterdings nicht, wie es das Bundesverfassungsgericht für das Recht auf informationelle Selbstbestimmung reklamiert,[1145] auf die Preisgabe einzelner Daten oder deren intransparente Nutzung unter Ausblendung der kommunikativen Rahmenbedingungen reduzieren.

[1138] BVerfG GRUR 2020, 74 Rn. 90 – Recht auf Vergessen I: Das Recht auf informationelle Selbstbestimmung sei „primär als Gewährleistung zu verstehen, die – neben der ungewollten Preisgabe von Daten auch im Rahmen privater Rechtsbeziehungen […] – insbesondere vor deren intransparenter Verarbeitung und Nutzung durch Private schützt. Es bietet Schutz davor, dass Dritte sich individueller Daten bemächtigen […]."

[1139] Vgl. auch *Peifer*, GRUR 2020, 34 (36).

[1140] Siehe etwa EuGH, Urt. v. 9.11.2010 – Rs. C-92/09 und C-93/09 (*Schecke*) – Rn. 52; Urt. v. 13.5.2014 – Rs. C-131/12 (*Google Spain*) – Rn. 53; *Schiedermair*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Einleitung Rn. 167; *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV, Art. 8 GRCh Rn. 1; so auch BVerfG GRUR 2020, 88 Rn. 98 f. – Recht auf Vergessen II.

[1141] EGMR, NJW 2020, 295 Rn. 86.

[1142] Siehe oben, § 4 A.II.2.b)aa)(1).

[1143] EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 48.

[1144] EuGH, Urt. v. 6.11.2003 – Rs. C-101/01 (*Lindqvist*) – Rn. 2.

[1145] Siehe den Nachweis in § 5, Fn. 1138.

(bb) Differenzen zwischen Grundrechten und Haftungsrecht

Für den Bereich des Haftungsrechts kommt zweitens hinzu, dass die vom Bundesverfassungsgericht vorgenommene verfassungsrechtliche Abgrenzung gerade nicht eins zu eins auf die Unterscheidung der deliktischen Anspruchsgrundlagen übertragen werden kann. Art. 82 DS-GVO und die Problematik einer Verdrängung von Anspruchsgrundlagen des nationalen Deliktsrechts wird vom Bundesverfassungsgericht denn auch gar nicht thematisiert. Das Gericht kapriziert sich in seiner Entscheidung vielmehr auf (die im Streitfall einschlägige) Öffnungsklausel für journalistische Tätigkeiten in Art. 85 DS-GVO, das sog. Medienprivileg.[1146] Daraus folgt die nicht vollständige unionsrechtliche Determination des journalistische Tätigkeiten erfassenden Äußerungsrechts – auch hinsichtlich personenbezogener Daten –,[1147] was wiederum die parallele Anwendbarkeit von nationalen und Unionsgrundrechten überhaupt erst ermöglicht.[1148] In seinem Beschluss betont das Gericht, dass das Unionsrecht im Bereich der Öffnungsklauseln in der Regel gerade nicht auf eine Einheitlichkeit des Grundrechtsschutzes ziele, wenn und soweit den Mitgliedstaaten im Fachrecht Gestaltungsspielräume eröffnet werden.[1149]

Der Verweis auf Öffnungsklauseln wie Art. 85 DS-GVO ist jedoch nach hier vertretener Auffassung für die Bestimmung der deliktischen Anspruchsgrundlage in zweifacher Hinsicht unergiebig. Denn der Schadensersatzanspruch nach Art. 82 Abs. 1 DS-GVO umfasst erstens, wie soeben gesehen,[1150] nach dem fünften Satz des 146. Erwägungsgrunds der DS-GVO gerade auch die Verletzung von Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der DS-GVO – mithin auch den Bereich von Art. 85 DS-GVO. Hinsichtlich der Voraussetzungen der Haftung zielt das Unionsrecht demzufolge, anders als nach Auffassung des Bundesverfassungsgerichts im Bereich des Grundrechtsschutzes, gerade doch auf Einheitlichkeit, zumindest hinsichtlich der Anspruchsgrundlage. Sonst sähen sich Verantwortliche, trotz der grundsätzlichen und für den Haftungsbereich auch hinsichtlich der Öffnungsklauseln im 146. Erwägungsgrund dokumentierten Harmonisierungsbemühungen der DS-GVO, einer Vielzahl potenziell abweichender Schadensersatzregeln gegenüber, was den freien Datenverkehr, immerhin eines der beiden Kernziele der DS-GVO, doch erheblich beeinträchtigen würde.[1151] So bestimmt Art. 82 Abs. 3 DS-GVO etwa, dass eine Haftung des Verantwortlichen ausscheidet,

[1146] BVerfG GRUR 2020, 74 Rn. 51 – Recht auf Vergessen I.
[1147] BVerfG GRUR 2020, 74 Rn. 51 – Recht auf Vergessen I.
[1148] BVerfG GRUR 2020, 74 Rn. 43 f., 50 ff. – Recht auf Vergessen I.
[1149] BVerfG GRUR 2020, 74 Rn. 48 ff. – Recht auf Vergessen I.
[1150] Siehe oben, § 5 C.III.4.a)bb)(1)(b).
[1151] Der EuGH zeigt sich zwar für mitgliedstaatliche Differenzen hinsichtlich des Zugangs zu Informationen im Bereich des Medienprivilegs offen, siehe EuGH, Urt. v. 24.9.2019 – Rs. C-507/17 (*Google/CNIL*) – Rn. 67; allerdings dürften diese Ausführungen angesichts des 146. Erwägungsgrunds der DS-GVO wiederum nicht auf das Haftungsrecht übertragbar sein.

wenn er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Diese Harmonisierung wäre zunichte gemacht, wenn nationales Deliktsrecht etwa eine verschuldensunabhängige Haftung vorsehen könnte.

Für diese Auslegung streitet zweitens auch die Regelung in Art. 85 Abs. 2 DS-GVO, die zwar den Mitgliedstaaten Abweichungsbefugnisse im Bereich des Medienprivilegs einräumt, davon jedoch das Kapitel der DS-GVO zu Sanktionen (Kapitel VIII, Art. 77 ff. DS-GVO) und damit auch Art. 82 DS-GVO gerade ausnimmt.[1152] Vielmehr gilt hier die allgemeine Aussage des ersten Satzes des 153. Erwägungsgrunds der DS-GVO, dass die mitgliedstaatlichen Regeln zum Medienprivileg mit der DS-GVO „in Einklang" gebracht werden müssen, ihr mithin nicht vorgehen. Generell erfasst auch die in Art. 23 DS-GVO vorgesehene mitgliedstaatliche Beschränkungsmöglichkeit zwar die Betroffenenrechte nach Art. 12 ff. DS-GVO, nicht aber das Haftungsregime der Art. 77 ff. DS-GVO.

(cc) Mangelnde Risikospezifizität

Ein drittes Argument ergibt sich aus dem bereits analysierten vierten Satz des 146. Erwägungsgrunds der DS-GVO.[1153] Mit Geltungsbeginn der DS-GVO wird man die dort angelegte Differenzierung zwischen einer Datenverarbeitung nach der DS-GVO und der Verletzung „andere[r] Vorschriften" fruchtbar machen müssen.[1154] Auch hier sind mithin, nach Maßgabe der allgemeinen, oben erarbeiteten Regeln, Risikospezifizität und Zielkompatibilität zur Ermittlung der Reichweite des Anwendungsvorrangs entscheidend.[1155] § 823 Abs. 1 BGB ist daher in Verbindung mit dem allgemeinen Persönlichkeitsrecht im engeren Sinne insoweit anwendbar, als Umstände betroffen sind, die im Rahmen von Art. 82 DS-GVO nicht berücksichtigt werden können. Dies ist insbesondere der Fall, wenn die Verletzung des allgemeinen Persönlichkeitsrechts nicht unmittelbar auf der Datenverarbeitung aufruht.

Soweit jedoch die Verletzung des allgemeinen Persönlichkeitsrechts mit einer von der DS-GVO erfassten Datenverarbeitung zusammenfällt, was bei der Allgegenwärtigkeit elektronisch vermittelter Äußerungsprozesse regelmäßig der Fall ist, wird nach hier vertretener Auffassung § 823 Abs. 1 BGB von Art. 82 Abs. 1 DS-GVO als *lex specialis* verdrängt.[1156] Lediglich juristische

[1152] Vgl. *Dix*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 85 DS-GVO Rn. 26; *Buchner/Tinnefeld*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 85 DS-GVO Rn. 30.

[1153] Siehe oben, § 5 C.III.1.

[1154] Siehe oben, § 5 C.III.1.

[1155] Siehe oben, § 5 A.I.1.

[1156] Ähnlich für § 7 BDSG aF *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 300 (§ 823 Abs. 1 BGB tritt grundsätzlich zurück); unklar insoweit *Jacquemain*, RDV 2017, 227 (232), wonach Art. 82 Abs. 1 DS-GVO *lex specialis* zu § 823 Abs. 1 BGB ist, diesen aber nicht verdrängt.

Personen, die nicht nach Art. 82 DS-GVO anspruchsberechtigt sind, können vollumfänglich auf § 823 Abs. 1 DS-GVO i. V. m. dem allgemeinen Persönlichkeitsrecht[1157] zurückgreifen.[1158] Natürliche Personen hingegen müssen zumeist den Weg über Art. 82 DS-GVO gehen. So hat auch der BGH zum Verhältnis des BDSG aF zu Ansprüchen nach § 823 Abs. 1 BGB geurteilt:

„Bei der Anerkennung [des allgemeinen Persönlichkeitsrechts] handelt es sich jedoch nur um einen sogenannten Auffangtatbestand, der gegenüber einer Spezialregelung des Persönlichkeitsrechts grundsätzlich zurücktritt. Zweifelhaft ist deshalb schon, ob nach Erlaß des Bundesdatenschutzgesetzes über § 823 Abs. 1 BGB Ansprüche infolge einer unzulässigen Datenverarbeitung entstehen können. Soweit das Gesetz die Rechte des Betroffenen aus unzulässiger Datenverarbeitung abschließend regelt, scheidet § 823 Abs. 1 BGB als weitere Anspruchsgrundlage aus."[1159]

Eine solche abschließende Regelung stellte nach Auffassung des BGH der Löschungsanspruch nach § 35 Abs. 3 BDSG aF dar.[1160] Heute wird man grundsätzlich in Art. 82 Abs. 1 DS-GVO eine ebensolche Regelung erblicken müssen. Denn es besteht in der Regel schon kein spezifisches äußerungsrechtliches Risiko, das nicht von der DS-GVO erfasst würde.

Dies zeigt abschließend folgendes Gedankenexperiment: Man stelle sich vor, dass ein Verantwortlicher ein Video aus der Intimsphäre einer betroffenen Person ins Internet hochlädt. Hierbei sind folgende Wechselwirkungen zwischen DS-GVO und allgemeinem Persönlichkeitsrecht denkbar: Wenn eine wirksame datenschutzrechtliche Einwilligung zur Veröffentlichung des Videos besteht (und auch die sonstigen Vorschriften der DS-GVO beachtet wurden), so ist ein Verstoß gegen unionales Datenschutzrecht ausgeschlossen. Zugleich ist das allgemeine Persönlichkeitsrecht nicht verletzt, weil die Einwilligung rechtfertigende Wirkung entfaltet.[1161] Gleiches dürfte für den Fall einer vertragserforderlichen Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO gelten. Besteht jedoch keine wirksame Einwilligung und kein Vertrag, so wird es für die datenschutzrechtliche Erlaubnis regelmäßig auf Art. 6 Abs. 1 lit. f DS-GVO ankommen. Wie gesehen, ist hierfür eine umfassende Interessenabwägung durchzuführen.[1162] Eine ebensolche wäre jedoch auch zur Bestimmung der Verletzung des allgemeinen Persönlichkeitsrechts erforderlich.[1163] Abweichungen in der Beurteilung sind hier nur dann denkbar, wenn für das allgemeine Persön-

[1157] Zu dessen Anwendbarkeit auf juristische Personen *Rixecker*, in: MüKo, BGB, 8. Aufl. 2018, Anhang zu § 12. Das Allgemeine Persönlichkeitsrecht Rn. 31 ff.

[1158] Siehe oben, Text bei und Nachweise in § 5, Fn. 1021.

[1159] BGH NJW 1981, 1738 (1740); siehe auch BGH GRUR 1984, 688 (689); kritisch dazu *Simitis*, NJW 1981, 1697 (1701).

[1160] BGH NJW 1986, 2505 (2606 f.).

[1161] *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, § 823 Rn. 78; *Forst*, AuR 2010, 106 (109).

[1162] Siehe oben, § 4 C.I.2.c).

[1163] Siehe nur BGH NJW 2012, 2197 Rn. 35; *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, § 823 Rn. 364.

lichkeitsrecht Gesichtspunkte relevant sind, die in der datenschutzrechtlichen Interessenabwägung keine Rolle spielen.

Es ist jedoch nicht ersichtlich, dass derartige Aspekte existieren.[1164] Dafür spricht nicht nur, dass der EuGH häufig zusätzlich zu Art. 8 GRCh auch auf den Schutz der Privatsphäre nach Art. 7 GRCh rekurriert.[1165] Vor allem sind die maßgeblichen Gesichtspunkte, die beim allgemeinen Persönlichkeitsrecht eine Rolle spielen, allesamt, wie gesehen,[1166] auch für die datenschutzrechtliche Abwägung bedeutsam, zum Beispiel: die Quelle der Daten,[1167] die Frage der Sensibilität,[1168] die Korrektheit[1169] oder auch die Veröffentlichung zur Unzeit.[1170] Auch der Zweck und die Umstände der Verarbeitung sind hier zu berücksichtigen,[1171] ferner die Frage einer etwaigen Weiterleitung an oder Zugriffsmöglichkeit durch Dritte,[1172] mithin die vom Bundesverfassungsgericht exklusiv dem allgemeinen Persönlichkeitsrecht zugeordneten kommunikativen Umstände. Insbesondere dürfte eine Verarbeitung, die nach deutschem Recht eine Verletzung des allgemeinen Persönlichkeitsrechts darstellt, den vernünftigen Erwartungen der betroffenen Person widersprechen, was nach dem 47. Erwägungsgrund der DS-GVO ein Abwägungsergebnis zugunsten der betroffenen Person indiziert. Letztlich rekurrieren beide Abwägungen daher auf den identischen Argumentationshaushalt. Insofern ist eine weitergehende Haftung des Verantwortlichen nach § 823 Abs. 1 BGB in Verbindung mit dem allgemeinen Persönlichkeitsrecht nicht statthaft, da schon kein spezifisches Risiko durch die nationale Norm adressiert wird. Die Harmonisierungswirkung der DS-GVO gebietet daher in diesen Fällen den Vorrang von Art. 82 Abs. 1 DS-GVO, im Rahmen der Öffnungsklauseln ggf. in Verbindung mit präzisierendem mitgliedstaatlichem Recht.[1173]

[1164] Vgl. auch BGH NJW 1986, 2505 (2606 f.); *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 300.

[1165] Siehe oben, § 5, Fn. 1140.

[1166] Siehe zu den Kriterien ausführlich oben, § 4 C.I.2.c)bb).

[1167] *Herfurth*, ZD 2018, 514 (516 f.).

[1168] *Herfurth*, ZD 2018, 514 (516).

[1169] *Herfurth*, ZD 2018, 514 (517). Denkbar ist etwa, dass ein Interview aufgezeichnet wird und die Verarbeitung der Aufzeichnung grundsätzlich durch eine wirksame Einwilligung gedeckt ist, der Inhalt des Interviews jedoch bei der Veröffentlichung durch eine Zeitung so verfälscht oder verkürzt wird, dass darin nach deutschem Recht eine Verletzung des allgemeinen Persönlichkeitsrechts zu erblicken ist (vgl. nur BGH NJW 1954, 1404 [1405]). Dann ist diese Verarbeitung nicht mehr von der Einwilligung oder einer möglichen Vertragspflicht umfasst; zugleich fällt wegen der Veränderung die Interessenabwägung zugunsten der betroffenen Person aus.

[1170] Auch darin liegen, insbesondere in Verbindung mit dem datenschutzrechtlichen Grundsatz von Treu und Glauben, abwägungsrelevante Umstände.

[1171] *Drewes*, ZD 2019, 296 (298); *Herfurth*, ZD 2018, 514 (519).

[1172] *Herfurth*, ZD 2018, 514 (518 f.); *Robrahn/Bremert*, ZD 2018, 291 (294); vgl. auch *DSK*, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019, 19; *Schantz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 6 Abs. 1 DS-GVO Rn. 105 f.

[1173] Siehe oben, § 5 C.III.4.a)bb)(1)(b).

Schließlich ist auch nicht zu erkennen, dass besonders schwerwiegenden Formen von Persönlichkeitsrechtsverletzungen (Beleidigungen, *hate speech*, Verletzungen der Intimsphäre), die nach herkömmlichem deutschen Verständnis einen Anspruch auf Geldentschädigung wegen immaterieller Schäden nach § 823 Abs. 1 BGB, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG auslösen,[1174] nicht auch im Rahmen von Art. 82 DS-GVO Rechnung getragen werden kann. Denn all jene Faktoren, die bei der Bemessung der Höhe des Schmerzensgeldes nach deutschem Recht relevant sind,[1175] können ohne Weiteres bei der Höhe des immateriellen Schadens, der durch die Datenschutzrechtsverletzung entsteht, berücksichtigt werden. Der 75. Erwägungsgrund der DS-GVO erkennt als datenschutzrechtliche Risiken gerade auch Möglichkeiten der Diskriminierung, der Rufschädigung und erhebliche gesellschaftliche Nachteile an. Insbesondere wird auch die Bewertung persönlicher Aspekte, welche „die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten […] betreffen", genannt. Ferner berücksichtigt die DS-GVO auch die Existenz besonders schutzbedürftiger Personengruppen.[1176] All diese Umstände können und müssen bei der Bemessung des immateriellen Schadensersatzes nach Art. 82 Abs. 1 DS-GVO berücksichtigt werden. Schließlich folgt auch der bei der Geldentschädigung wegen Verletzung des allgemeinen Persönlichkeitsrechts anerkannte Präventionsgedanke[1177] im Rahmen von Art. 82 Abs. 1 DS-GVO zwanglos aus dem Effektivitätsgrundsatz des Unionsrechts.[1178]

Damit zeigt sich, dass die abwägungsrelevanten Gesichtspunkte so oder so zum Tragen kommen – im Rahmen von § 823 Abs. 1 BGB oder von Art. 82 DS-GVO. Der Anwendungsvorrang des Unionsrechts gebietet in diesen Fällen zumindest, dass die unionsrechtliche Beurteilung nicht durch eine abweichende nationale Entscheidung in Frage gestellt wird. Kommen beide Vorschriften, § 823 Abs. 1 BGB und Art. 82 DS-GVO, zum selben Ergebnis, so wäre die Anwendung von § 823 Abs. 1 BGB zwar im Grunde unschädlich; die besseren systematischen Argumente sprechen jedoch nach hier vertretener Ansicht dagegen. Auch wenn man von einer Anspruchskonkurrenz beider Normen aus-

[1174] Grundlegend BGH NJW 1958, 827 (829 f.); ferner BGH NJW 1961, 2059 (2060); aus der jüngeren Rechtsprechung BGH NJW 2010, 763; BGH NJW-RR 2016, 1136 (1137).

[1175] BGH NJW 2005, 215 (Genugtuung des Opfers, Präventionsgedanke und Intensität der Persönlichkeitsrechtsverletzung als Bemessungsfaktoren); dazu *Wagner*, ZEuP 2000, 200 (204 ff.); *Beater*, JZ 2004, 889 (892 f.); *Wagner*, AcP 206 (2006), 352 (380 ff.); ausführlich zu den Faktoren *Rixecker*, in: MüKo, BGB, 8. Aufl. 2018, Anhang zu § 12. Das Allgemeine Persönlichkeitsrecht Rn. 301 ff.

[1176] Siehe wiederum den 75. Erwägungsgrund sowie Art. 8–10, 22 Abs. 4 DS-GVO.

[1177] Siehe bereits die Nachweise in § 5, Fn. 1175.

[1178] Vgl. *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 82 DS-GVO Rn. 27; *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 17; zur Anerkennung des Präventionsgedankens im unionalen Schadensersatzrecht allgemein *Heinze*, Schadensersatz im Unionsprivatrecht, 2017, 546 f.; *Ebers*, Rechte, Rechtsbehelfe und Sanktionen im Unionsprivatrecht, 2016, 286.

gehen wollte, gäbe es jedoch nur ein Gericht, das die Frage der Konkordanz von § 823 Abs. 1 BGB und Art. 82 DS-GVO letztinstanzlich entscheiden könnte: den EuGH. Daher wird es, auf dem ein oder anderen Weg, zu einer erheblichen Verschiebung des Persönlichkeitsrechts ins Unionsprivatrecht kommen.

(c) Zusammenfassung zum Verhältnis von allgemeinem Persönlichkeitsrecht und Art. 82 DS-GVO

Insgesamt lässt sich der vom Bundesverfassungsgericht angenommene Vorrang des allgemeinen Persönlichkeitsrechts im äußerungsrechtlichen Bereich daher auf die Frage der deliktischen Haftung nicht übertragen. Vielmehr stellt sich, sofern die öffentliche Kommunikation mit einer Datenverarbeitung einhergeht, Art. 82 Abs. 1 DS-GVO auch insoweit grundsätzlich als *lex specialis* zu § 823 Abs. 1 BGB dar. Eine eigenständige Bedeutung gewinnt die Haftung nach nationalem Recht nur, sofern dafür Umstände von Belang sind, die im Rahmen der DS-GVO nicht berücksichtigt werden können. Derartige Fälle dürften aber im digitalen Zeitalter selten sein. Daher wird die schadensersatzrechtliche Haftung auf Grundlage des allgemeinen Persönlichkeitsrechts künftig in ganz erheblichem Umfang durch Art. 82 DS-GVO übernommen werden.

b) § 823 Abs. 2 BGB i. V. m. Normen der DS-GVO

In ähnlicher Weise lässt sich auch die Frage lösen, ob die Verletzung von Normen der DS-GVO, deren Schutzgesetzqualität unterstellt, eine Haftung nach § 823 Abs. 2 BGB auslösen können. Die Antwort darauf ist jedenfalls, soviel kann vorab festgehalten werden, unabhängig von der Beurteilung der Normen als Verbotsgesetz nach § 134 BGB.[1179]

Dass die Verletzung datenschutzrechtlicher Vorschriften auch nach § 823 Abs. 2 BGB sanktioniert werden kann, entsprach schon unter der Geltung des BDSG der ganz überwiegenden Meinung.[1180] Mit Geltungsbeginn der DS-GVO ist diese Frage ungleich weniger relevant geworden, da nun auch der Ersatz immaterieller Schäden in Art. 82 Abs. 1 DS-GVO ausdrücklich anerkannt ist und sich der Schädiger gemäß Art. 82 Abs. 3 DS-GVO hinsichtlich seines Verschuldens entlasten muss. Damit ist es für den Geschädigten allemal besser, den Anspruch auf Art. 82 Abs. 1 DS-GVO zu stützen als auf § 823 Abs. 2

[1179] Konkret zum BDSG aF BGH NJW 2007, 2106 Rn. 34.

[1180] BGH NJW 1981, 1738 (1740); BGH NJW 1991, 1532 (1533); OLG Hamburg, NJW-RR 2011, 1611 (zu § 4 BDSG aF); OLG Köln ZUM 2008, 869 (874) (zu § 4 BDSG aF); OLG Frankfurt a. M., Urt. v. 15.11.2004, BeckRS 2005, 11716 Rn. 26 (zu § 28 Abs. 1 Nr. 2 BDSG aF); OLG Hamm, NJW 1996, 131 (zu § 29 Abs. 2 BDSG aF); AG Bamberg, Urt. v. 15.1.2015, BeckRS 2015, 9554 (zu § 43 Abs. 1 Nr. 8a BDSG aF); *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, § 823 Rn. 526; *Forst*, AuR 2010, 106 (110); *Zech*, Information als Schutzgegenstand, 2012, 218 mit zutreffendem Verweis auf die Differenzierung zwischen einzelnen Normen des BDSG aF.

BGB. Die Frage der Anwendbarkeit des letzteren ist daher eher von theoretischem Interesse.

Der überwiegende Teil der Literatur nimmt an, dass auch zwischen Art. 82 Abs. 1 DS-GVO und § 823 Abs. 2 BGB hinsichtlich der Verletzung von in der DS-GVO enthaltenen Schutzgesetzen Anspruchskonkurrenz herrscht.[1181] Zutreffend dürfte demgegenüber jedoch die Auffassung sein, welche auch insoweit Art. 82 Abs. 1 DS-GVO als *lex specialis* ansieht.[1182] Denn nach dem Rechtsgedanken des vierten Satzes des 146. Erwägungsgrunds der DS-GVO ist eine abweichende Bewertung der Haftungssituation durch nationale Vorschriften ohnehin nicht möglich, da gerade nicht die Verletzung von Rechtsvorschriften außerhalb der DS-GVO im Raum steht.[1183] Alle Fälle, die durch § 823 Abs. 2 BGB in Verbindung mit Vorschriften der DS-GVO erfasst werden könnten, werden daher abschließend durch Art. 82 Abs. 1 DS-GVO geregelt.

c) § 824 BGB

§ 824 BGB, der einen Schadensersatzanspruch wegen Kreditgefährdung gewährt, wird nach verbreiteter Ansicht neben Art. 82 DS-GVO für anwendbar gehalten.[1184] Allerdings stellt nach hier vertretener Auffassung Art. 82 DS-GVO wiederum eine *lex specialis* dar.[1185] Denn das Risiko einer Kreditgefährdung durch unwahre Tatsachen wird in der DS-GVO durchaus adressiert, etwa durch den Grundsatz der Datenrichtigkeit, Art. 5 Abs. 1 lit. d DS-GVO,[1186] durch Art. 22 Abs. 3 DS-GVO i. V. m. dem zweiten Absatz des 71. Erwägungsgrunds der DS-GVO und durch den Umstand, dass bei inkorrekten Daten auch die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO regelmäßig zu Gunsten des Betroffenen ausfällt[1187] und daher die Datenverarbeitung rechtswidrig ist. Daher greift Art. 82 DS-GVO wiederum als *lex*

[1181] *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 26; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 20; *Pötters*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 1 DS-GVO Rn. 13; *Quaas*, in: BeckOK Datenschutzrecht, 29. Ed. 2019, Art. 82 DS-GVO Rn. 11; *Nemitz*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 82 Rn. 7 mit Fn. 9; *Moos/Schefzig*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 82 DS-GVO Rn. 103; *Thon*, RabelsZ 84 (2020), 24 (29).

[1182] *Boehm*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 82 DS-GVO Rn. 32; ebenso für § 7 BDSG aF *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 300 Fn. 4.

[1183] Siehe oben, § 5 C.III.1.

[1184] *Gola/Piltz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 82 Rn. 27; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 82 DS-GVO Rn. 20; *Quaas*, in: BeckOK Datenschutzrecht, 29. Ed. 2019, Art. 82 DS-GVO Rn. 11; *Moos/Schefzig*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 82 DS-GVO Rn. 103; für die Anwendbarkeit neben § 823 Abs. 2 i. V. m. § 32 Abs. 2 BDSG aF *Winkelmann*, MDR 1985, 718 (720).

[1185] Ebenso für § 7 BDSG aF *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 300 Fn. 4.

[1186] Siehe dazu oben, § 4 A.III.2.b)(ff).

[1187] *Herfurth*, ZD 2018, 514 (517).

specialis,[1188] sofern die Behauptung oder Verbreitung der kreditgefährdenden, unwahren Tatsache nach § 824 BGB zugleich eine Verarbeitung unrichtiger personenbezogener Daten darstellt. Dies wird unter den Bedingungen des digitalen Zeitalters regelmäßig der Fall sein.[1189] Es ist auch nicht ersichtlich, dass die unionsrechtliche Norm hinter dem Schutzumfang von § 824 BGB zurückbleibt, da auch nach dieser Vorschrift die Unwahrheit der Tatsache und die fahrlässige Unkenntnis des Anspruchsgegners nachgewiesen werden müssen.[1190]

d) § 826 BGB

Eine Sonderstellung im Bereich der deliktischen Datenverarbeitung nimmt § 826 BGB ein. Das Risiko einer sittenwidrigen Verarbeitung bzw. einer schweren Äquivalenzstörung ist in der DS-GVO, wie bereits dargetan, nicht adressiert.[1191] Daher ist § 826 BGB in gleichem Umfang wie § 138 BGB neben der DS-GVO und insbesondere ihrem Art. 82 anwendbar.[1192]

Hinsichtlich des Vorliegens der Sittenwidrigkeit kann allerdings nicht rundweg auf die Ausführungen zu § 138 BGB verwiesen werden. Denn insoweit ist anerkannt, dass der Begriff der Sittenwidrigkeit wegen der funktionalen Unterschiede von § 138 BGB (Grenze der Privatautonomie) zu § 826 BGB (Bewertung und Steuerung deliktischen Handelns) in beiden Normen nicht strikt identisch ausgelegt werden muss.[1193] Insbesondere lässt sich bei einer Äquivalenzstörung fragen, ob bereits bei einem besonders groben Missverhältnis von Leistung und Gegenleistung die Schwelle der Sittenwidrigkeit nach § 826 BGB erreicht ist.

Die Rechtsprechung hat bei wertlosen Kapitalanlagen eine Sittenwidrigkeit angenommen, wenn ein Anbieter „hohe Gewinne […] erzielen [möchte], indem er möglichst viele Geschäfte realisiert, die für den Anleger auf Grund überhöhter Gebühren und Aufschläge chancenlos sind."[1194] Dahinter steht die

---

[1188] Für eine Anpassung der Auslegung von § 824 BGB an § 32 Abs. 2 BDSG aF trat bereits ein *Winkelmann*, MDR 1985, 718 (720).

[1189] Rein physische Transportvorgänge sind von § 824 BGB nicht erfasst, es bedarf vielmehr der Kundgabe der Tatsache aus eigener Überzeugung oder der Mitteilung der Tatsache als Gegenstand fremder Überzeugung, siehe *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, § 824 Rn. 31.

[1190] Siehe nur *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, § 824 Rn. 27, 46 ff.

[1191] Siehe oben, § 5 C.II.2.a)bb)(1).

[1192] Für eine Anwendbarkeit neben der DS-GVO auch *Moos/Schefzig*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 82 DS-GVO Rn. 103; aA für § 7 BDSG aF *Buchner*, Informationelle Selbstbestimmung im Privatrecht, 2006, 300 Fn. 4 (Zurücktreten von § 826 BGB).

[1193] BGH NJW 1970, 657 (658); *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, § 826 Rn. 11; *Oechsler*, in: Staudinger, BGB, 2018, § 826 Rn. 44; *Barkhausen*, NJW 1953, 1666, vgl. auch BGH NJW 1953, 1665; aA (Identität) *Mayer-Maly*, JZ 1996, 419; *Kohte*, NJW 1985, 2217 (2220).

[1194] BGH NZG 2010, 550 (551).

Wertung, das nicht hingenommen werden kann, „uninformierte, leichtgläubige Menschen unter sittenwidriger Ausnutzung ihres Gewinnstrebens und ihres Leichtsinns als Geschäftspartner zu gewinnen und sich auf deren Kosten zu bereichern."[1195] Sie lässt sich nicht nur auf chancenlose Immobiliengeschäfte übertragen,[1196] sondern auch auf das Angebot von dysfunktionalen Produkten, die gegen einen signifikanten Datenpreis überlassen werden.

Darüber hinaus nimmt die Rechtsprechung jedoch auch bei einem „lediglich" auffälligen Missverhältnis im Sinne eines wucherähnlichen Geschäfts eine Sittenwidrigkeit nach § 826 BGB an.[1197] In der Tat ist kein Grund ersichtlich, aus dem für diese Fallgruppe die Bewertung der Sittenwidrigkeit nach § 138 Abs. 1 BGB von denjenigen nach § 826 BGB abweichen sollte.[1198] Allerdings ist bei der Annahme des Schädigungsvorsatzes Zurückhaltung angebracht angesichts der erheblichen Bewertungsschwierigkeiten, die mit datenbasierten Leistungen einhergehen. Lediglich bei dysfunktionalen Produkten wird man den Vorsatz typischerweise bejahen können.[1199] Bei nur funktional beschränkten oder geringwertigen Produkten hingegen, bei denen ein signifikanter Datenpreis zu einer Unwirksamkeit des Vertrags nach § 138 Abs. 1 BGB führt,[1200] dürfte ein Anspruch aus § 826 BGB regelmäßig zumindest an mangelndem Schädigungsvorsatz scheitern.

In der Rechtsfolge ist bei Vorliegen der Voraussetzungen von § 826 BGB Schadensersatz nach Maßgabe der §§ 249 ff. BGB zu leisten. Im Rahmen der insoweit nach § 249 Abs. 1 BGB vorrangigen Naturalrestitution muss der Anbieter die Gegenleistung des Nutzers herausgeben. Lediglich bei Unmöglichkeit oder Unzulänglichkeit der Naturalrestitution kann der Geschädigte Wertersatz nach § 251 Abs. 1 BGB verlangen.[1201] Dabei kann jeweils nicht unterstellt werden, dass ohne die sittenwidrige Äquivalenzstörung ein gerade noch nicht sittenwidriger Vertrag geschlossen worden wäre. Vielmehr ist die tatsächliche Vermögenssituation des Geschädigten mit einer Lage völlig ohne Vertrag zu vergleichen.[1202] Auf die Herausgabe der Gegenleistung muss daher der im Wege des Vertrags erlangte Vorteil, die Leistung des Anbieters, womöglich wertmäßig angerechnet werden.[1203] Dies darf jedoch, wie schon beim berei-

[1195] BGH BKR 2012, 78 Rn. 32.
[1196] *Junglas*, NJOZ 2013, 49 (64).
[1197] So für eine überhöhte Maklerprovision BGH NJW 2000, 2669 (2669 f.); OLG Brandenburg, NJW-RR 2010, 635 (636 f.); für einen Immobilienkaufvertrag OLG Koblenz VersR 2018, 1008 (1011); OLG Naumburg, Urt. v. 22.2.2000 – 11 U 197/99, juris, Rn. 44.
[1198] So auch OLG Koblenz VersR 2018, 1008 (1011); siehe auch *Oechsler*, in: Staudinger, BGB, 2018, § 826 Rn. 44 (Identität, wenn das deliktische Verhalten auf die Setzung von rechtsgeschäftlichen Rechtsfolgen zielt).
[1199] Vgl. *Evers*, BB 1992, 1365 (1372).
[1200] Siehe oben, § 5 C.II.2.b).
[1201] *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, § 826 Rn. 53.
[1202] Vgl. zur parallelen Problematik bei der *culpa in contrahendo* oben, § 5, Fn. 1061.
[1203] Vgl. *Oetker*, in: MüKo, BGB, 8. Aufl. 2019, § 249 Rn. 228 ff.

cherungsrechtlichen Ausgleich,[1204] zur Wahrung des unionsrechtlichen Effektivitätsgrundsatzes nicht zu einer Abschreckung des Nutzers hinsichtlich der Geltendmachung seiner Rechte führen. Daher ist die Vorteilsanrechnung regelmäßig zu versagen.

e) § 831 BGB

Schließlich kann eine Haftung auf § 831 Abs. 1 S. 1 BGB gestützt werden, sofern ein Verrichtungsgehilfe die haftungsrelevante Handlung vollzogen hat. Hinsichtlich der objektiv rechtswidrigen Erfüllung eines Deliktstatbestandes ist jedoch zu differenzieren. Soweit die §§ 823 ff. BGB anwendbar sind, können diese ohne Weiteres herangezogen werden. Richtigerweise wird man ferner auch die objektiv rechtswidrige Erfüllung des Tatbestands von Art. 82 Abs. 1 DS-GVO zugrunde legen können. Denn auch sonst ist anerkannt, dass § 831 Abs. 1 BGB in Verbindung mit deliktischen Normen außerhalb des BGB Anwendung finden kann.[1205] Dies muss umso mehr gelten, als Art. 82 Abs. 1 DS-GVO nach hier vertretener Auffassung *lex specialis* zu §§ 823 ff. BGB ist. Da es sich insoweit nicht um eine verschuldensunabhängige Haftung handelt, spielt der Streit über die Anwendbarkeit von § 831 Abs. 1 BGB auf Tatbestände der Gefährdungshaftung[1206] keine Rolle.[1207]

f) Zusammenfassung zu deliktischen Ansprüchen

Die Anwendbarkeit einzelner deliktsrechtlicher Anspruchsgrundlagen neben Art. 82 DS-GVO ist jeweils für die einzelnen Normen gesondert zu klären. Art. 82 Abs. 1 DS-GVO ist dabei nach hier vertretener Auffassung grundsätzlich *lex specialis* gegenüber § 823 Abs. 1 BGB in Verbindung mit dem Recht auf informationelle Selbstbestimmung, dem Recht auf Vertraulichkeit und Integrität von informationstechnischen Systemen und auch dem allgemeinen Persönlichkeitsrecht. Lediglich in seltenen Fällen, in denen im Rahmen des allgemeinen Persönlichkeitsrechts Umstände Berücksichtigung finden können, die im Rahmen der DS-GVO keine Rolle spielen, kann auf § 823 Abs. 1 BGB zurückgegriffen werden. Damit geht einher, dass § 823 Abs. 1 BGB in den genannten Bereichen gegenüber Art. 82 Abs. 1 DS-GVO ganz erheblich an Bedeutung verlieren wird.

Auch gegenüber § 823 Abs. 2 in Verbindung mit Normen der DS-GVO und § 824 BGB ist Art. 82 Abs. 1 DS-GVO *lex specialis*. Eine eigenständige Bedeu-

[1204] Siehe oben, Text bei § 5, Fn. 550.

[1205] Siehe etwa *Föster*, in: BeckOK BGB, 51. Ed. 2019, § 831 Rn. 9; *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, § 831 Rn. 7 (außervertragliche Verschuldenshaftung) und Rn. 9; *Wagner/Potsch*, JZ 2006, 1085 (1090); *Adomeit/Mohr*, NJW 2007, 2522 (2544) (jeweils zum AGG).

[1206] Ablehnend etwa *Wagner*, in: MüKo, BGB, 7. Aufl. 2017, § 831 Rn. 7; befürwortend *Föster*, in: BeckOK BGB, 51. Ed. 2019, § 831 Rn. 9.

[1207] Bei funktionaler Betrachtung gilt dies ebenso, wenn man Art. 82 Abs. 3 DS-GVO als rechtsvernichtende Einwendung begreift.

tung kommt hingegen § 826 BGB auch im Bereich datenbasierter Austauschverhältnisse zu. Der Begriff der Sittenwidrigkeit deckt sich mit jenem aus § 138 Abs. 1 BGB, soweit ein wucherähnliches Geschäft in Rede steht. Allerdings wird ein Schädigungsvorsatz wegen der wertmäßigen Unbestimmtheit der datenbasierten Gegenleistung regelmäßig nicht schon bei einem funktional begrenzten oder geringwertigen Produkt des Anbieters angenommen werden können, sondern erst bei einem dysfunktionalen Produkt.

Schließlich ist § 831 BGB anwendbar, auch in Verbindung mit der Verletzung von Art. 82 Abs. 1 DS-GVO. Jedoch dürfte ihm neben der Anwendung von § 278 S. 1 BGB, im Rahmen von Art. 82 Abs. 1 DS-GVO, keine entscheidende Bedeutung zukommen.

D. Ergebnisse von § 5

Das fünfte Kapitel dieser Arbeit hat die mannigfaltigen Wechselwirkungen zwischen DS-GVO und dem allgemeinen Zivilrecht beleuchtet. Dabei zeigte sich noch einmal in aller Schärfe, dass zwischen der datenschutzrechtlichen Einwilligungserklärung einerseits und einem Vertrag zwischen datenschutzrechtlich Verantwortlichem und Nutzer andererseits streng getrennt werden muss. Im Einzelnen liefert die Analyse folgende Ergebnisse:

1. Bei der Bestimmung des Verhältnisses von unionalem Datenschutzrecht und allgemeinem Privatrecht muss dogmatisch streng zwischen dem Anwendungsvorrang einerseits und einer Sachintegration von Normen ebenengleicher Provenienz unterschieden werden. Inhaltlich lassen sich jedoch für beide Kategorien übergreifende Kriterien zur Bestimmung der Wechselwirkungen zwischen Datenschutz- und allgemeinem Privatrecht formulieren. So ist jeweils entscheidend, ob auf unionsrechtlicher Ebene (Anwendungsvorrang) oder im Rahmen eines speziellen Rechtsgebiets (Sachintegration) ein bestimmtes Risiko eine abschließende Regelung dergestalt erfahren hat, dass alle Eventualitäten berücksichtigt werden sollten. Sofern eine mitgliedsstaatliche Regelung ein eigenständiges Risiko adressiert (Risikospezifizität), und im Rahmen des Anwendungsvorrangs zudem mit den Zielsetzungen des Unionsrechts vereinbar ist (Zielkompatibilität), kann sie neben der DS-GVO Anwendung finden.

2. In schuldrechtlicher Hinsicht können Anbieter und Nutzer, im Rahmen der gesetzlichen Grenzen der Privatautonomie, eine Verpflichtung zur Überlassung von personenbezogenen Daten oder auch zur Abgabe einer Einwilligungserklärung, kumulativ oder alternativ, zum Gegenstand einer Gegenleistungspflicht machen.

3. Zur Verzahnung von Datenschutz- und Privatrecht kann und muss die datenschutzrechtliche Einwilligungserklärung in die Rechtsgeschäftslehre des

BGB integriert werden. Der Rückgriff auf Vorschriften des allgemeinen Teils des BGB kann jedoch grundsätzlich nur beschränkt und punktuell erfolgen, um das Ziel der DS-GVO, hinsichtlich der Einwilligung eine Harmonisierung der Wirksamkeitsvoraussetzungen herbeizuführen, nicht zu gefährden. Der Anwendungsvorrang der DS-GVO muss daher vor einem Rückgriff stets nach der hier entwickelten zweistufigen Prüfung (Risikospezifizität; Zielkompatibilität) ausgeschlossen werden.

4. Die Einwilligung stellt nach hier vertretener Auffassung eine geschäftsähnliche Handlung dar. Die für Rechtsgeschäfte geltenden Vorschriften können im hier untersuchten Kontext wegen des Anwendungsvorrangs des Unionsrechts jedoch nur in zwei Fällen analog auf die Einwilligungserklärung angewandt werden. Erstens ist eine Anfechtung der Einwilligungserklärung möglich analog § 119 Abs. 1 und 2 BGB, wenn der datenschutzrechtlich Verantwortliche die Anfechtbarkeit kannte oder kennen musste (§ 142 Abs. 2 BGB). Die Anfechtung geht in ihren Rechtsfolgen nach § 142 Abs. 1 BGB über die lediglich ex nunc wirkende Möglichkeit des jederzeitigen Widerrufs nach Art. 7 Abs. 3 DS-GVO hinaus. Ein zweiter Rückgriff auf die Rechtsgeschäftslehre des BGB ist hinsichtlich der Stellvertretung bei der Einwilligung notwendig. Diese ist grundsätzlich zulässig und vollzieht sich analog §§ 164 ff. BGB.

5. Die weiteren hier untersuchten Fragen der Rechtsgeschäftslehre müssen für die Einwilligung unionsrechtsimmanent gelöst und Antworten daher durch Auslegung der DS-GVO entwickelt werden. So ist für das Wirksamwerden der Einwilligung unter Abwesenden bereits die Abgabe ausreichend, ein Zugang entbehrlich (Entäußerungstheorie). Auch Kriterien für die Einwilligungsfähigkeit und die Abgabe der Einwilligung können aus der DS-GVO selbst gewonnen werden. Ferner ist der Rückgriff auf Anfechtungsgründe des BGB, mit Ausnahme der soeben angesprochenen Kenntnis bzw. fahrlässigen Unkenntnis von der Anfechtbarkeit, ausgeschlossen: Entweder besteht neben der Widerrufsmöglichkeit kein Bedürfnis für eine Anfechtung oder die Einwilligung ist ohnehin wegen eines Verstoßes gegen das Kriterium der Freiwilligkeit (Art. 4 Nr. 11 DS-GVO) ex tunc unwirksam.

6. Gänzlich anders stellt sich das Verhältnis zwischen Rechtsgeschäftslehre und DS-GVO hinsichtlich solcher Vertragsbedingungen dar, auf welche die Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO gestützt werden soll. Hier kann und muss umfassend auf das BGB zurückgegriffen werden, da es an Regelungen in der DS-GVO schlichtweg mangelt. Lediglich punktuell wird die Rechtsgeschäftslehre des BGB hier durch Wertungen der DS-GVO modifiziert. Dies ist insbesondere relevant für die Erfassung des Drittbezugs der Datenverarbeitung auf vertragsrechtlichem Wege.

7. Eine Einbeziehung von Drittanbietern in den Vertrag zwischen Nutzer und Erstanbieter (z. B. beim *third-party tracking*) ist grundsätzlich möglich, schei-

tert jedoch in der Praxis häufig am Abschlusstatbestand. Konkludent kann die Datenüberlassung an Drittanbieter grundsätzlich nur über eine konditionale Verknüpfung relevant gemacht werden. Bei einer ausdrücklichen Regelung ist hingegen auch ein mehrseitiger Vertrag, ein bilateraler Vertrag unter Nutzung des Erstanbieters als Stellvertreter oder auch ein Vertrag zugunsten Dritter möglich.

8. Deutlich schwieriger hingegen gestaltet sich die Etablierung eines Vertragsverhältnisses zwischen Anbietern und Drittnutzern von IoT-Geräten. Soweit sich der Vertrag als Substitut für eine Einwilligungserklärung darstellt, muss nach hier vertretener Auffassung das Gebot der Unmissverständlichkeit aus Art. 4 Nr. 11 DS-GVO auf die Willenserklärung des Drittnutzers zur Vermeidung von Wertungswidersprüchen zwischen nationalem Vertragsrecht und unionalem Datenschutzrecht übertragen werden. Umgekehrt können Drittnutzer auch bei Scheitern eines direkten Vertrags zwischen ihnen und einem Anbieter über die Rechtsfigur des Vertrags mit Schutzwirkung zugunsten Dritter in den Genuss vertraglicher Ansprüche gelangen. Die Ermöglichungsstrukturen des Vertragsrechts bieten daher letztlich einen angemessenen Ausgleich zwischen den Interessen von Anbietern zur privatautonomen Regelung ihrer Rechtsverhältnisse mit Nutzern und dem Schutzbedürfnis von unbeteiligten Drittnutzern, deren Daten durch IoT-Geräte miterfasst werden.

9. Die privatautonomen Arrangements zwischen Anbieter und Nutzer, durch Einwilligung und Vertrag, finden jedoch ihre Grenzen in den allgemeinen regulatorischen Strukturen der Rechtsgeschäftslehre und des Vertragsrechts. Insbesondere bei Vertragsbedingungen kompensieren diese das Fehlen von spezifischen datenschutzrechtlichen Schutzvorschriften zur Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO.

10. So schlägt die Datenschutzrechtswidrigkeit einer Datenverarbeitung bei einem Vertrag zwischen einem datenschutzrechtlich Verantwortlichen und einem Dritten (zum Beispiel beim Datenhandel) nach § 134 BGB auf die Wirksamkeit des Vertrags durch. Entgegen der bislang herrschenden Meinung gilt dies nach hier vertretener Auffassung jedoch nicht für Verträge zwischen der betroffenen Person und dem datenschutzrechtlich Verantwortlichen. Hier kommt es vielmehr zu einer Entkopplung des Vertragsrechts vom Datenschutzrecht: Auch wenn der Vertrag auf die Überlassung von Daten gerichtet ist, deren Verarbeitung datenschutzrechtswidrig wäre, scheitert dessen Wirksamkeit nicht an § 134 BGB.

11. Die Inhaltskontrolle von Einwilligungserklärungen und Vertragsbedingungen vollzieht sich vor allem nach den §§ 305 ff. BGB. Diesen kommt neben der DS-GVO eine eigenständige Bedeutung zu; das Datenschutzrecht kann nicht mehr als alleiniger Prüfungsmaßstab der AGB-Kontrolle angesehen werden. Der BGH wird seine dahingehende Rechtsprechung aufgeben müssen.

12. Hinsichtlich des AGB-rechtlichen Transparenzgebots kommt es allerdings im Wesentlichen lediglich zu einem Nachvollzug der in der DS-GVO festgehaltenen Informationspflichten.

13. Eine eigenständige Bedeutung erlangt die AGB-Kontrolle hingegen bei der Inhaltskontrolle im engeren Sinne. Hier ist entscheidend, dass in teleologischer Reduktion von § 307 Abs. 3 S. 1 BGB bei richtlinienkonformer Auslegung auch die Hauptleistungspflichten kontrollfähig sind. Denn die rechtsökonomischen Voraussetzungen für deren Ausnahme von der AGB-Kontrolle liegen bei datenbasierten Austauschverhältnissen regelmäßig nicht vor.

14. Maßstab der Inhaltskontrolle ist dann einerseits das Datenschutzrecht (§ 307 Abs. 2 Nr. 1 BGB) und andererseits, über dieses hinausgehend, der hypothetische Vertragsverhandlungsmechanismus, den der EuGH in seiner *Aziz*-Rechtsprechung entwickelt hat (§ 307 Abs. 1 S. 1 BGB). Dies eröffnet Möglichkeiten, in marktkonformer Weise eine Inhaltskontrolle auch im Bereich der Hauptleistungspflichten zu operationalisieren. Diese muss jedoch zugleich wegen der Ergebnisoffenheit des *Aziz*-Tests und aus Respekt vor der residualen Steuerungsmacht des Marktes und der Privatautonomie erheblich zurückgenommen werden. Unwirksam können jedoch insbesondere weite, mit der Hauptleistungspflicht des Anbieters inkonnexe Nebenleistungspflichten des Anbieters sein, über die eine Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO legitimiert werden soll.

15. Die Unwirksamkeit einer Einwilligungserklärung oder einer Vertragsklausel infolge einer eigenständigen AGB-rechtlichen, nicht nur reflexhaft das Datenschutzrecht nachvollziehenden Unangemessenheit führt grundsätzlich zu einer Verletzung des datenschutzrechtlichen Grundsatzes von Treu und Glauben, wenn die Datenverarbeitung auf diese Grundlage gestützt wird. In methodologischer Hinsicht sind daher Schlüsse zwischen DS-GVO und AGB-Kontrolle in beide Richtungen möglich.

16. Als verlängerter Arm der AGB-Kontrolle implementiert § 138 Abs. 1 BGB eine „datenbasierte *laesio enormis*". Auch hier gilt, wegen der teleologischen Reduktion von Art. 4 Abs. 2 der Klauselrichtlinie in richtlinienkonformer Auslegung von § 138 Abs. 1 BGB, der *Aziz*-Test. Das Äquivalenzverhältnis zwischen Leistung und Gegenleistung ist jedoch erst dann hinreichend gestört, wenn einer umfangreichen Datenüberlassung lediglich ein funktional stark begrenztes Produkt oder ein Produkt mit sehr geringem Marktwert gegenübersteht. Funktional leistet § 138 Abs. 1 BGB daher eine objektive Datenexzesskontrolle. Regelmäßig ist in diesen Fällen auch der datenschutzrechtliche Grundsatz von Treu und Glauben verletzt.

17. Demgegenüber kommt § 242 BGB im hier interessierenden Kontext keine Bedeutung für die Inhaltskontrolle, sondern nur für die Ausübungskontrolle

bei Rechtsmissbrauch zu. Hinsichtlich der Einwilligung wird § 242 BGB allerdings durch den allgemeinen unionsrechtlichen Grundsatz von Treu und Glauben begrenzt. § 242 BGB ist jedoch auf die Datenverarbeitung potenziell legitimierende Vertragsbedingungen anwendbar, wenn sich der Erwerb dieser Rechtsposition oder die Berufung auf diese als rechtsmissbräuchlich darstellt. In beiden Fällen ist grundsätzlich, wenn die Datenverarbeitung tatsächlich erfolgt und auf die Einwilligung oder die Vertragsbedingungen gestützt wird, ebenfalls der datenschutzrechtliche Grundsatz von Treu und Glauben verletzt.

18. Kommt ein Vertrag nach Maßgabe des soeben Erörterten wirksam zustande, stellt sich insbesondere die Frage der Wechselwirkung zwischen DS-GVO und vertraglichen Nebenpflichten. Nach hier vertretener Auffassung können nur die wesentlichen Pflichten der DS-GVO im Wege der Vertragsauslegung nach §§ 133, 157 BGB als vertragliche Nebenpflichten identifiziert werden. Dies ist jedoch von reduzierter Bedeutung, weil die Datenverarbeitung nach hier vertretener Auffassung ein Sonderrechtsverhältnis begründet, auf das § 278 BGB ohnehin anwendbar ist. Insofern ist unschädlich, dass die vertragliche und vorvertragliche Haftung aus § 280 Abs. 1 BGB wegen Verletzung einer datenschutzrechtlichen Nebenpflicht, die unmittelbar aus der DS-GVO gewonnen wird, durch Art. 82 Abs. 1 DS-GVO als *lex specialis* verdrängt wird.

19. Insbesondere dann, wenn kein wirksamer Vertrag zustande kommt, ist die außervertragliche Haftung des Anbieters gegenüber dem Nutzer relevant, und hier vor allem das Deliktsrecht. Grundsätzlich stellt Art. 82 Abs. 1 DS-GVO auch diesbezüglich eine *lex specialis* dar. Der datenschutzrechtliche Schadensersatzanspruch nach Art. 82 DS-GVO ist auch insofern gegenüber deliktischen Ansprüchen nach dem BGB vorteilhafter, als immaterielle Schäden voraussetzungslos ersetzt werden und der Verantwortliche sich hinsichtlich eines Verschuldens selbst entlasten muss.

20. Neben Art. 82 DS-GVO ist § 823 BGB in Verbindung mit dem allgemeinen Persönlichkeitsrecht nur anwendbar, soweit Umstände betroffen sind, die im Rahmen der DS-GVO keinerlei Relevanz entfalten, was jedoch im Zeitalter der ubiquitären Datenverarbeitung selten sein dürfte. Dieser Anspruch dürfte daher gegenüber Art. 82 DS-GVO erheblich an Bedeutung verlieren. Grundsätzlich anwendbar ist § 826 BGB, der allerdings nicht schon, wie § 138 Abs. 1 BGB, bei funktional stark limitierten oder geringwertigen, sondern erst bei dysfunktionalen Produkten einschlägig ist.

21. Dem individuellen Kontrollverlust im Bereich datenbasierter Austauschprozesse kann daher bereits jetzt durch die konsequente Nutzung und Auslegung der durch das Datenschutz- und das allgemeine Privatrecht vorgehaltenen regulatorischen Strukturen entgegengetreten werden. Jedoch verschiebt sich dabei die Kontrollinstanz von den betroffenen Personen hin zu Behörden und Gerichten. Diese wachen über die Grenzen der Privatautonomie. Das

allgemeine Zivilrecht hält hingegen kaum Ressourcen zur aktiven Unterstützung von Entscheidungen in komplexen, technikgeprägten Umfeldern vor, die über Informationspflichten, etwa bei Fernabsatzverträgen, hinausgingen. Es besteht daher in diesem Kontext erheblicher Reformbedarf zur Ermöglichung der wirksamen Inanspruchnahme von Privatautonomie durch die betroffenen Personen. Dem widmet sich der folgende, dritte Teil der Arbeit.

Teil 3

Reformperspektiven

§6 Präferenzverwirklichung durch Technikgestaltung

Das fünfte Kapitel dieser Arbeit hat gezeigt, dass eine Einhegung besonders ausgeprägter datenschutzrechtlicher Risiken durch die regulatorischen Strukturen des allgemeinen Zivilrechts, zum Teil in Verbindung mit dem Datenschutzrecht, durchaus möglich ist, jedoch nur um den Preis einer Verschiebung der Kontrolle der Bedingungen der Datenverarbeitung weg vom individuellen Nutzer hin zu datenschutzrechtlichen Aufsichtsbehörden und Gerichten. Die darin liegende Abkehr vom Anspruch individueller Datensouveränität ist den im dritten Kapitel der Arbeit beschriebenen Formen von Marktversagen geschuldet und insofern die logische Konsequenz der bisherigen funktionalen Rahmenbedingungen datenmediierter Austauschprozesse.

Gänzlich unvermeidlich ist diese Lastenverschiebung vom Individuum hin zu institutionalisierten Kontrollinstitutionen jedoch nicht. Vielmehr soll dieses Kapitel Mechanismen ausloten, durch die individuelle Nutzer die Hoheit über ihre Daten zumindest partiell wiedererlangen und Austauschbeziehungen auch materiell privatautonom gestalten können.[1] Dann könnte das Datenprivatrecht sein Versprechen einlösen, neben seiner regulatorischen Komponente zumindest *auch* ein effektives, souveränitätsförderndes, aber zugleich grundrechtssensibles Datenermöglichungsrecht zu sein. Eine Unterstützung individueller Kontrollmöglichkeiten kann sich dabei auf zwei Wegen vollziehen. Einerseits muss Code als weiterer Kontrollmechanismus ernst genommen werden,[2] der sowohl auf Seiten der Unternehmen als auch jener der Nutzer für präferenzkonformere Austauschmodelle fruchtbar gemacht werden kann. Dies ist die erste Dimension der Technikgestaltung: Gestaltung *durch* Technik.[3] Ande-

[1] Zu diesem Desiderat auch *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter II.4. (bei Fn. 43) sowie III.1.; *Metzger*, in: Festschrift Basedow, 2018, 131 (133 ff.).

[2] Grundlegend *Lessig*, Code. And Other Laws of Cyberspace, 1999; siehe auch *Brownsword*, 8 Law, Innovation and Technology 2016, 100; *Shadmy*, 37 Boston University International Law Journal 2019, 307; *Micklitz*, in: Grundmann/Micklitz/Renner (Hrsg.), Privatrechtstheorie, Band II, 2015, 1221 (1222 ff.); *Pałka*, in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, 135 (154 ff.).

[3] Angemerkt sei jedoch, dass das klassische Verständnis des Begriffs „Technikgestaltung", der ursprünglich aus der Techniksoziologie stammt, nur die sogleich genannte zweite, nicht die hier genannte erste Dimension umfasst, siehe nur *Grunwald*, in: Grunwald (Hrsg.), Technikgestaltung zwischen Wunsch und Wirklichkeit, 2003, 1 (1, 6 f.); *Bijker/Law*, in: Bijker/Law (Hrsg.), Shaping Technology/Building Society. Studies in Sociotechnical Change, 1992, 1 (4 f., 11).

rerseits kann das Recht in Form neuer Regulierung Möglichkeiten zur Unterstützung autonomer individueller Entscheidungen erschließen. Darin liegt die zweite Dimension der Technikgestaltung: Gestaltung *von* Technik.[4] Im Rahmen dieser Untersuchung interessiert dabei – wenig überraschend – besonders die Gestaltung durch das Recht.

Dabei muss jedoch die bereits mehrfach angesprochene Heterogenität von Datenschutzpräferenzen immer mitgedacht werden. Zielpunkt einer Entscheidungsunterstützung durch Technik oder Recht sollte daher sein, technische oder rechtliche Selektionsangebote bereitzustellen, durch welche die Nutzer stärker als gegenwärtig das faktisch gebotene Datenschutzniveau an ihre Präferenzen anpassen können. Eine individuelle *Absenkung* des Schutzniveaus unter den gegenwärtig geltenden datenschutzrechtlichen Standard dürfte allerdings rechtspolitisch kaum durchsetzbar sein.[5] Es sollte jedoch angesichts der U-förmigen Verteilung der Datenschutzpräferenzen denjenigen Nutzern, welche stark ausgeprägte Präferenzen haben, möglich sein, stärker als bisher Kontrolle über ihre Daten auszuüben oder sogar in rechtlich für sie vorteilhaftere Regime hineinzuoptieren, das Schutzniveau mithin selektiv *anzuheben*.

Bevor über neue Formen der Regulierung nachgedacht werden kann (C.), muss jedoch eruiert werden, welche Formen der Minimierung von Datenschutzrisiken bereits jetzt technisch möglich sind und ob hinreichende Anreize zu deren Umsetzung, durch Anbieter oder Nutzer, bestehen (B.). Für diese Diskussionen ist jedoch zunächst eine Vergewisserung über die begriffliche und praktische Bedeutung von Autonomie und Informiertheit in vernetzten Umgebungen notwendig (sogleich unter A.).

A. Autonomie, Informiertheit und Datenschutzpräferenzen

Ziel dieses Kapitels ist die Diskussion von verschiedenen technischen und rechtlichen Ansätzen, mit denen die Souveränität von Nutzern über ihre Daten gestärkt werden kann. Damit soll insbesondere die Verwirklichung materieller Privatautonomie in vernetzten Umgebungen und datenbasierten Austauschprozessen gefördert werden. Dies bedingt jedoch eine Reflexion auf die Zusammenhänge zwischen den Begriffen von Autonomie, Informiertheit und Datenschutzpräferenzen. Dabei können und sollen Begriff und Bedeutung der (Privat-)Autonomie hier nicht in ganzer Tiefe entfaltet werden. Dazu liegen bereits mannigfaltige Abhandlungen vor.[6] Der Verfasser hat seine eigene

[4] Siehe die Nachweise in § 6, Fn. 3.

[5] Siehe für dahingehende Erwägungen aber *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (452); *Hacker*, 7 International Data Privacy Law 2017, 266 (282 f.); *Becker*, JZ 2017, 171 (178 f.); zur Personalisierung datenschutzrechtlicher Normen auch *Busch*, 86 The University of Chicago Law Review 2019, 309 (319 ff.).

[6] Zum rechtlichen Begriff *von Hippel*, Das Problem der rechtsgeschäftlichen Privat-

Konzeption an anderer Stelle bereits ausführlich dargelegt,[7] sodass hier die Fragestellung auf Autonomie in vernetzten Umgebungen zugespitzt werden kann.

Privatautonomie, verstanden als Prinzip willentlicher Selbstbestimmung durch rechtliche Selbstgestaltung,[8] ist ganz unbestritten ein zentraler Wert einer freiheitlichen Privatrechtsordnung.[9] Dabei dürfte mittlerweile auch konsentiert sein, dass die Gewährung allein formaler Wahlfreiheit (Vertragsabschlussfreiheit) unzureichend ist, wenn nicht zugleich zumindest im Grundsatz sichergestellt wird, dass die tatsächlichen Voraussetzungen für eine eigenverantwortliche Ausübung der Wahl vorliegen.[10] Ein solcher materieller Begriff der Privatautonomie kann an die kontemporäre Autonomietheorie, die insbeson-

---

autonomie, 1936; *Flume*, in: von Caemmerer et al. (Hrsg.), Hundert Jahre deutsches Rechtsleben, 1960, 135; *Bydlinski*, Privatautonomie und objektive Grundlagen des verpflichtenden Rechtsgeschäfts, 1967; *Schaack*, Zu den Prinzipien der Privatautonomie im deutschen und französischen Rechtsanwendungsrecht, 1990; *Wagner*, Prozeßverträge. Privatautonomie im Verfahrensrecht, 1998; *Busche*, Privatautonomie und Kontrahierungszwang, 1999; *Canaris*, AcP 200 (2000), 273 (277 ff.); *Specht*, Diktat der Technik, 2019, 77 ff.; zum philosophischen Begriff *Christman*, Autonomy in Moral and Political Philosophy, The Stanford Encyclopedia of Philosophy, 2015, https://plato.stanford.edu/archives/spr2018/entries/autonomy-moral/; *Schneewind*, The Invention of Autonomy. A History of Modern Moral Philosophy, 1998.

[7] *Hacker*, Verhaltensökonomik und Normativität, 2017, 223 ff.; *Hacker*, in: Micklitz et al. (Hrsg.), Research Methods in Consumer Law. A Handbook, 2018, 77.

[8] *von Hippel*, Das Problem der rechtsgeschäftlichen Privatautonomie, 1936, 71 und 62 mit Fn. 7; *Flume*, in: von Caemmerer et al. (Hrsg.), Hundert Jahre deutsches Rechtsleben, 1960, 135 (136); *Flume*, AT II, 4. Aufl. 1992, 1; *Bydlinski*, Privatautonomie und objektive Grundlagen des verpflichtenden Rechtsgeschäfts, 1967, 114; *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, 1971, 413; *Canaris*, AcP 200 (2000), 273 (277); *Schaack*, Zu den Prinzipien der Privatautonomie im deutschen und französischen Rechtsanwendungsrecht, 1990, 28; *Lorenz*, Der Schutz vor dem unerwünschten Vertrag, 1997, 15; *Busche*, Privatautonomie und Kontrahierungszwang, 1999, 13; *Grundmann/Kerber/Weatherill*, in: Grundmann et al. (Hrsg.), Party Autonomy and the Role of Information in the Internal Market, 2001, 3 (4); *Möslein*, Dispositives Recht, 2011, 46; *Hellgardt*, Regulierung und Privatrecht, 2016, 542; *Riesenhuber*, ZfPW 2018, 352 (355 f.).

[9] Siehe bereits die Nachweise oben, § 5, Fn. 178; ferner, mit Blick auf das Privatrecht insgesamt, *Böhm*, ORDO 17 (1966), 75 (80); aus der neuren Literatur *Riesenhuber*, ZfPW 2018, 352 (357); *Hellgardt*, Regulierung und Privatrecht, 2016, 545; eine Hypertrophie des Rekurses auf Privatautonomie jedoch konstatierend *Röthel*, in: Bumke/Röthel (Hrsg.), Autonomie im Recht, 2017, 91 (95 ff.) („mystifizierendes Leuchtfeuer"); kritisch ebenfalls zuvor *Wagner*, AcP 206 (2006), 352 (423 f.) („Armut der Privatautonomie als Rechtsprinzip").

[10] Siehe nur BVerfG NJW 1994, 36 (38); BVerfG NJW 2005, 2363 (2365); BVerfG NJW 2005, 2376 (2377 f.); *Zöllner*, AcP 196 (1996), 1 (28); *Canaris*, AcP 200 (2000), 273 (besonders 296 ff.); *Auer*, Materialisierung, Flexibilisierung, Richterfreiheit, 2005, 23 f., 28 ff.; *Hellgardt*, Regulierung und Privatrecht, 2016, 69 f.; *Grundmann*, in: Festschrift Canaris, 2017, 907 (912); *Hacker*, Verhaltensökonomik und Normativität, 2017, 233 ff., 277 ff.; *Riesenhuber*, ZfPW 2018, 352 (358); *Specht*, Diktat der Technik, 2019, 96 ff.; siehe auch bereits *Flume*, in: von Caemmerer et al. (Hrsg.), Hundert Jahre deutsches Rechtsleben, 1960, 135 (146 f.); *Schmidt*, JZ 1980, 153 (155 f.); ferner für das europäische Privatrecht *Colombi Ciacchi*, 6 European Review of Contract Law 2010, 303 (306 f.).

dere im Bereich der praktischen Philosophie entwickelt wird, anschließen.[11] Danach erscheint es sinnvoll, mit dem vielleicht führenden Autonomietheoretiker *Gerald Dworkin* drei notwendige Bedingungen für autonome Handlungen zu unterscheiden,[12] die auch für die Wahrnehmung von Autonomie in digitalen Austauschprozessen von entscheidender Bedeutung sind.[13]

Erstens setzt Autonomie voraus, dass der Akteur in der Lage ist, überhaupt Präferenzen zu bilden.[14] Spezifischer sind mehrstufige Präferenzen erforderlich, insbesondere also auch Präferenzen zweiter Stufe, die sich auf Präferenzen erster Stufe beziehen, welche wiederum direkt auf Handlungen referieren.[15] So mag ein Nutzer zwar in einer konkreten Situation die Präferenz erster Stufe haben, sich durch Überlassung personenbezogener Daten monetär kostenfrei den Zugang zu einer Dienstleistung zu verschaffen, zugleich aber eine Präferenz zweiter Stufe, rein datenbasierte Austauschprozesse wegen datenschutzrechtlicher Risiken nicht mehr einzugehen und daher die Präferenz erster Stufe zu ändern. Diese Modellierung passt durchaus zu der Differenz von erklärten und gelebten Präferenzen im datenschutzrechtlichen Bereich (*privacy paradox*)[16] sowie zu der Kontextabhängigkeit von Datenschutzpräferenzen, die später noch umfänglicher thematisiert wird.[17] Wichtig ist zunächst einmal zu erkennen, dass praktisch alle Akteure in der digitalen Wirtschaft Datenschutzpräferenzen ausbilden und diesen zumindest potenziell auch kritisch gegenüberstehen können, wobei sich ein Spannungsverhältnis zwischen Präferenzen unterschiedlicher Ordnung manifestieren kann. Ob sich letztlich die Präferenz erster oder höherer Ordnung durchsetzt, ist für den Grad der Autonomie einer Entscheidung nicht erheblich; wichtig ist lediglich, dass eine Änderung von Präferenzen erfolgen *kann*.

Diese Änderung oder Formierung von Präferenzen ist Gegenstand des zweiten Kriteriums für Autonomie. Danach müssen Präferenzen auf einen hinreichend von externen Einflüssen unabhängigen kognitiven Prozess des jeweiligen Akteurs zurückgehen.[18] Da äußere Einflüsse bei Individuen, die in einem sozialen Kontext leben, naturgemäß nicht eliminiert werden können,[19] ist Kern

---

[11] *Hacker*, Verhaltensökonomik und Normativität, 2017, 229 ff.; grundsätzlich so auch *Riesenhuber*, ZfPW 2018, 352 (356).

[12] *Dworkin*, The Theory and Practice of Autonomy, 1988, 15 ff.

[13] So auch *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (451).

[14] *Dworkin*, The Theory and Practice of Autonomy, 1988, 15 ff.

[15] *Dworkin*, The Theory and Practice of Autonomy, 1988, 14 f., im Anschluss an *Frankfurt*, 68 The Journal of Philosophy 1971, 5 (8 f.).

[16] Siehe oben, § 3 B.II.1.

[17] Siehe unten, § 6 C.I.3.b)bb)(2)(a).

[18] *Dworkin*, The Theory and Practice of Autonomy, 1988, 18; siehe auch *Scanlon*, 1 Philosophy and Public Affairs 1972, 204 (215); *Rawls*, Political Liberalism, 1993, 73; *Sen*, 45 Oxford Economic Papers 1993, 519 (524); *Wolff*, In Defense of Anarchism, 1970, 14; *Arneson*, in: Coleman/Buchanan (Hrsg.), In Harm's Way: Essays in Honor of Joel Feinberg, 1991, 42 (56 ff.); *Berofsky*, Liberation from Self, 1995, 182.

[19] Vgl. *Hausman/Welch*, 18 Journal of Political Philosophy 2010, 123 (127).

dieser Bedingung die Möglichkeit kritischer, rationaler Reflexion der jeweiligen Einflüsse.[20] Für den Kontext der Datenschutzpräferenzen ist dies insoweit von erheblicher Bedeutung, als empirische Studien zeigen, dass diese Präferenzen in hohem Maße durch externe Interventionen formbar sind (*malleability*).[21] In rechtlicher Hinsicht bildet das Lauterkeitsrecht die Schranke der hinnehmbaren Einflussnahme, das im Rahmen dieser Studie jedoch nicht eingehend untersucht werden kann.[22] Durchaus nicht unumstritten ist demgegenüber in autonomietheoretischer Hinsicht die Rolle, die Informationen bei der Formierung von Präferenzen zukommen muss. Während nach Ansicht mancher Autoren nur eine hinreichend informierte Entwicklung von Präferenzen als autonom gelten kann,[23] beharrt *Dworkin* zu Recht darauf, dass authentische, autonome Entscheidungen auch auf objektiv minimaler Informationsgrundlage getroffen werden können, solange keine Täuschung durch Dritte erfolgt.[24] Denn sonst wäre Autonomie lediglich einer kleinen Minderheit vorbehalten.

Jedenfalls für den Bereich der Entwicklung von Datenschutzpräferenzen dürfte daher gelten, dass Informationen über die konkreten Formen der Datenverarbeitung und datenschutzrechtliche Risiken zwar für die Wahrnehmung von Autonomie nicht strikt notwendig, aber doch in hohem Grade hilfreich sind, da sie insbesondere die Austarierung von Präferenzen unterschiedlicher Ordnung ermöglichen. Dies impliziert, dass transparenzbasierte Ansätze, welche die Informationslage der jeweiligen Nutzer verbessern sollen, grundsätzlich auch aus autonomietheoretischer Perspektive unterstützenswert sind. Andererseits folgt aus dem Gesagten jedoch auch, dass Entscheidungen nicht deshalb die Autonomie abgesprochen werden sollte, weil sie nicht in – wie auch immer definierter – hinreichend informierter Weise vorgenommen wurden. Andernfalls bliebe für einen Großteil der Nutzer gerade im datenschutzrechtlichen Bereich keine Möglichkeit zur Verwirklichung autonomer Entscheidungen,[25] da rationale Ignoranz nach wie vor für die überwältigende Mehrheit die

[20] *Scanlon*, 1 Philosophy and Public Affairs 1972, 204 (216); *Dworkin*, The Theory and Practice of Autonomy, 1988, 17.

[21] *Acquisti/Brandimarte/Loewenstein*, 347 Science 2015, 509 (512 f.).

[22] Siehe aber *Helberger*, in: Schulze/Staudenmayer (Hrsg.), Digital Revolution: Challenges for Contract Law in Practice, 2016, 135; *Hacker*, in: Busch/de Franceschi (Hrsg.), Data Economy and Algorithmic Regulation: A Handbook on Personalized Law, 2020 (im Erscheinen).

[23] Siehe *Christman*, Autonomy in Moral and Political Philosophy, The Stanford Encyclopedia of Philosophy, 2015, https://plato.stanford.edu/archives/spr2018/entries/autonomy-moral/, unter 1.2. („competency"); *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (457).

[24] Siehe *Dworkin*, The Theory and Practice of Autonomy, 1988, 17, 20, 31 f.; im Ergebnis zustimmend *Hacker*, Verhaltensökonomik und Normativität, 2017, 256 f.

[25] Vgl. *Dworkin*, The Theory and Practice of Autonomy, 1988, 7, 17; *Christman*, Autonomy in Moral and Political Philosophy, The Stanford Encyclopedia of Philosophy, 2015, https://plato.stanford.edu/archives/spr2018/entries/autonomy-moral/, unter 1.1.: „basic autonomy" muss den meisten Personen zugesprochen warden können; *Hacker*, Verhaltensökonomik und Normativität, 2017, 255.

präferierte Strategie darstellt. Insbesondere kann daher einer Handlung nicht das Prädikat der Autonomie verwehrt werden, weil die Kenntnisnahme und Auswertung von Informationen an Dritte delegiert wurde.[26] Autonomie kann daher selbst dann noch bestehen, wenn inhaltliche Entscheidungen bewusst an Datenschutzassistenten ausgelagert werden, da auch dies einer rationalen Einteilung knapper kognitiver Ressourcen entspricht.[27] Technologiebasierte Ansätze, die adaptive, zum Teil auf maschinellem Lernen basierende Entscheidungsunterstützung bieten und von denen später noch ausführlich die Rede sein wird,[28] können daher letztlich trotz Informations- und Handlungsentlastung der Nutzer deren Autonomie dienen.

Die letzte Bedingung für eine autonome Handlung ist, dass dergestaltige, hinreichend unabhängig geformte Präferenzen auch in der Wirklichkeit realisiert werden können.[29] An dieser Durchsetzungsmöglichkeit fehlt es, wenn entweder Nutzer mit niedrigen Datenschutzpräferenzen daran gehindert werden, ihre personenbezogenen Daten zur Budgeterweiterung einzusetzen, oder Nutzer mit hohen Datenschutzpräferenzen bestimmte Geräte, Dienste oder Applikationen nicht rein monetär, sondern nur gegen die Überlassung von personenbezogenen Daten nutzen können. Zwar muss dabei im Auge behalten werden, dass die Durchsetzung idiosynkratischer Datenschutzpräferenzen niemals unbedingt sein kann: Sie muss nicht nur mit den Interessen und Grundrechten der Anbieter von Produkten, sondern auch den Datenschutzpräferenzen anderer Nutzer, die im Wege negativer Externalitäten beeinträchtigt werden, abgewogen werden. Nichtsdestoweniger lässt sich festhalten, dass zumindest aus der genannten autonomietheoretischen Sicht zu einer autonomieförderlichen Umgebung auch die Möglichkeit der Realisierung eigener

[26] *Dworkin*, The Theory and Practice of Autonomy, 1988, 21; *Arneson*, in: Coleman/Buchanan (Hrsg.), In Harm's Way: Essays in Honor of Joel Feinberg, 1991, 42 (47–49); gegen eine Notwendigkeit der inhaltlich rationalen Entscheidung in jedem Einzelfall auch *Hill*, Autonomy and Self-Respect, 1991, 36; siehe auch *Sartor*, in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, 263 (272); *Hacker*, Verhaltensökonomik und Normativität, 2017, 256 f.; gegen eine Delegation autonomer Entscheidungen an externe Instanzen sprechen sich jedoch Vertreter substantieller Autonomiekonzeptionen aus, etwa *Lucas*, The Principles of Politics, 1966, 101; *Scanlon*, 1 Philosophy and Public Affairs 1972, 204 (216 f.); *Rachels*, 7 Religious Studies 1971, 325 (334); *Wolff*, In Defense of Anarchism, 1970, 14, 41.

[27] *Sartor*, in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, 263 (272).

[28] Siehe unten, § 6 C.I.3.a)bb) und § 6 C.I.3.c)aa).

[29] *Dworkin*, The Theory and Practice of Autonomy, 1988, 14, 17; *Sen*, 45 Oxford Economic Papers 1993, 519 (522, 524); *Raz*, The Morality of Freedom, 1986, 371 f.; *Arneson*, in: Coleman/Buchanan (Hrsg.), In Harm's Way: Essays in Honor of Joel Feinberg, 1991, 42 (68, 72); *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (451); teilweise wird die Realisierungsmöglichkeit auch lediglich dem Bereich der Freiheit zugeordnet, siehe *Christman*, Autonomy in Moral and Political Philosophy, The Stanford Encyclopedia of Philosophy, 2015, https://plato.stanford.edu/archives/spr2018/entries/autonomy-moral/, unter 1.1., was ihr jedoch nicht die Relevanz für die hier verhandelte Fragestellung nimmt.

Präferenzen gehört. Darauf wird im Rahmen der Verbesserung reeller Wahlmöglichkeiten zurückzukommen sein.[30]

Zugleich sollte nicht verkannt werden, dass die alleinige Fixierung des Autonomiebegriffs auf Wahlfreiheit ein verkürztes Autonomieverständnis offenbart. Zu Autonomie gehört mehr als bloße Wahlfreiheit: Diese ist notwendig, aber nicht hinreichend zur Begründung von autonomen Handlungen, wie die übrigen zwei Elemente des Autonomiebegriffs gezeigt haben. Die Durchdringung der rechtlichen Konsequenzen dieses reichhaltigen Autonomiebegriffs in vernetzten Umgebungen, die sich insbesondere auf das Lauterkeitsrecht kaprizieren müsste, muss jedoch einer gesonderten Abhandlung vorbehalten bleiben. In der Folge soll es daher um das enger gefasste Problem der Durchsetzung von heterogenen Datenschutzpräferenzen am Markt gehen.

B. Minimierung von Datenschutzrisiken durch Technik

Die Realisierung auch stark ausgeprägter Datenschutzpräferenzen wäre leichter möglich, wenn technische Applikationen von vornherein die Möglichkeit der sicheren Minimierung von datenschutzrechtlichen Risiken böten. Technischer Fortschritt muss zweifelsohne nicht notwendig zulasten des Datenschutzes ausfallen. Vielmehr beinhaltet die Möglichkeit der freien Wahl der Zielsetzungen und Parameter technischer Implementierungen, dass gerade auch autonomiestützende und datenschutzfreundliche Applikationen entwickelt werden können. In der Tat werden zunehmend Instrumente angeboten, um Datenschutzrisiken auf technischem Wege zu erkennen und zu reduzieren. Dem gehen die folgenden Abschnitte nach.

Bei allem Optimismus hinsichtlich der Gestaltungsbreite und Wirkmächtigkeit technischer Innovationsprozesse muss dabei jedoch vorab festgehalten werden, dass Technik das Recht im Allgemeinen und die Durchsetzung der DS-GVO im Besonderen nicht wird ersetzen können, da rechtliche Regeln, gerade die vagen Formulierungen der DS-GVO, schon aufgrund semantischer Offenheit nicht exakt in Code übersetzt werden[31] und auch durch Anwendungen maschinellen Lernens aus dem Bereich des *natural language processing* nur approximiert werden können.[32]

---

[30] Siehe unten, § 6 C.II.

[31] *Koops/Leenes*, 28 International Review of Law, Computers & Technology 2014, 159 (166); *Leenes*, *Ronald/Lucivero*, 6 Law, Innovation and Technology 2014, 193 (211 f.); *Pagallo*, in: Gutwirth et al. (Hrsg.), European Data Protection: In Good Health?, 2012, 331 (335 ff.); *Koops*, 5 Legisprudence 2011, 171 (193); siehe für den Bereich des Anti-Diskriminierungsrechts auch *Wachter/Mittelstadt/Russell*, Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI, Working Paper, 2020, https://ssrn.com/abstract=3547922.

[32] Dazu sogleich, unter § 6 B.II.1.a)bb).

Eine Reduzierung datenschutzrechtlicher Risiken durch Technik ist jedoch möglich, sowohl durch Applikationen auf Seiten von Unternehmen (dazu bereits oben, § 4 C.III.) als auch auf Seiten der Nutzer selbst (dazu sogleich). Die Implementierung datenschutzrechtlicher Prinzipien und Regeln auf Ebene der Technik, welche die Anbieter implementieren, wird bereits seit geraumer Zeit unter dem Schlagwort *privacy by design* verhandelt und wurde im Rahmen von Art. 25 DS-GVO bereits eingehend besprochen.[33] Der Geltungsbeginn der DS-GVO hat hier jedoch, trotz der Rechtspflicht aus Art. 25 DS-GVO, bislang noch keine Abkehr von der auf Tracking ausgerichteten Grundkonfiguration der meisten Anwendungen mit sich gebracht. Zwar nehmen seit Geltungsbeginn der DS-GVO ersten empirischen Ergebnissen zufolge mehr Nutzer ihr Recht auf Opt-Out wahr, sofern es angeboten wird; die verbliebenen werden dafür jedoch umso intensiver getrackt.[34] Besonders bedenklich ist dabei, dass 80 % der populärsten Webseiten der EU im Beobachtungszeitraum 2018/19 nicht einmal die Möglichkeit boten, aus der Setzung von Cookies hinauszuoptieren.[35] Die Anreize für die datenschutzfreundliche Gestaltung technologischer Applikationen scheinen daher auf Anbieterseite immer noch nicht hoch genug zu sein, um stark ausgeprägte Datenschutzpräferenzen zu befriedigen.

Von besonderem Interesse ist daher, inwiefern Nutzer selbst zu Mitteln greifen können, um ihre Datenschutzpräferenzen durchzusetzen und damit zugleich Wahlfreiheit hinsichtlich der Austauschbedingungen in der digitalen Wirtschaft aufrechtzuerhalten. Derartige Strategien würden, wenn sie wirksam und verbreitet wären, zugleich ein milderes Mittel gegenüber regulatorischen Eingriffen darstellen. Schon aus diesem Grund müssen sie vor der Diskussion weiterer Regulierungsvorschläge (dazu § 6 C.) eingehend geprüft werden. Eine Entscheidungs- und Präferenzunterstützung durch Technik kann sich dabei einerseits auf sog. *privacy-enhancing technologies* auf Nutzerseite (I.), andererseits aber auch auf eine automatisierte Rechtmäßigkeitskontrolle unter Verwendung maschinellen Lernens gründen (II.). Der folgende Abschnitt stellt beide Techniken kurz vor und fragt zugleich nach ihrem rechtlichen Rahmen sowie den Anreizen für ihre Verwendung und ihren Limitationen. Beide Varianten sind auf die *Minimierung* von Datenschutzrisiken durch einseitige, technische Maßnahmen angelegt. Angesichts ihrer Beschränkungen werden in der Folge dann noch Möglichkeiten zu diskutieren sein, wie Nutzer ihre Präferenzen technologisch unterstützt an Verantwortliche *kommunizieren* und rechtlich *durchsetzen* können (§ 6 C.I.3.).

---

[33] Siehe oben, § 4 C.III.

[34] *Aridor et al.*, The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR, NBER Working Paper No. w26900, 2020, https://www.nber.org/papers/w26900.

[35] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (1).

I. Privacy-enhancing technologies

Privacy-enhancing technologies werden bereits seit geraumer Zeit erforscht und sind Teil des technologiebasierten Regelungsansatzes von *privacy by design*. Unter *privacy-enhancing technologies* werden daher verschiedene Strategien zusammengefasst,[36] etwa Authentifizierungsverfahren,[37] *attribute-based credentials*,[38] *statistical disclosure control*,[39] *privacy-preserving data mining*[40] und dessen Nachfolger, *privacy-preserving machine learning*.[41] Einige Techniken und Anforderungen an den Datenschutz durch Technikgestaltung wurden bereits im Rahmen von Art. 25 DS-GVO diskutiert.[42] Dort stand die Frage im Mittelpunkt, welche datenschutzfreundlichen Gestaltungsvarianten anbieterseitig in Produkte integriert werden müssen.[43] Demgegenüber beleuchten die folgenden Ausführungen die, von Art. 25 DS-GVO nicht direkt erfasste, Marktgegenseite: die Nutzer. Untersucht werden daher solche Technologien, die Nutzer in die Lage versetzen, ihre Privatsphäre effektiv selbst zu schützen bzw. Souveränität über die Verwendung ihrer Daten zu erlangen. Solche nutzerseitigen Strategien der Minimierung von Datenschutzrisiken werden häufig auch als Selbstdatenschutz bezeichnet[44] (teilweise auch: *obfuscation strate-*

[36] Siehe den Überblick bei *Danezis et al.*, Privacy and Data Protection by Design – from policy to engineering, ENISA Report, 2014, 22 ff.; *Fischer-Hübner/Berthold*, in: Vacca (Hrsg.), Computer and Information Security Handbook, 3. Aufl. 2017, 759.

[37] Siehe etwa *Burrows/Abadi/Needham*, 426.1871 Proceedings of the *Royal Society* of London. A. Mathematical and Physical Sciences 1989, 233; *Aiello et al.*, 7(2) ACM Transactions on Information and System Security 2004, 1.

[38] Siehe etwa *Chaum*, 28(10) Communications of the ACM 1985, 1030; *Camenisch/Lysyanskaya*, in: Pfitzmann (ed.), International Conference on the Theory and Applications of Cryptographic Techniques, 2001, 93; *Rannenberg/Camenisch/Sabouri* (Hrsg.), Attribute-based Credentials for Trust, 2015.

[39] Siehe etwa *Willenborg/De Waal*, Elements of Statistical Disclosure Control, 2001; *Hundepool et al.*, Statistical Disclosure Control, 2012.

[40] Siehe etwa *Agrawal/Srikant*, 29 ACM Sigmod Record 2000, 439; *Verykios et al.*, 33 ACM Sigmod Record 2004, 50; *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (411 ff.); *Royal Society*, Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis, Report, 2019, 26 ff.

[41] *Chaudhuri/Monteleoni*, Advances in Neural Information Processing Systems 2009, 289; *Xu et al.*, IEEE 35th international conference on distributed computing systems 2015, 318; *Mohassel/Zhang*, IEEE Symposium on Security and Privacy (SP) 2017, 19; Überblick etwa bei *Winter/Battis/Halvani*, ZD 2019, 489 (492).

[42] Siehe oben, § 4 C.III.

[43] Siehe für die drei Leitfälle insbesondere oben, § 4 C.III.5.

[44] Siehe etwa *Johannes/Roßnagel*, Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt, 2016, 21 ff.; *Gola/Klug*, NJW 2019, 639 (642); *Kuntz*, ZD-Aktuell 2016, 05177; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 63; *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 172; *ULD Schleswig-Holstein*, Selbstdatenschutz: ein wichtiges Instrument für Datenschutz, Pressemitteilung vom 1.6.2016, https://www.datenschutzzentrum.de/artikel/1046-Selbstdatenschutz-ein-wichtiges-Instrument-fuer-Datenschutz-Forschungsprojekte-vernetzen-sich.html.

gies[45]). Diese werden in dreierlei Hinsicht im Folgenden untersucht: Zunächst wird danach unterschieden, welche Maßnahmen *technisch* möglich und sinnvoll sind (1.). Dann wird gefragt, inwiefern Anbieter *rechtlich* verpflichtet sind, derartige Maßnahmen zu unterstützen bzw. zu tolerieren (2.), und schließlich, ob hinreichende *Anreize* zu ihrer Verwendung bestehen (3.).

1. Relevante nutzerbasierte Techniken (Selbstdatenschutz)

Nutzerbasierte Technologien zum Schutz und zur Kontrolle der Privatsphäre sind vielfältig und können hier nicht umfassend dargestellt werden.[46] Besonders relevant für die hiesigen Zwecke sind solche, die den Kommunikationsvorgang selbst schützen (Verschlüsselung, unter a)), die Zugriffsrechte definieren und digitale Identitäten abgrenzen (Identity-Management-Systeme, unter b)) und die digitale Spuren bei der Nutzung von Online-Diensten beseitigen (Anti-Tracking-Tools, unter c)). All diese Techniken weisen jedoch auch signifikante Defizite auf.

a) Verschlüsselung

Verschlüsselungssysteme sind fast so alt wie menschliche Kommunikation selbst.[47] Sie basierten lange Zeit darauf, dass die Kommunikationspartner einen Schlüssel austauschen und mit dessen Hilfe die Nachrichten sowohl verschlüsseln als auch entschlüsseln (symmetrische Verschlüsselung).[48] Problematisch war und ist dabei insbesondere der sichere Austausch des Schlüssels selbst.[49] Einen echten Durchbruch lieferte daher ab den 1970er Jahren die Entwicklung asymmetrischer Verschlüsselungssysteme durch die *public-key cryptography*.[50]

---

[45] Siehe etwa *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (409, 422).

[46] Siehe zu weiteren, hier nicht behandelten datenschützenden Technologien im Bereich der computergestützten Berechnung und der Datenbankabfrage (z. B. *zero-knowledge proofs*) *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (405 ff.); zu Technologien der Entscheidungshilfe, die Verbraucher nutzen können, wie Bewertungs- und Vergleichsportalen oder persönlichen digitalen Assistenten, *Gal/Elkin-Koren*, 30 Harvard Journal of Law and Technology 2016, 309 (313 ff.); *Gal*, 25 Michigan Telecommunication & Technology Law Review 2018, 59 (64 ff.); zu Märkten, auf denen Nutzer ihre Daten selbst monetarisieren können (*personal data economy*), *Reiners*, ZD 2015, 51; *Elvy*, 117 Columbia Law Review 2017, 1369 (1392 ff.); *Acquisti/Taylor/Wagman*, 54 Journal of Economic Literature 2016, 442 (473 f.).

[47] Siehe den historischen Überblick bei *Kahn*, The Codebreakers, 1973, Kapitel 3; knapp *Kaijser/Markwitz*, DuD 2008, 396.

[48] *Menezes*, in: *Menezes* et al. (Hrsg.), Handbook of Applied Cryptography, 1996, 1 (15 ff.).

[49] *Hellmann*, 40(5) IEEE Communications Magazine 2002, 42 (44).

[50] Grundlegend *Diffie*, *Whitfield/Hellman*, 22 IEEE Transactions on Information Theory 1976, 644; *Rivest/Shamir/Adleman*, 21 Communications of the ACM 1978, 120; Übersicht bei *Hellmann*, 40(5) IEEE Communications Magazine 2002, 42 (44 ff.); *Menezes*, in: *Menezes* et al. (Hrsg.), Handbook of Applied Cryptography, 1996, 1 (25 ff.).

Sie macht sich bestimmte mathematische Einwegfunktionen zu Nutze (*trapdoor one-way functions*), bei denen zwar ein Funktionswert zu einem beliebigen Eingabewert schnell errechnet werden kann, jedoch Eingabewerte, die einen bestimmten Funktionswert ergeben, mit heute zur Verfügung stehender Rechenleistung[51] nur in prohibitiv langer Zeit gefunden werden können (zum Beispiel Primfaktoren bei Produkten aus sehr großen Primzahlen).[52] So kann schnell überprüft werden, dass der private zum öffentlichen Schlüssel gehört, der private jedoch aus dem öffentlichen Schlüssel nicht mit sinnvollem Ressourceneinsatz abgeleitet werden.[53] Dadurch wird der sichere Schlüsselaustausch entbehrlich, weil jedermann mit einem öffentlich zur Verfügung stehenden Schlüssel Informationen so verschlüsseln kann, dass sie nur der Inhaber des privaten Schlüssels wieder entschlüsseln kann. Damit A eine verschlüsselte Nachricht an B senden kann, muss A daher nur den von B zur Verfügung gestellten öffentlichen Schlüssel kennen. Die Dechiffrierung kann jedoch nur A vornehmen, wenn sonst niemand im Besitz des privaten Schlüssels ist. Dieses Verfahren liegt etwa digitalen Signaturen[54] und der Blockchain-Technologie zu Grunde.[55] Eine Kombination von symmetrischer und asymmetrischer Verschlüsselung wird für das https-Protokoll genutzt, das sichere Datenübertragung im Internet ermöglicht[56] und durch Nutzer als Standard definiert werden kann,[57] sowie für die Verschlüsselung von Messagingdiensten wie WhatsApp[58] oder Threema.[59]

Asymmetrische Verschlüsselung hat daher sicheren Nachrichtenaustausch zu sehr geringen Kosten möglich gemacht.[60] Im hier interessierenden Kontext stellen sich jedoch bereits auf technischer Ebene zwei Probleme. Erstens nützt eine Verschlüsselung des Datenstroms nur gegen ein Auslesen durch Nichtberechtigte, nicht aber gegen Tracking durch Erstanbieter von Webseiten oder Apps oder aber Drittanbieter, denen der Erstanbieter eine Berechtigung erteilt hat. Wer auf amazon.com bestellt, muss mit Amazon interagieren und es

[51] Zum bislang nur theoretisch möglichen Bruch asymmetrischer Verschlüsselung durch Quantencomputer (Shor's algorithm), siehe *Nielsen/Chuang*, Quantum Computation and Quantum Information, 10th Anniversary Edition, 2010, 11.

[52] *Menezes*, in: *Menezes* et al. (Hrsg.), Handbook of Applied Cryptography, 1996, 1 (8 f.); siehe auch *Rivest/Shamir/Adleman*, 21 Communications of the ACM 1978, 120 (122 f.); *Hellmann*, 40(5) IEEE Communications Magazine 2002, 42 (44).

[53] *Menezes*, in: *Menezes* et al. (Hrsg.), Handbook of Applied Cryptography, 1996, 1 (25 f.).

[54] *Rivest/Shamir/Adleman*, 21 Communications of the ACM 1978, 120; *Menezes*, in: *Menezes* et al. (Hrsg.), Handbook of Applied Cryptography, 1996, 1 (28 ff.).

[55] *Narayanan et al.*, Bitcoin and Cryptocurrency Technologies, 2016, Kapitel 1.

[56] *Zakir et al.*, Proceedings of the 2013 Conference on Internet Measurement Conference 2013, 291 (292); *TipTopSecurity*, How Does HTTPS Work? RSA Encryption Explained (10.9.2017), https://TipTopSecurity.com/how-does-https-work-rsa-encryption-explained/.

[57] Siehe etwas https://addons.mozilla.org/de/firefox/addon/https-everywhere/.

[58] *WhatsApp*, Encryption Overview, Technical White Paper, 2017, 4 ff.

[59] *Threema*, Cryptography Whitepaper, 2019, 4 ff.

[60] *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (400 f.).

wissen lassen, was er wann zu welchen Konditionen bestellen möchte. Daher schützt https naturgemäß nicht gegenüber dem Rezipienten der Informationen.[61] Zudem wird https von vielen Drittanbietern von vornherein nicht unterstützt.[62] Substantielle Abhilfe bieten identitätsverschleiernde, verschlüsselnde Browser wie Tor,[63] die jedoch selten genutzt werden.[64]

Zweitens nimmt Verschlüsselung Rechenkapazität in Anspruch. Zwar wird an Verschlüsselungsformen gearbeitet, die mit geringer Rechenkapazität auskommen (*lightweight cryptography*);[65] im Internet der Dinge haben einzelne Objekte jedoch häufig nur äußerst beschränkte Verarbeitungsressourcen, sodass selbst *lightweight cryptography* nicht immer einsetzbar bzw. zielführend ist.[66] Insgesamt schützt Verschlüsselung daher eher gegen Hacking, weniger gegen Tracking.

b) Identity-Management-Systeme

Im Gegensatz zur Verschlüsselung von Inhalten, die den Kommunikationsprozess selbst betreffen, geht es bei Identity-Management-Systemen im Schwerpunkt um Zugriffsrechte auf bestimmte Informationen oder Funktionalitäten.[67] So soll etwa sichergestellt werden, dass nur berechtigte Nutzer auf ein Gerät zugreifen und keine Informationen über Aktivitäten anderer Nutzer auslesen können. Dies ist gerade für das Internet der Dinge essenziell. Eigenschaften wie *unlinkability* und *unobservability* kennzeichnen dabei technische Schranken, die verhindern, dass Dritte erfahren können, wofür bestimmte (IoT-)Geräte genutzt werden.[68] Besonders wichtig ist es, dafür zu sorgen, dass IoT-Geräte multiple Identitäten managen können, sodass Dritte diese Geräte nutzen können, ohne dass in gleicher Weise wie vom Eigentümer oder regelmäßigen Nutzer Daten erhoben werden. Hier helfen beispielsweise einfach zu bedienende Optionen für nicht identifizierte Gästenutzer oder für pseudonyme Nutzung.[69] Verwirklicht werden kann dies mit Protokollen wie dem von

---

[61] *TipTopSecurity*, How Does HTTPS Work? RSA Encryption Explained (10.9.2017), https://TipTopSecurity.com/how-does-https-work-rsa-encryption-explained/.

[62] *Englehardt/Narayanan*, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 1388 (1396).

[63] *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (402).

[64] *Datta*, The World Wide Web Conference 2019, 351 (354, 359).

[65] *Eisenbarth et al.*, 24 IEEE Design & Test of Computers 2007, 522; *Omrani/Rhouma/Sliman*, in: Tobji et al. (Hrsg.), International Conference on Digital Economy, Cham 2018, 107.

[66] *McKay et al.*, Report on Lightweight Cryptography, NISTIR 8114, 2017, 1.

[67] *Hansen et al.*, 9 Information Security Technical Report 2004, 35; *Independent Centre for Privacy Protection Schleswig-Holstein/Studio Notarile Genghini*, Identity Management Systems (IMS): Identification and Comparison, Study prepared under contract for Institute for Prospective Technological Studies, Sevilla 2003.

[68] *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (399f.); *Rosner/Kenneally*, Clearly Opaque. Privacy Risks of the Internet of Things, Bericht, 2018, 106.

[69] Siehe etwa die Idemix-Anwendung von *Camenisch/Van Herreweghen*, Proceedings of

Maler entwickelten *User-Managed Access* (UMA), bei dem eine zentrale Protokollinstanz geschaffen wird, über die Verfügungsberechtigte an verschiedene Personen abgestufte Formen der Erlaubnis der Nutzung von Geräten und Daten erteilen können.[70] Letztlich geht es also bei Identitätsmanagementsystemen um ein nuanciertes System von Berechtigungen des Zugriffs auf Daten, das sowohl nach unterschiedlichen Nutzern als auch nach unterschiedlichen Verarbeitern differenziert. Hier greifen also unternehmensseitige und nutzerseitige Technologien ineinander.

Ein zentraler Schwachpunkt besteht jedoch darin, dass die grundlegende Infrastruktur zunächst einmal seitens des Anbieters bereitgestellt werden muss, da sonst die Kontrollversuche des Nutzers ins Leere laufen.[71] Jedenfalls dann, wenn derartige Systeme mit ökonomisch vertretbarem Aufwand und ohne signifikante Störung der technischen Funktionalität anbieterseitig installiert werden können, dürfte dies regelmäßig bereits *de lege lata* im Rahmen von Art. 25 Abs. 1 DS-GVO geschuldet sein.[72] Allerdings stellt die Interoperabilität verschiedener Identity-Management-Systeme eine ungelöste Herausforderung dar.[73]

c) Anti-Tracking-Tools

Zumeist allein auf Nutzerinitiative basiert hingegen die Verwendung von Anti-Tracking-Tools. Dabei handelt es sich um technische Vorrichtungen, die den Einsatz von Geräte-Identifiern verhindern oder zumindest erschweren sollen. Eine Reihe von Browser-Erweiterungen können etwa Signale aussenden, die Webseiten oder Apps kommunizieren, dass der Nutzer kein Tracking wünscht (*do not track* http-Header).74 Diesen Anwendungen mangelt es jedoch bislang an umfassender rechtlicher und technischer Bindungswirkung.[75] Andere Strategien zur Abwehr von Cookies sind entweder ineffektiv (Löschung der Brow-

---

the 9th ACM Conference on Computer and Communications Security 2002, 21; ferner allgemein *Rosner/Kenneally*, Clearly Opaque. Privacy Risks of the Internet of Things, Bericht, 2018, 106; *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (403 f.).

[70] *Maler*, 2015 IEEE Security and Privacy Workshops 2015, 175.

[71] *Hansen et al.*, 9 Information Security Technical Report 2004, 35 (40 f.).

[72] Dazu genauer unten, § 6 B.I.2.b).

[73] *El Haddouti/El Kettani*, 12 IJCSI International Journal of Computer Science Issues 2015, 98 (104 f.).

[74] Etwa die *do not track*-Erweiterung (siehe https://support.google.com/chrome/answer/2790761; oder https://www.i-dont-care-about-cookies.eu/.

[75] Siehe dazu im Einzelnen unten, § 6 C.I.3.c)aa)(2); ferner *Libert*, Proceedings of the 2018 World Wide Web Conference, 207 (213 f.); *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 9; Europäisches Parlament, Bericht über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG, A8–0324/2017, vom 20.10.2017, 102; *Franken/Van Goethem/Joosen*, 27th USENIX Security Symposium (USENIX Security 18) 2018, 151; *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (421); *Tavanti*, RDV 2016, 295 (302).

ser-Historie[76]) oder technisch verhältnismäßig komplex. Zwar bieten manche Entwickler von Drittanbietercookies auf ihrer Webseite eine Möglichkeit zum Opt-Out an (zum Beispiel Google Analytics[77]), jedoch müssten Nutzer dafür letztlich eine Vielzahl von Anbietern ausfindig machen und aufsuchen,[78] was bei mehr als 81.000 Drittanbietern[79] nicht realistisch erscheint. Zunehmend erfolgreicher sind jedoch Browser-Erweiterungen, die nicht nur Präferenzen kommunizieren, sondern getrackte Informationen unitarisieren, randomisieren,[80] oder Anfragen für Drittanbietercookies blockieren.[81] Diese sind mittlerweile etwa bei Firefox als Voreinstellung eingerichtet,[82] und standardmäßig in die Anti-Tracking-Browser Tor[83] oder Brave integriert.[84] Firefox, Tor und Brave werden jedoch bislang nur von einer Minderheit genutzt;[85] zudem können auch ihre Maßnahmen überwunden werden.[86]

Technisch noch schwieriger umzusetzen sind Maßnahmen, die gegen *fingerprinting* gerichtet sind.[87] Bei diesen kommt erschwerend hinzu, dass Tracking auf der Grundlage von *fingerprinting* Durchschnittsnutzern ohnehin kaum bekannt ist, was noch verschärft auf mögliche Abwehrstrategien zutrifft. Auch hier bieten erste Browser-Erweiterungen Hilfe,[88] sie sind jedoch deutlich weniger effektiv als bei der Blockierung von Drittanbietercookies.[89]

---

[76] *Soltani et al.*, 2010 AAAI Spring Symposium Series, 158; *Ayenson et al.*, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning, Working Paper, 2011, https://ssrn.com/abstract=1898390; *Acar et al.*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security 2014, 674 (684).

[77] https://tools.google.com/dlpage/gaoptout; siehe auch *Degeling et al.*, 26th Annual Network and Distributed System Security Symposium (NDSS '19), 1 (11).

[78] Siehe etwa https://www.ckl-kore.de/en/cookie-and-opt-out-notes.html.

[79] *Englehardt/Narayanan*, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 1388 (1394 f.); allerdings waren 2016 nur Google, Facebook, Twitter, Amazon, AdNexus und Oracle auf mehr als 10 % der Seiten als Drittanbieter tätig (ebd.).

[80] Siehe die Aufstellung bei *Datta*, The World Wide Web Conference 2019, 351 (354).

[81] Die Firefox-Erweiterung zur Blockierung von Drittanbietercookies ließ unter den 1 Million populärsten Webseiten lediglich bei 0,4 % der Webseiten Drittanbietercookies zu, die Erweiterung Ghostery reduzierte ebenfalls die Anzahl erheblich, siehe *Englehardt/Narayanan*, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 1388 (1396 f.).

[82] https://support.mozilla.org/en-US/kb/disable-third-party-cookies.

[83] https://www.torproject.org/de/about/history/.

[84] https://brave.com/de/features/.

[85] *Muth*, Dieser Anti-Tracking-Browser will Nutzer fürs Werbungschauen belohnen, SZ (19.11.2019), https://www.sueddeutsche.de/digital/brave-browser-chrome-werbung-netz-javascript-tracking-1.4688866.

[86] *Franken/Van Goethem/Joosen*, 27th USENIX Security Symposium (USENIX Security 18) 2018, 151.

[87] *Acar et al.*, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security 2014, 674 (684).

[88] Etwa die Browser-Erweiterung von Firefox, https://blog.mozilla.org/firefox/de/loesche-deinen-digitalen-fingerabdruck-in-firefox/.

[89] *Englehardt/Narayanan*, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 1388 (1400) zeigen, dass lediglich etwa die Hälfte aller

Der dritte Typ von Geräte-Identifiern, die *unique strings*, können zum Teil manuell abgeschaltet oder geändert werden.[90] Dies setzt jedoch Kenntnisse und Eigeninitiative in einer Form voraus, die bei Durchschnittsnutzern typischerweise nicht anzutreffen ist. Vor allem implantieren etwa zwei Drittel aller Smartphone Apps eigene, persistente, nicht veränderbare *unique strings*, so dass die manuelle Änderung der Android Werbe-ID oder der iOS Ad-ID ins Leere läuft.[91] Schließlich bieten mehrere Intermediäre – etwa Privad[92] und Adnostic[93] – Lösungen für personalisierte Werbung an, bei denen die personenbezogenen Attribute gegenüber den Werbetreibenden nicht offenbart werden, aber dennoch nutzungsbasierte Werbung gezeigt werden kann.[94] Auch diese Intermediäre werden jedoch gegenwärtig kaum genutzt. Zudem haben sie Zugriff auf die personenbezogenen Daten, sodass zumindest Interessenkonflikte bestehen, die zu einer Kompromittierung der Privatsphäre der Nutzer führen können.

2. *Rechtlicher Rahmen*

Den maßgeblichen rechtlichen Rahmen für die Beurteilung von Instrumenten des Selbstdatenschutzes in datenbasierten Austauschverhältnissen bietet Art. 25 DS-GVO in seiner Verzahnung mit dem Vertragsrecht. Art. 25 DS-GVO richtet sich allerdings, schon ausweislich Art. 24 Abs. 1 DS-GVO, lediglich an die Verantwortlichen, also die Anbieter, nicht jedoch an die Nutzer.[95] Daher können nutzerseitige Datenminimierungsstrategien von den Verpflichtungen in Art. 25 DS-GVO nur mittelbar erfasst sein. Insoweit wird vertreten, dass Anbieter auch im Rahmen von Vertragsverhältnissen durch die Pflicht zu Datenschutz durch Technikgestaltung zumindest gezwungen sind, Maßnahmen des Selbstdatenschutzes zu tolerieren.[96] Nach hier vertretener Auffassung wird man zwar nach den einzelnen Maßnahmen und auch der vertraglichen Regelung differenzieren müssen. Es lässt sich jedoch grundsätzlich noch

---

fingerprinting scripts durch Erweiterungen wie Disconnect oder EasyList und EasyPrivacy blockiert werden; auch die Firefox Tracking Protection hilft kaum, siehe *Datta*, The World Wide Web Conference 2019, 351 (359).

[90] So etwa die Werbe-ID von Android und die Ad-ID von iOS, siehe *Ruhenstroth*, Smartphone-Nutzer sollten jetzt ihre Werbe-ID ändern, Mobilsicher (24.5.2018), https://mobilsicher.de/hintergrund/smartphone-nutzer-sollten-jetzt-ihre-werbe-id-aendern#WerbeID3.

[91] *Reyes et al.*, Proceedings on Privacy Enhancing Technologies 2018 (3), 63 (63, 73).

[92] *Guha/Cheng/Francis*, 8th USENIX Symposium on Networked Systems Design and Implementation 2011, 169.

[93] *Toubiana et al.*, Adnostic: Privacy Preserving Targeted Advertising, Network and Distributed System Security Symposium 2010, o. S.; https://crypto.stanford.edu/adnostic/.

[94] *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (408 f.).

[95] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 20.

[96] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 63.

weitergehend aus Art. 25 DS-GVO die Maßgabe entnehmen, dass Anbieter den Einsatz derartiger Instrumente nicht nur nicht erschweren dürfen, sondern vielmehr ihre Anwendung, im Rahmen der Gewährleistung der Funktionalität des angebotenen Produkts, ermöglichen und aktiv unterstützen müssen.

a) Allgemeine Kriterien

Allerdings kann der Umfang einer diesbezüglichen Pflicht immer nur im Einzelfall festgestellt werden. Schon aus dem Wortlaut von Art. 25 Abs. 1 DS-GVO erhellt dabei, dass eine Reihe von Faktoren berücksichtigt werden müssen (technische Möglichkeiten, Implementierungskosten, Typ der Verarbeitung, Risiken). Insbesondere sind Verantwortliche nicht verpflichtet, Maßnahmen zu unterstützen oder auch nur zu tolerieren, welche die technische Funktionalität des Angebots, inklusive der IT-Sicherheit, gefährden. Zentral ist hier auch, wie effektiv die Maßnahmen dazu beitragen, erhebliche datenschutzrechtliche Risiken zu minimieren („Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken", Art. 25 Abs. 1 DS-GVO), und welche Kosten sie verursachen. Maßnahmen, die sensitive Daten verschleiern, muss daher mit deutlich stärkerem Entgegenkommen begegnet werden als anderen. Rein ökonomische Interessen der Anbieter jedenfalls sprechen nicht grundsätzlich gegen eine Unterstützungs- oder Tolerierungspflicht.

Die Maßstäbe für die rechtliche Behandlung des Selbstdatenschutzes in Vertragsverhältnissen unter Geltung der DS-GVO sind im Einzelnen noch weitgehend ungeklärt. Die folgenden Richtlinien können für eine differenzierte Betrachtung aufgestellt werden, die jeweils auf die unterschiedlichen Faktoren und Interessen im Einzelfall Rücksicht nehmen muss.

b) Unterstützungspflicht

Am weitesten geht eine Unterstützungspflicht der Verantwortlichen, die eine Obligation umfasst, technische Kompatibilität mit Instrumenten des Selbstdatenschutzes jeweils aktiv herzustellen, zum Beispiel durch die Bereitstellung von entsprechenden Schnittstellen.[97] Das Bundesverfassungsgericht hat, mit Blick auf das grundgesetzliche Recht auf informationelle Selbstbestimmung, geurteilt, dass informationeller Selbstschutz auch tatsächlich möglich und zumutbar sein müsse und insofern eine staatliche Verantwortung im Sinne einer Schutzpflicht bestehe.[98] Dieser Rechtsgedanke lässt sich auch für die Auslegung von Art. 25 DS-GVO fruchtbar machen. Eine Unterstützungspflicht wird man nach der DS-GVO jedenfalls dann grundsätzlich annehmen können, wenn die Datenverarbeitung, welche durch die jeweiligen Instrumente verhin-

[97] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 63; siehe auch *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 172.

[98] BVerfG MMR 2007, 93 (93).

dert werden soll, rechtswidrig wäre[99] – unabhängig davon, ob sie durch den Verantwortlichen oder Dritte erfolgen würde. Wenn also beispielsweise die Erhebung von Ortsdaten durch den Anbieter ohnehin als datenschutzrechtswidrig eingestuft werden müsste, so muss der Anbieter, im Rahmen des technisch Möglichen und ökonomisch Zumutbaren, auch die Nutzung des Dienstes unter Verwendung von Instrumenten, welche Ortsdaten verschleiern,[100] aktiv ermöglichen. A fortiori besteht dann eine Pflicht zur Tolerierung derartiger Instrumente.

c) Tolerierungspflicht

Schwieriger ist der Fall zu entscheiden, wenn die Verarbeitung der betreffenden Daten rechtmäßig wäre. Nach hier vertretener Auffassung ist dann danach zu differenzieren, inwieweit die Überlassung dieser Daten explizite vertragliche Gegenleistung für die Erbringung des Dienstes ist. Grundsätzlich wird man aus Art. 25 Abs. 1 DS-GVO ableiten können, dass die Verwendung von Instrumenten des Selbstdatenschutzes zwar nicht aktiv unterstützt, aber doch toleriert werden muss, sofern diese ohne Weiteres mit dem Angebot des Anbieters technisch kompatibel sind.[101] In der Folge muss der Anbieter seinen Dienst so erbringen, als ob keine nutzerseitigen *privacy-enhancing technologies* eingesetzt würden. Wenn dies allerdings zu signifikanten Einbußen des Anbieters führt, etwa weil der Wert der Gegenleistung durch die Verschleierung erheblich sinkt, so führt dies zu Kosten, die man als indirekte Implementierungskosten bezeichnen könnte. Diese müssen nach Art. 25 Abs. 1 DS-GVO zugunsten des Anbieters berücksichtigt werden – richtigerweise jedoch nur dann, wenn der Anbieter einen Anspruch auf die Überlassung dieser Daten hat bzw. die Überlassung eine wirksame Bedingung für die Leistungserbringung darstellt. Wäre hingegen eine Verarbeitung der Daten zwar rechtmäßig, ist sie jedoch vertraglich nicht vorgesehen, so ist das Risiko, dass die Daten nicht wie erhofft erhoben und verarbeitet werden können, vertraglich dem Anbieter zugewiesen. Diese vertragliche Wertung muss sich auch in Art. 25 Abs. 1 DS-GVO fortsetzen: Diesbezügliche Kosten (z. B. Gewinneinbußen) sind dann nicht berücksichtigungsfähig. Folglich muss der Anbieter die Anwendung von Instrumenten des Selbstdatenschutzes tolerieren.

Eine Tolerierungspflicht scheidet daher nach hier vertretener Auffassung lediglich dann aus, wenn die Überlassung der infrage stehenden Daten wirk-

[99] Vgl. auch *Johannes/Roßnagel*, Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt, 2016, 18 f.

[100] Dazu etwa *Johannes/Roßnagel*, Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt, 2016, 105.

[101] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 25 DS-GVO Rn. 63; siehe auch *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 172; *Hornung/Spiecker gen. Döhmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Einleitung Rn. 246.

samer Inhalt einer konkludenten Bedingung für die Leistungserbringung oder einer synallagmatischen Verpflichtung ist. Denn letztlich wirkt die Verschleierung von Daten für den Anbieter ähnlich wie eine Nichtüberlassung. Bei einer Nichtüberlassung jedoch wäre eine Leistungserbringung in diesen Fällen nicht geschuldet, weil entweder die Bedingung nicht erfüllt ist (§ 158 BGB[102]) oder die synallagmatische Gegenleistung nicht erbracht wurde (§ 320 Abs. 1 S. 1 BGB).[103] Allerdings wird man auch in diesen Fällen, wie in § 4 bereits ausgeführt,[104] den Einsatz von Instrumenten des Selbstdatenschutzes in Ansehung von Art. 25 DS-GVO und dem Datenschutzgrundrecht bzw. dem Recht auf informationelle Selbstbestimmung regelmäßig nicht als *rechtswidrige* Pflichtverletzung qualifizieren können. Rechtsfolge des Einsatzes von Verschleierungsstrategien durch den Anbieter ist daher, selbst wenn eine Tolerierungspflicht abgelehnt wird, lediglich ein Leistungsverweigerungsrecht des Anbieters, nicht aber ein Anspruch auf Schadensersatz.

3. Anreize und Beschränkungen

Nicht nur ist nach dem Gesagten die Pflicht zur Unterstützung oder auch nur Tolerierung von Maßnahmen des Selbstdatenschutzes rechtlich noch wenig konturiert. Alle genannten Verfahren haben ferner technische oder praktische Unzulänglichkeiten, die dazu führen, dass eine vollständige Souveränität von Nutzern über die eigenen Daten auf technischem Wege selbst bei hochsophistizierten Akteuren nicht gewährleistet werden kann.[105] Schwerer wiegt jedoch, dass vor allem Durchschnittsnutzer bislang keine hinreichenden Anreize zur Verwendung von kontrollerhöhenden Technologien zu haben scheinen. Außerhalb von Protokollen, die bereits in gängige Produkte vorinstalliert und dort voreingestellt sind, werden nutzerbasierte *privacy-enhancing technologies* wenig eingesetzt.[106] Dies kann letztlich wiederum durch die Typen von Marktversagen, welche auch sonst für das Paradox der Privatheit verantwortlich zeichnen,[107] erklärt werden.[108]

Erschwerend kommt hinzu, dass die meisten nutzerbasierten Technologien auf ein Entgegenkommen seitens der Anbieter angewiesen sind, das jedoch häufig nur unvollständig oder gar nicht gewährt wird, obwohl dies, bei aller Relevanz der Konstellation im Einzelfall, tendenziell wie gesehen nach

---

[102] Dazu näher *Hacker*, ZfPW 2019, 148 (175 f.).

[103] Siehe dazu genauer oben, § 4 B.I.3.b)bb)(3)(b).

[104] Siehe § 4 B.I.3.b)bb)(3)(a)(bb)a.

[105] Siehe *Johannes/Roßnagel*, Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt, 2016, 24.

[106] Siehe die Zahlen in *Datta*, The World Wide Web Conference 2019, 351 (354); ferner *Acquisti/Taylor/Wagman*, 54 Journal of Economic Literature 2016, 442 (476); *Johannes/Roßnagel*, Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt, 2016, 25 f.

[107] Siehe oben, § 3 B.II.1.

[108] *Solove*, 126 Harvard Law Review 2013, 1880 (1883 ff.).

Art. 25 DS-GVO geschuldet ist. So erfasst eine Verschlüsselung, die zum Beispiel von WhatsApp standardmäßig implementiert wird, sämtliche Inhaltsdaten, die auch vor dem Zugriff durch WhatsApp selbst verborgen werden.[109] Metadaten hingegen, die für die Ableitung von Präferenzen und Persönlichkeitseigenschaften ebenso wichtig sein können,[110] sind vor einem Zugriff durch WhatsApp nicht geschützt.[111] Ob dies mit Art. 25 DS-GVO in Einklang steht, darf durchaus bezweifelt werden.[112] Ferner besteht auch eine sich verstärkende Tendenz zur Verwendung von Identity-Management-Systemen durch abgestufte Möglichkeiten der Zuweisung von Berechtigungen, etwa im Rahmen von unterschiedlichen Graden der Öffentlichkeit eines Facebook-Kontos.[113] Allerdings adressieren diese Berechtigungen bislang in den allermeisten Fällen lediglich, welche anderen Nutzer auf bestimmte Inhalte zugreifen dürfen; sie regeln nicht die hier an sich zentrale Frage, welche Unternehmen die mittels Tracking-Technologien erhobenen Daten für eigene Zwecke verwenden dürfen.[114] Hier scheinen die Anreize für die Unternehmen, derartige Systeme zur Verfügung zu stellen, wiederum noch nicht hoch genug zu sein. Besonders augenfällig ist die Möglichkeit der Konterkarierung nutzerbasierter Strategien bei Anti-Tracking-Tools: Zu ihrer technischen Überwindbarkeit kommt hinzu, dass technisch äußerst einfach *tracking walls* (z. B. mittels *overlay*) implementiert werden können.[115] Die Analyse des vierten Kapitels dieser Arbeit hat zwar gezeigt, dass ihre datenschutzrechtliche Zulässigkeit äußerst umstritten ist.[116] Solange die hier vertretene weitgehende Unzulässigkeit jedoch nicht eindeutig gerichtlich festgestellt ist, stellen *tracking walls* nach wie vor ein effektives Mittel dar, den Nutzen von Anti-Tracking-Tools zu beschränken.

Insbesondere der ständige Wettbewerb zwischen den Entwicklern von Anti-Tracking-Tools einerseits und von neuen Tracking-Methoden andererseits zeigt, dass auch bei hinreichenden Anreizen zur Nutzung dieser Werkzeuge erhebliche Friktionen entstehen können. Beide Lager liefern sich einen technologischen Rüstungswettstreit unter Einsatz erheblicher Ressourcen,[117] die

[109] *WhatsApp*, Encryption Overview, Technical White Paper, 2017, 4 ff.

[110] Siehe etwa *Chittaranjan/Blom/Gatica-Perez*, 17 Personal and Ubiquitous Computing 2013, 433; Übersicht bei *Piwek/Joinson*, in: Little et al. (Hrsg.), Behavior Change Research and Theory, 2017, 137 (140–147).

[111] https://www.whatsapp.com/legal/?eea=1#privacy-policy (zuletzt abgerufen am 14.10.2019).

[112] Siehe genauer oben, § 4 C.III. sowie soeben, § 6 B.I.2.

[113] *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (422).

[114] *Hansen et al.*, 9 Information Security Technical Report 2004, 35 (40 f.); *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (423).

[115] *Degeling et al.*, 26th Annual Network and Distributed System Security Symposium (NDSS '19), 1 (11).

[116] Siehe oben, § 4 B.I.3.a)dd)(5)(b) und § 4 C.I.3.b).

[117] Siehe etwa *Kerkmann*, Wer hat die Macht über den Werbeblock?, Handelsblatt (12.8.2016), https://www.handelsblatt.com/unternehmen/it-medien/facebook-vs-adblock-plus-wer-hat-die-macht-ueber-den-werbeblock/14005570-all.html; *Hacker*, ZfPW 2019, 148 (174).

letztlich zu einem großen Teil soziale Kosten darstellen.[118] Auf eine Verbesserung des Schutzes wird typischerweise mit einer Verbesserung der Tracking-Möglichkeiten unter Umgehung bisheriger Schutzvorkehrungen geantwortet. Demgegenüber erscheint es nicht nur für die Nutzerkontrolle über Daten effektiver, sondern auch volkswirtschaftlich effizienter, gesetzlich klare Alternativen zu bieten, welche die Durchsetzung heterogener Datenschutzpräferenzen am Markt ermöglichen (dazu § 6 C.II.).

II. Rechtmäßigkeitskontrolle durch maschinelles Lernen

Die soeben vorgestellten *privacy-enhancing technologies* zielten darauf ab, durch technische Instrumente zu verhindern, dass personenbezogene Daten überhaupt gesammelt, durch Dritte abgegriffen oder zweckentfremdet werden. Eine zweite Form technischer Minimierung von Datenschutzrisiken setzt hingegen nicht an den Daten selbst, sondern an der Analyse der Verlautbarungen von Verantwortlichen an, in denen der intendierte Umgang mit den Daten beschrieben wird. Dafür bieten sich insbesondere Nutzungsbedingungen und Datenschutzerklärungen an, die standardmäßig von allen großen Anbietern veröffentlicht werden.

Bereits seit etlichen Jahren bestehen Initiativen von Datenschützern, die eine Kontrolle dieser Veröffentlichungen durch kollektive Anstrengungen gewährleisten wollen.[119] Nutzer lesen und bewerten im Rahmen dieser Initiativen etwa Nutzungsbedingungen oder Datenschutzerklärungen, die dann auf Webseiten gebündelt zur Verfügung gestellt werden.[120] Diese manuelle Form der Kontrolle stößt naturgemäß schnell an Ressourcengrenzen, kann aber nunmehr zunehmend automatisiert werden. *Ackerman* und *Cranor* entwickelten bereits 1999 den Prototyp eines automatisierten Agenten (*privacy critic*), der die Privatsphäreentscheidungen der Nutzer beobachtet und kritisch kommentiert.[121] In jüngerer Vergangenheit werden nun verstärkt Techniken maschinellen Lernens genutzt, um die Analyse von unternehmensseitigen Veröffentlichungen voranzutreiben. Die Idee dahinter ist jeweils, dass eine verhältnismäßig geringe Anzahl von Nutzungsbedingungen oder Datenschutzerklärungen annotiert wird, um Trainingsdaten bereitzustellen, mit denen ein selbstlernendes algorithmisches Modell kalibriert wird. Dieses kann dann auf bislang nicht bewertete Veröffentlichungen angewandt werden und so Nutzer gezielt vor besonders weitgehenden oder rechtswidrigen Praktiken der Datenerhebung warnen.

---

[118] *Wagner/Eidenmüller*, 86 University of Chicago Law Review 2019, 581 (587, 589).

[119] *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (417 f.).

[120] Siehe etwa Terms of Service; Didn't Read (http://tosdr.org/), bei dem Nutzungsbedingungen Noten erhalten; TOSBack (https://tosback.org/), bei dem Änderungen in Nutzungsbedingungen nachvollziehbar gemacht werden.

[121] *Ackerman/Cranor*, CHI Extended Abstracts 1999, 258.

1. Relevante Techniken

Automatisierte Formen der Kontrolle der Rechtmäßigkeit und Risiken von datenbezogenen Veröffentlichungen konzentrieren sich auf die Analyse von Datenschutzerklärungen einerseits und Nutzungsbedingungen andererseits, da diese Dokumente die meisten Informationen über die geplante Datenverarbeitung von Anbietern beinhalten. Zugleich muss die Analyse unter dem caveat erfolgen, dass die tatsächliche Form der Datenverarbeitung von der in den Dokumenten beschriebenen abweichen kann: Empirische Untersuchungen zeigen, dass Datenschutzerklärungen, sofern sie nicht gänzlich fehlen, häufig unvollständig sind.[122] Nichtsdestoweniger bieten sie wertvolle Anhaltspunkte für die tatsächliche Datenverarbeitung, gewissermaßen in Form einer unteren Schranke.

a) Automatisierte Kontrolle der Datenschutzerklärung

Wie bereits mehrfach angesprochen, leiden Datenschutzerklärungen unter massiver rationaler und auch beschränkt rationaler Ignoranz.[123] Selbst wenn diese Pflichtinformationen daher wertvolle Hinweise für informierte Entscheidungen von Nutzern beinhalten, werden sie kaum zur Kenntnis genommen, was insbesondere durch die Komplexität und Länge der Erklärungen bedingt ist. Eine automatisierte Erfassung und Aufbereitung des Inhalts kann daher einen erheblichen Beitrag dazu leisten, Transparenz hinsichtlich der Bedingungen der Datenverarbeitung herzustellen und Informationen so zu komprimieren, dass ihre Rezeption wahrscheinlicher und kognitiv weniger belastend wird (*transparency-enhancing technologies*[124]). Mehrere Modelle sind hier in den letzten Jahren entwickelt worden.[125] Sie basieren jeweils auf Anwendungen aus dem Bereich *natural language processing*[126] und implementieren zumeist Strategien des überwachten Lernens.[127] Sie können einerseits die Nutzer

---

[122] Siehe sogleich, unter § 6 B.II.1.a)bb); ferner *Marotta-Wurgler*, Does ‚Notice and Choice' Disclosure Regulation Work? An Empirical Study of Privacy Policies, Michigan Law: Law and Economics Workshop, 2015, www.law.umich.edu/centersandprograms/lawandeconomics/workshops/Documents/Paper13.Marotta-Wurgler.Does%20Notice%20and%20Choice%20Disclosure%20Work.pdf, 5.

[123] Siehe oben, § 3 B.II.1.a) und b).

[124] Siehe den Überblick bei *Fischer-Hübner/Berthold*, in: Vacca (Hrsg.), Computer and Information Security Handbook, 3. Aufl. 2017, 759 (772 ff.).

[125] Siehe den Überblick bei *Pałka/Lippi* in: Vogl, Roland (Hrsg.), Research Handbook on Big Data Law, im Erscheinen, https://ssrn.com/abstract=3347364,Teil3.2.

[126] Dadurch werden Elemente eines Texts automatisiert analysiert, siehe etwa den Überblick bei *Story et al.*, Proceedings of the PAL: Privacy-Enhancing Artificial Intelligence and Language Technologies 2019, 24; *Pałka/Lippi* in: Vogl, Roland (Hrsg.), Research Handbook on Big Data Law, im Erscheinen, https://ssrn.com/abstract=3347364; *Manning et al.*, Proceedings of 52nd Annual Meeting of the Association for Computational Linguistics: System Demonstrations 2014, 55.

[127] Dazu oben, § 2 B.II.1.a).

selbst (aa)), andererseits aber auch Aufsichtsbehörden und andere Rechtsdurchsetzungsinstitutionen unterstützen (bb)).

aa) Modelle zur Unterstützung von Nutzern

Für Nutzer selbst ist technische Unterstützung essenziell, wenn Datenschutzerklärungen handlungsleitend werden sollen. Es besteht bereits eine Vielzahl von unterschiedlich stark ausgereiften Instrumenten, auf die Nutzer zugreifen können. So stellte ein Team der Carnegie Mellon University 2013 das „Usable Privacy Policy Project" vor.[128] Dieses Tool nutzt verschiedene Techniken, unter anderem maschinelles Lernen, um die wichtigsten Teile aus Datenschutzerklärungen zu extrahieren und Nutzern in einem verständlichen Format anzuzeigen. Auch andere Instrumente bieten derartige Zusammenfassungen.[129] Die Grundlage für die Identifizierung der bedeutsamen Abschnitte sind beim Usable Privacy Policy Project die Entscheidungen von Experten und Nutzern (*crowdsourcing*),[130] die 115 Datenschutzerklärungen von Hand analysiert haben (Datensatz OPP-115).[131] Das Modell hat mittlerweile bereits über 7000 Datenschutzerklärungen maschinell untersucht und annotiert.[132] Ein anderes Forschungsteam aus der Schweiz und den USA hat etwas später, basierend auf dem Datensatz OPP-115, zwei Instrumente entwickelt, mit denen sich einerseits der Inhalt von Datenschutzerklärungen visualisieren lässt (Polisis)[133] und andererseits spezifische Fragen zu einer Datenschutzerklärung gestellt werden können, die ein *chatbot* beantwortet (PriBot).[134] Beide Applikationen untersuchten automatisiert ein Korpus von 130.000 Datenschutzerklärungen; Polisis erreicht eine Genauigkeit (*accuracy*) von 88 %; die Antworten von PriBot enthalten in 82 % der Fälle eine richtige innerhalb der drei höchst gerankten Antworten.[135] Deutsche und japanische Forscher wiederum entwickelten, gestützt auf einen neuen Datensatz von 45 manuell annotierten Datenschutzerklärungen und einen Naive Bayes Algorithmus, ein Modell (PrivacyGuide), das

[128] *Sadeh et al.*, The Usable Privacy Policy Project, Technical Report, CMU-ISR-13–119, 2013.

[129] Eine Zusammenfassung von Datenschutzerklärungen bietet auch das Tool von *Tomuro/Lytinen/Hornsburg*, Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy 2016, 133; sowie der PrivacyCheck von *Zaeem/German/Barber*, 18(4) ACM Transactions on Internet Technology (TOIT) 2018, Article 53.

[130] *Sadeh et al.*, The Usable Privacy Policy Project, Technical Report, CMU-ISR-13–119, 2013, 9; zur Validität dieses Crowdsourcing-Ansatzes *Wilson et al.*, Proceedings of the 25th International Conference on World Wide Web 2016, 133; *Wilson et al.*, 13 (1) ACM Transactions on the Web (TWEB) 2018, Article 1; Fortschrittsbericht bei *Liu et al.*, Proceedings of COLING 2014, the 25th International Conference on Computational Linguistics: Technical Papers 2014, 884.

[131] https://explore.usableprivacy.org/?view=human.

[132] Siehe https://explore.usableprivacy.org/?view=machine.

[133] https://pribot.org/polisis.

[134] https://pribot.org/bot.

[135] *Harkous et al.*, 27th USENIX Security Symposium 2018, 531.

ebenfalls gute Performancewerte erreichte bei der Zusammenfassung von Datenschutzerklärungen (74 % *accuracy*) und bei Risikowarnungen (90 % *accuracy*).[136] Ein Team von der Columbia University erreichte durchschnittlich 84 % *accuracy* bei der Extraktion der wesentlichen Aspekte einer Datenschutzerklärung (Privee), wobei vor allem das manuell erstellte Korpus von Terms of Service; Didn't Read[137] genutzt wurde.[138] Ein weiteres Projekt, Guard, entwickelt zurzeit ein spanischer Forscher.[139] Das Instrument wird auf Basis von Antworten, die Nutzer in einem Quiz geben, für die Analyse von Datenschutzerklärungen trainiert.[140] Dabei achtet der Entwickler sorgsam auf Diversität unter den Teilnehmern, welche die Trainingsdaten zur Verfügung stellen.[141] In der Folge kann das Modell adaptiv Datenschutzerklärungen untersuchen, Risiken aufzeigen und einen Gesamtscore zwischen null und 100 vergeben.[142] Daraus soll letztlich eine App entstehen, die Nutzern live Hilfestellung bei der Auswahl von Anbietern leistet. Ebenfalls im Aufbau befindet sich zum Zeitpunkt der Abfassung dieses Manuskripts das von einem am EUI angesiedelten Forscherteam entwickelte Modell CLAUDETTE, das Datenschutzerklärungen analysieren und bestimmte Risiken in der Erklärung (*insufficient information*; *unclear language*; *problematic processing*) hervorheben kann.[143] Das Trainingskorpus wurde von Hand durch Experten annotiert.[144] Eine darauf trainierte *support-vector machine* lieferte vielversprechende Performancewerte.[145]

---

[136] *Tesfay et al.*, Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics 2018, 15; siehe auch *Tesfay et al.*, Companion Proceedings of the The Web Conference 2018, 163.

[137] Siehe oben, § 6, Fn. 120.

[138] *Zimmeck/Bellovin*, 23rd USENIX Security Symposium 2014, 1 (7).

[139] https://useguard.com; *Samuel*, Don't want to read privacy policies? This AI tool will do it for you, Vox (27.9.2019), https://www.vox.com/future-perfect/2019/9/27/20883458/ai-digital-privacy-policy-guard.

[140] https://useguard.com, unter „Teach the AI".

[141] https://useguard.com, unter „AI Status".

[142] https://useguard.com/products.

[143] *Contissa et al.*, CLAUDETTE Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence, Report, 2018, https://ssrn.com/abstract=3208596; http://www.claudette.eu/gdpr.

[144] *Contissa et al.*, CLAUDETTE Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence, Report, 2018, https://ssrn.com/abstract=3208596, 53: Korpus von 14 Datenschutzerklärungen; Erweiterung auf 32 Datenschutzerklärungen in *Liepina et al.*, Proceedings of the Third Workshop on Automated Semantic Analysis of Information in Legal Text (ASAIL 2019) 2019, Article 9.

[145] *Contissa et al.*, CLAUDETTE Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence, Report, 2018, https://ssrn.com/abstract=3208596, 54 ff.; Legal Knowledge and Information Systems (JURIX) 2018, 51 (58 f.); *Liepina et al.*, Proceedings of the Third Workshop on Automated Semantic Analysis of Information in Legal Text (ASAIL 2019) 2019, Article 9.

bb) Modelle zur Unterstützung von Aufsichtsbehörden

Die automatisierte Analyse von Datenschutzerklärungen kann nicht nur für Nutzer, sondern auch für Aufsichtsbehörden und andere Rechtsdurchsetzungsinstitutionen von Interesse sein. Ein US-amerikanisches Forscherteam hat ein Klassifizierungsmodell entwickelt (Mobile Apps Privacy System: MAPS), mit dem der Inhalt von Datenschutzerklärungen mit der tatsächlichen Datenverarbeitung von Smartphone Apps verglichen werden kann.[146] Dafür wird einerseits der Code der Apps und andererseits der Inhalt der Datenschutzerklärung mithilfe verschiedener Techniken maschinellen Lernens analysiert.[147] Grundlage für das Training war ein neues Korpus von 350 durch Experten annotierten Datenschutzerklärungen (APP-350).[148] Anhand einer Untersuchung von über 1 Million Apps, die auf dem Google Play Store angeboten werden, zeigten sich mannigfache Defizite; die Performancewerte des Modells waren dabei durchweg im hohen Bereich.[149] Fast 50 % der Apps verfügten auf dem Google Play Store über gar keine Datenschutzerklärung.[150] Bei den übrigen führten 31 % der Links auf Datenschutzerklärungen zu keiner analysierbaren Erklärung, etwa weil das Dokument nicht in englischer Sprache abgefasst war.[151] Im Durchschnitt vollführte jede App 2,89 Verarbeitungen, die nicht in einer Datenschutzerklärung erwähnt wurden.[152] 12 % der Apps wiesen zumindest eine Divergenz im Bereich der Ortsdaten (*location data*) auf.[153] Insgesamt zeigte sich, dass gerade Praktiken der Datenweiterleitung an *ad networks/exchanges* vielfach nicht oder nur unzureichend in der Datenschutzerklärung ausgewiesen werden.[154] Das Modell wurde bereits von der US-amerikanischen Aufsichtsbehörde (FTC) zur Unterstützung ihrer Aufgaben im Bereich der Durchsetzung des Datenschutzrechts getestet.[155]

Erhebliche Compliance-Defizite ergeben sich nicht nur im Bereich der Smartphone Apps, sondern auch der klassischen Webseiten. Eine Untersuchung zeigte, dass signifikante Divergenzen zwischen Datenschutzerklärungen von Webseiten und tatsächlicher Datenverarbeitung durch diese im Bereich

[146] *Zimmeck et al.*, Proceedings on Privacy Enhancing Technologies 2019 (3), 66; Vorstudie in *Zimmeck et al.*, Network and Distributed System Security Symposium 2017, 1; eine ähnliches, aber bislang weniger leistungsstarkes Modell wurde entwickelt von *Austin et al.*, Towards Dynamic Transparency: The AppTrans (Transparency for Android Applications) Project, Working Paper, 2018, https://ssrn.com/abstract=3203601.

[147] *Zimmeck et al.*, Proceedings on Privacy Enhancing Technologies 2019 (3), 66 (70 ff.).

[148] *Zimmeck et al.*, Proceedings on Privacy Enhancing Technologies 2019 (3), 66 (69).

[149] *Zimmeck et al.*, Proceedings on Privacy Enhancing Technologies 2019 (3), 66 (72–74, 80).

[150] *Zimmeck et al.*, Proceedings on Privacy Enhancing Technologies 2019 (3), 66 (74 f.): 49,1 %.

[151] *Zimmeck et al.*, Proceedings on Privacy Enhancing Technologies 2019 (3), 66 (75).

[152] *Zimmeck et al.*, Proceedings on Privacy Enhancing Technologies 2019 (3), 66 (76).

[153] *Zimmeck et al.*, Proceedings on Privacy Enhancing Technologies 2019 (3), 66 (77).

[154] *Zimmeck et al.*, Proceedings on Privacy Enhancing Technologies 2019 (3), 66 (77).

[155] *Zimmeck et al.*, Proceedings on Privacy Enhancing Technologies 2019 (3), 66 (80).

des *third-party tracking* bestehen.[156] Die Analyse von 200.000 Webseiten und ihren korrespondierenden Datenschutzerklärungen ergab, dass weniger als 15 % der Datenströme an Drittanbieter offengelegt werden.[157] Auch dies ist, als wahrscheinliche Verletzung des Datenschutzrechts, für Aufsichtsbehörden von erheblichem Interesse. Weitere Anwendungen (*static flow analysis techniques*), z. B. DroidSafe,[158] ermöglichen es schließlich, Datenströme von Smartphone Applikationen live zu überwachen und so die Weitergabe von sensitiven oder nicht von der Einwilligung umfassten Informationen sichtbar zu machen.[159]

b) Automatisierte Kontrolle der Nutzungsbedingungen

Nutzungsbedingungen können, wie gesehen, ebenfalls einen erheblichen Einfluss auf die Datenverarbeitung nehmen, da in ihnen die Grundlage für eine Datenverarbeitung nach Art. 6 Abs. 1 lit. b DS-GVO gelegt werden kann. Insofern sind die Bemühungen von Interesse, nicht nur Datenschutzerklärungen, sondern zunehmend auch Nutzungsbedingungen automatisiert zu untersuchen. Das bereits erwähnte, am EUI entwickelte Modell CLAUDETTE wurde ursprünglich konzipiert und eingesetzt, um die substantielle Angemessenheit von AGB mithilfe von Techniken maschinellen Lernens zu überprüfen.[160] Das Trainingskorpus basierte auf 50 Verträgen, die von Experten annotiert wurden.[161] Darauf wurden verschiedene Klassifizierungsmodelle trainiert, die mit guter Genauigkeit bestimmte Typen unangemessener Klauseln erkennen können.[162] Für hiesige Zwecke besonders interessant ist die durch CLAUDETTE ermöglichte Identifizierung und Bewertung von Klauseln, nach denen ein Vertrag zwischen dem Anbieter und dem Nutzer bereits durch jedwede Nutzung des Produkts zustande kommen soll.[163] Wie im fünften Kapitel der Arbeit gesehen, widerspricht dies jedenfalls dann, wenn der Vertrag Grundlage einer Datenverarbeitung sein soll, den durch das Kriterium der Unmissverständlichkeit geprägten Anforderungen an den Vertragsabschlusstatbestand.[164] Bei dieser Klauselkategorie erzielt CLAUDETTE sogar besonders hohe Performancewerte.[165] Das Modell wurde mittlerweile auf einem Webserver für Anfragen

[156] *Libert*, Proceedings of the 2018 World Wide Web Conference, 207.
[157] *Libert*, Proceedings of the 2018 World Wide Web Conference, 207 (212): 14,8 %.
[158] *Gordon et al.*, Network and Distributed System Security (NDSS) Symposium 2015, 110.
[159] Überblick und Vergleich bei *Qiu/Wang/Rubin*, Proceedings of the 27th ACM SIGSOFT International Symposium on Software Testing and Analysis 2018, 176.
[160] *Lippi et al.*, Automated Detection of Unfair Clauses in Online Consumer Contracts, Legal Knowledge and Information Systems (JURIX) 2017, 145; *Lippi et al.*, 27 Artificial Intelligence and Law 2019, 117.
[161] *Lippi et al.*, 27 Artificial Intelligence and Law 2019, 117 (121 ff.).
[162] *Lippi et al.*, 27 Artificial Intelligence and Law 2019, 117 (132): precision, recall und F1-Werte im Bereich von 80–85 %.
[163] *Lippi et al.*, 27 Artificial Intelligence and Law 2019, 117 (119).
[164] Siehe oben, § 5 B.III.2.b)aa)(b)(cc).
[165] *Lippi et al.*, 27 Artificial Intelligence and Law 2019, 117 (133).

durch Nutzer zur Verfügung gestellt.[166] Weitere Typen von AGB untersucht ein Team der TU München, das ebenfalls problematische Klauseln extrahieren, vereinfacht widergeben und automatisiert mithilfe einer *knowledge base* bewerten kann (Software Aided Analysis of Terms of Service: SaToS).[167] Dieses Modell wurde Verbraucherzentralen zur Verfügung gestellt und mit ihnen weiterentwickelt.[168]

2. *Rechtlicher Rahmen*

Der rechtliche Rahmen einer automatisierten Rechtmäßigkeitskontrolle kann hier nur skizziert werden. Im Grundsatz ist der Zugriff auf Dokumente wie Datenschutzerklärungen zu Analysezwecken zwar rechtlich unproblematisch, wenn diese von den Verantwortlichen veröffentlicht wurden. Sie sind ja gerade dazu bestimmt, die Öffentlichkeit, aber auch Aufsichtsbehörden und Informationsintermediäre zu informieren.[169] Der Umstand, dass die Analyse mithilfe von Techniken maschinellen Lernens erfolgt, darf jedenfalls aus rechtspolitischer Sicht nicht zu einer anderen Bewertung der Rechtmäßigkeit führen. Insofern gilt jedenfalls im Grundsatz: „the right to read is the right to mine".[170]

Aus der Debatte um die rechtlichen Konsequenzen von Text und Data Mining ist jedoch bekannt, dass der Teufel hier häufig im Detail steckt. So ist denkbar, dass Verantwortliche in ihren AGB festhalten, dass die von ihnen publizierten Dokumente nicht mit maschinellen Mitteln untersucht werden dürfen. Nach hier vertretener Auffassung verstößt dies jedoch gegen § 307 Abs. 2 Nr. 1 BGB, da die Rechtmäßigkeitskontrolle gerade die Ziele des Datenschutzrechts befördert, die mit den Pflichtinformationen ebenfalls verfolgt werden. Unwahrscheinlich ist es hingegen, dass an den zu untersuchenden Dokumenten immaterialgüterrechtliche Schutzrechte (etwa ein Urheberrecht nach § 2 Abs. 1 Nr. 7 UrhG) bestehen, da die Materialien regelmäßig einen hohen Grad an Standardisierung aufweisen.[171] Sollte dem doch einmal anders sein, so müssen die Grenzen der Schranke für Text und Data Mining (§ 60d UrhG, Art. 3 f. DSM-Richtlinie[172]) beachtet werden. Hierzu existiert eine reiche Debatte im

---

[166] http://claudette.eui.eu/demo/.

[167] *Braun et al.*, Internationales Rechtsinformatik Symposium (IRIS) 2018, 627; *Braun et al.*, INFORMATIK 2019: 50 Jahre *Gesellschaft für Informatik* – Informatik für Gesellschaft 2019, 407.

[168] *Braun et al.*, INFORMATIK 2019: 50 Jahre *Gesellschaft für Informatik* – Informatik für Gesellschaft 2019, 407 (410).

[169] Siehe oben, § 4 B.I.5.b).

[170] *Murray-Rust/Molloy/Cabell*, in: Moore (Hrsg.), Issues in Open Research Data, 2014, 11 (27 f.); *Geiger/Frosio/Bulayenko*, The Exception for Text and Data Mining (TDM) in the Proposed Directive on Copyright in the Digital Single Market – Legal Aspects, Briefing for the JURI committee of the European Parliament, 2018, 21.

[171] Siehe nur BGH GRUR 1981, 352 (353) – Staatsexamensarbeit; GRUR 1986, 739 (740 f.) – Anwaltsschriftsatz; GRUR 1993, 34 (35) – Bedienungsanweisung.

[172] Richtlinie (EU) 2019/790 des Europäischen Parlaments und des Rates vom 17. April

Schrifttum,[173] die hier nicht vertieft werden kann und zu welcher der Verfasser andernorts Stellung genommen hat.[174]

Rechtlich besonders schwierig zu beurteilen sind Fälle, in denen Dokumente untersucht werden sollen, die bislang nicht vom Verantwortlichen freiwillig öffentlich gemacht wurden (Whistleblowing). Auch diese Fragestellung kann hier nicht abschließend behandelt werden. Allerdings bietet Art. 58 Abs. 1 lit. b DS-GVO eine Rechtsgrundlage für behördliche Datenschutzüberprüfungen, in deren Rahmen nach Art. 58 Abs. 1 lit. a DS-GVO auch die Vorlage von Dokumenten gefordert werden kann. Wenn Private Zugang zu Dokumenten begehren oder erlangen,[175] ist nunmehr zudem § 5 Nr. 2 GeschGehG zu beachten, wonach die Erlangung und Nutzung eines Geschäftsgeheimnisses nicht verboten ist, wenn dies zur Aufdeckung einer rechtswidrigen Handlung erfolgt, sofern dies geeignet ist, das allgemeine öffentliche Interesse zu schützen. Zwar dürfte bei Datenverarbeitungen, die eine Mehrzahl von Personen betreffen, regelmäßig ein öffentliches Interesse vorliegen.[176] Nichtsdestoweniger ist hier eine Verhältnismäßigkeitsprüfung erforderlich,[177] die selbstverständlich auch das Vorlageverlangen durch Behörden nach Art. 58 Abs. 1 lit. a DS-GVO begrenzt.

Damit lässt sich in der Summe festhalten, dass die automatisierte Analyse jedenfalls von durch den Verantwortlichen veröffentlichten Dokumenten regelmäßig nach geltender Rechtslage möglich ist. Vorsicht ist hingegen bei der Analyse von Dokumenten geboten, die ein Geschäftsgeheimnis darstellen können. Hier bleibt die Anwendung und Interpretation des neuen GeschGehG durch die Rechtsprechung abzuwarten.

3. Anreize und Beschränkungen

Die vorgestellten Techniken der automatisierten Rechtmäßigkeitskontrolle haben zweifelsohne erhebliches Potenzial. Allerdings darf man nicht übersehen, dass ihre Wirkung gegenwärtig noch starken außerrechtlichen Beschränkungen unterliegt.

2019 über das Urheberrecht und die verwandten Schutzrechte im digitalen Binnenmarkt, ABl. 2019 L 130/92.

[173] Siehe dazu etwa *de la Durantaye*, Allgemeine Bildungs- und Wissenschaftsschranke, 2014; *Ducato/Strowel*, IIC 2019, 649; *Raue*, ZUM 2019, 684; *Ory/Sorge*, NJW 2019, 710 (712 f.); *Obergfell*, in: Ahrens et al. (Hrsg.), Festschrift Büscher, 2018, 223.

[174] *Hacker*, in: Merkt *et al.*, Festschrift Hopt, 2020, 351 (361 ff.); siehe auch *Hacker*, A Legal Framework for AI Training Data, 13 Law, Innovation and Technology (im Erscheinen), https://ssrn.com/abstract=3556598.

[175] Bei einem Vorlageverlangen durch Behörden gilt das GeschGehG nicht, § 1 Abs. 2 GeschGehG, siehe auch *Alexander*, in: Köhler/Bornkamm/Feddersen, UWG, 38. Auflage 2020, § 1 GeschGehG Rn. 27–29.

[176] Vgl. *Ohly*, GRUR 2019, 441 (448); *Alexander*, in: Köhler/Bornkamm/Feddersen, UWG, 38. Auflage 2020, § 5 GeschGehG Rn. 40.

[177] Siehe dazu *Ohly*, GRUR 2019, 441 (448 f.); *Alexander*, in: Köhler/Bornkamm/Feddersen, UWG, 38. Auflage 2020, § 5 GeschGehG Rn. 43–45.

Erstens steckt ihre Entwicklung und Anwendung noch in den Kinderschuhen,[178] sodass einigen Produkten die Technikreife für einen gezielten Einsatz noch fehlt. Insbesondere wirkt sich hierbei aus, dass die Trainingsdaten bei einigen Anwendungen deutlich unter 100 Dokumente umfassen, sodass abzuwarten bleibt, wie die Modelle im Feld unter den sich ständig ändernden Bedingungen der digitalen Wirtschaft funktionieren werden.[179] Zwar sind erste Anwendungen vielversprechend, doch hinsichtlich der Übertragbarkeit dieser Ergebnisse auf neue Erscheinungsformen und Strukturen von datenschutzrechtlich erheblichen Veröffentlichungen sollte man zumindest vorsichtig sein.[180] Der Inhalt von Sätzen ist zudem häufig kontextabhängig, was eine besondere Herausforderung für die automatisierte Erfassung ihres semantischen Gehalts darstellt.[181] Gleiches gilt für die Mehrsprachigkeit der untersuchten Dokumente.[182] Modelle werden typischerweise (im Kontext der DS-GVO) zunächst für die englische Sprache entwickelt, sodass gerade für EU-Sprachen mit wenig Sprechern auch längerfristig Anwendungslücken bestehen bleiben können.[183]

Ein Hauptproblem dürfte zweitens darin liegen, dass technische Kontrollmechanismen jedenfalls unmittelbar keine zusätzlichen vertraglichen Optionen schaffen können, die insbesondere Nutzern mit stark ausgeprägten Datenschutzpräferenzen präferenzkonforme Austauschprozesse ermöglichen würden. Wer etwa die Nutzungsbedingungen und Datenschutzerklärung von Facebook mit Mitteln maschinellen Lernens überprüft, mag noch klarer als zuvor Kenntnisse der datenschutzrechtlichen und sonstigen rechtlichen Risiken vermittelt bekommen. Eine Alternative für die Nutzung von Facebook ohne signifikante Preisgabe von Nutzerdaten erhält er oder sie dadurch jedoch nicht. Technische Mechanismen der Rechtmäßigkeitskontrolle helfen daher die zur Verfügung stehenden Optionen auf diejenigen zu beschränken, die präferenzkonform sind, kreieren aber keine neuen Optionen.

Dies könnte, drittens, allenfalls dann gelingen, wenn durch die Nutzung entsprechender Instrumente hinreichender Marktdruck zum Angebot datenschutzfreundlicher Dienste gerade durch besonders marktstarke Anbieter aufgebaut würde. Allerdings sind die Modelle, auch soweit sie bereits gute Ergeb-

---

[178] *Lippi et al.*, 1 Nature Machine Intelligence 2019, 168 (168).

[179] Skeptisch insoweit *Micklitz et al.*, 40 Journal of Consumer Policy 2017, 367 (384); siehe auch Vogl, Roland (Hrsg.), Research Handbook on Big Data Law, im Erscheinen, https://ssrn.com/abstract=3347364,Teil4.2.

[180] *Gallé/Christofi/Elsahar*, Proceedings of the PAL: Privacy-Enhancing Artificial Intelligence and Language Technologies 2019, 21.

[181] *Liepina et al.*, Proceedings of the Third Workshop on Automated Semantic Analysis of Information in Legal Text (ASAIL 2019) 2019, Article 9, 4.

[182] *Liepina et al.*, Proceedings of the Third Workshop on Automated Semantic Analysis of Information in Legal Text (ASAIL 2019) 2019, Article 9, 5.

[183] Für eine Anwendung für deutsche Datenschutzerklärungen siehe https://datenschutz-scanner.de.

nisse liefern, noch wenig bekannt und werden noch seltener genutzt.[184] Ihre Anwendung beruht bislang vollständig auf der Eigeninitiative besonders sophistizierter oder interessierter Nutzer. Angesichts der hinsichtlich des Umgangs mit personenbezogenen Daten identifizierten Typen von Marktversagen, insbesondere rationaler Ignoranz und verhaltensökonomischer Effekte, darf man zumindest skeptisch sein, ob Selbsthilfemechanismen Breitenwirkung entfalten, solange Nutzer aktiv werden müssen, um sie einzusetzen.[185] Zwar werden die Kosten für eine Kenntnisnahme der wichtigsten Inhalte von Datenschutzerklärungen oder Nutzungsbedingungen durch automatisierte Analyseverfahren erheblich gesenkt; für viele Nutzer dürfte der Aufwand jedoch immer noch prohibitiv hoch sein. Ein Instrument zur Zusammenfassung von Datenschutzerklärungen (PrivacyCheck) ist zum Beispiel sogar als Browser-Erweiterung für Chrome verfügbar, wird jedoch über 18 Monate nach seiner Einführung bislang lediglich von gut 900 Nutzern weltweit eingesetzt.[186]

Denkbar ist immerhin, dass sich eine informierte Minderheit bildet, die groß genug ist, um marktdisziplinierend zu wirken; ob dies faktisch geschieht, ist jedoch gegenwärtig nicht abzusehen. Dafür müsste sich wohl ein *privacy assistant* durchsetzen, der unterschiedliche Analyse- und Bewertungsfunktionen in einer App oder Browser-Erweiterung vereint[187] und mit den vielfältigen Akteuren, welche die Datenverarbeitung in der digitalen Wirtschaft prägen, kompatibel ist.[188] Es verbleiben jedoch auch dann die bekannten Probleme der Einschätzung datenschutzrechtlicher Risiken durch die Nutzer;[189] präferenzkonforme Entscheidungen können jedoch durch Selbsthilfe-Mechanismen nur insoweit gestützt werden, als Präferenzen hinreichend klar und stabil geformt[190] und Entscheidungen hinreichend rational, unter Einbezug der Möglichkeit der Aggregation und sekundären Analyse von Daten, getroffen werden. Für den individuellen Nutzer dürften daher auf maschinellem Lernen basierende Analyseapplikationen zwar zu einer Verbesserung der Entscheidungsumgebung führen, die empirischen Probleme einer informierten und freien Entscheidung jedoch nicht vollständig lösen.

Eine deutlich größere Reichweite können die Modelle viertens freilich entwickeln, wenn sie durch Aufsichtsbehörden oder mit Klagebefugnis ausgestattete Rechtsdurchsetzungsinstitutionen wie Verbraucherverbände genutzt werden.[191] Wie oben gesehen, sind erste Kooperationen hier bereits angelaufen.

---

184 Vgl. *Braun et al.*, INFORMATIK 2019: 50 Jahre *Gesellschaft für Informatik* – Informatik für Gesellschaft 2019, 407 (410).

185 So auch *Solove*, 126 Harvard Law Review 2013, 1880 (1883 ff.).

186 https://chrome.google.com/webstore/detail/privacycheck/poobeppenopkcbjejfjenbiepifcbclg.

187 Siehe dazu noch ausführlich unten, § 6 C.I.3.a)bb).

188 Skeptisch insoweit *Solove*, 126 Harvard Law Review 2013, 1880 (1888 f., 1902).

189 *Solove*, 126 Harvard Law Review 2013, 1880 (1883 ff., 1889 f.).

190 Siehe dazu unten, § 6 C.II.2.b).

191 *Micklitz et al.*, 40 Journal of Consumer Policy 2017, 367 (372).

Sie lassen einen signifikanten Beitrag zur Durchsetzung des Datenschutz- und AGB-Rechts erhoffen.[192] Diese Applikationen sind auch deshalb dringend notwendig, weil die nutzerorientierten Instrumente lediglich die Spitze des Eisbergs erfassen, nämlich jene Verarbeitungen, die in Datenschutzerklärungen oder Nutzungsbedingungen offengelegt werden. Wie gesehen sind problematische Verarbeitungen jedoch darin häufig gar nicht enthalten.[193] Diese können lediglich durch die genannten durchsetzungsorientierten Instrumente aufgedeckt werden, welche nicht lediglich textbasierte Veröffentlichungen untersuchen, sondern auch den Code und die Wirkweise der angebotenen Anwendungen analysieren.

III. Zusammenfassung zur Minimierung von Datenschutzrisiken durch Technik

Die Minimierung von Datenschutzrisiken durch technische Applikationen ist ein aktives und stark expandierendes Forschungsgebiet. Auf Unternehmensseite haben diese Anstrengungen im Rahmen von *privacy by design* allerdings, trotz der nun in Art. 25 DS-GVO aufgenommenen Rechtspflicht, bislang noch keine durchschlagende Wirkung erzielen können.

Damit sind vermehrt die Nutzer selbst und Rechtsdurchsetzungsinstitutionen gefordert. Apps und Browser-Erweiterungen, welche die Nutzer selbst implementieren können (Selbstdatenschutz), sind zwar vorhanden und müssten von Anbietern auch regelmäßig toleriert oder, unter bestimmten Bedingungen, gar aktiv durch die Bereitstellung von Schnittstellen unterstützt werden. Sie werden aber insgesamt nur spärlich genutzt. Dies liegt aller Wahrscheinlichkeit nach an denselben Gründen, die auch für das Paradox der Privatheit verantwortlich zeichnen, etwa rationaler Ignoranz und verhaltensökonomischen Effekten. Wirkmächtig werden diese Instrumente erst dann, wenn sie als standardmäßige Voreinstellung in gängige Produkte eingebaut werden, wie dies zum Teil bei dem Firefox Browser der Fall ist. Auch die hier zur Verfügung gestellten und standardmäßig aktivierten Anti-Tracking-Tools können jedoch überwunden werden und erfassen längst nicht alle Formen der Nachverfolgung. Die nutzerorientierte Rechtmäßigkeitskontrolle durch Anwendungen maschinellen Lernens ist demgegenüber bislang noch stärker auf die nur beschränkt vorhandene Eigeninitiative von Nutzern angewiesen. Problematisch ist hier insbesondere auch, dass die Analyse von Datenschutzerklärungen und Nutzungsbedingungen regelmäßig nur die Spitze des Eisbergs erfasst, nämlich jene Datenverarbeitungen, die auch tatsächlich freiwillig offengelegt werden.

---

[192] *Lippi et al.*, 1 Nature Machine Intelligence 2019, 168 (168); *Micklitz et al.*, 40 Journal of Consumer Policy 2017, 367; Vogl, Roland (Hrsg.), Research Handbook on Big Data Law, im Erscheinen, https://ssrn.com/abstract=3347364,Teil4.1.

[193] Siehe oben, § 6, Fn. 150 ff.

Empirische Untersuchungen zeigen aber, dass gerade problematische und potenziell rechtswidrige Formen der Datenverarbeitung in den Erklärungen nicht zu finden sind.

Das vielleicht größte Potenzial besteht daher in der Nutzung automatisierter Analyseinstrumente durch Aufsichtsbehörden und mit Klagebefugnis ausgestattete Verbraucher- oder Wettbewerbsverbände. Angesichts beschränkter Ressourcen können hier besonders problematische Angebote schnell und skalierbar identifiziert werden. Der Durchsetzung des rechtlichen Rahmens für die digitale Wirtschaft ist dies allemal zuträglich. Code tritt damit als weitere Kontrollinstanz neben Nutzer, Behörden und Gerichte.

Allen in diesem Abschnitt diskutierten Anwendungen eignen jedoch zwei Nachteile. Erstens führen sie regelmäßig zu einer technischen Reaktion der Anbieter zur Umgehung der Schutz- und Analyseinstrumente, die in einen Rüstungswettbewerb mit sozialen Kosten münden. Zweitens tragen die genannten Instrumente zwar zu einer Verbesserung der Informationslage bei, sie können jedoch keine zusätzlichen vertraglichen Optionen kreieren, mit denen Nutzer, die stärker ausgeprägte Datenschutzpräferenzen haben, diese durchsetzen könnten. Dies weist auf die Notwendigkeit rechtlicher Unterstützung von technischen Strategien (dazu sogleich unter C.). Technologische Lösungen allein können die Souveränität der Nutzer über ihre Daten zwar erhöhen, aber nicht in jedem Fall auf ein zufriedenstellendes Niveau bringen.

C. Entscheidungsunterstützung durch Recht

Die technischen Ansätze, die Gegenstand der vorangegangenen Abschnitte waren, können die Souveränität der Nutzer über ihre Daten zwar stärken, aber nicht im Alleingang gewährleisten. Vielmehr haben die mannigfaltigen Limitationen technischer Schutz- und Kontrollinstrumente gezeigt, dass diese einer Verbindung mit neuen rechtlichen Strukturen bedürfen, um stärker als bislang eine Breitenwirkung zu entfalten. Der kommende Abschnitt der Arbeit konstruiert daher eine rechtlich grundierte Kontrollarchitektur, die auch Aufsichtsbehörden und Marktgestaltung in den Blick nimmt, aber zuvorderst der (Wieder-)Herstellung von materieller Privatautonomie als Zielsetzung verpflichtet ist.[194] Dabei soll zunächst exploriert werden, inwieweit das bislang zentrale Instrument privatautonomer Gestaltung im Bereich digitaler Austauschprozesse – die Einwilligung – verbessert und zu einem Instrument genereller Kommunikation von Datenschutzpräferenzen ausgebaut werden kann (I.). Da auch dadurch jedoch eine Durchsetzung von Datenschutzpräferenzen nicht immer in hinreichender Weise unterstützt werden kann, wird abschlie-

[194] Vgl. *Lynskey*, The Foundations of EU Data Protection Law, 2015, 257 f.; *Clifford/Ausloos*, 37 Yearbook of European Law 2018, 130 (145).

ßend vorgeschlagen, sektorspezifisch in defizitäre Marktstrukturen zu intervenieren durch ein Recht auf eine datenschonende Vertragsoption (II.).

I. Verbesserung der Einwilligung und der Präferenzkommunikation

Vorschläge zur Verbesserung des Einwilligungsregimes sind bereits in großer Zahl entwickelt worden.[195] Für die hiesigen Zwecke kann daher ein Überblick genügen, der aufzeigt, welche Möglichkeiten bestehen, die Einwilligung selbst bzw. die Pflichtinformationen, auf denen sie basiert, so zu gestalten, dass die in § 3 angesprochenen Typen von Marktversagen zumindest reduziert werden. Hier sind erstens transparenzbasierte rechtliche Strategien zur Verbesserung der Verständlichkeit von und Aufmerksamkeit gegenüber Datenschutzerklärungen zu diskutieren, die rationale Ignoranz und Informationsüberlastung verringern können (1.). Zweitens sollen kurz verhaltensbasierte Ansätze angesprochen werden (*privacy nudges*), mit denen unter anderem verhaltensökonomischen Effekten entgegengewirkt werden kann (2.). Schließlich werden die rechtlichen Rahmenbedingungen erörtert, die geschaffen werden müssen, damit technologiebasierte Ansätze wie personalisierte Mastereinwilligungen verwirklicht werden können (3.). Aus den Limitationen dieser Verbesserungsstrategien erwächst dann erst die Notwendigkeit einer umfassenderen Marktstrukturintervention (II.).

1. Transparenzbasierte Ansätze

In den vergangenen Abschnitten wurden bereits diverse Techniken vorgestellt, mit denen bestehende Datenschutzerklärungen und Nutzungsbedingungen analysiert und nutzerfreundlich aufbereitet werden können. Dies wäre allerdings dann nicht oder nur eingeschränkt notwendig, wenn derartige Transparenzstrategien bereits rechtlich vorgeschrieben wären und sinnvoll in den existierenden Datenschutzerklärungen implementiert würden. Darum soll es im Folgenden gehen: um die Verbesserung der Verständlichkeit der Datenschutzerklärungen selbst, nicht, wie in § 6 B., um deren technische Analyse oder Aufbereitung.

[195] Siehe nur *Solove*, 126 Harvard Law Review 2012, 1880; *Zuiderveen Borgesius*, Improving Privacy Protection in the Area of Behavioural Targeting, 2015, Kapitel 8; *Lynskey*, The Foundations of EU Data Protection Law, 2015, Kapitel 8; *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 357 ff.; *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 53 ff.; *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (451 ff.); *Waldman*, 21 Stanford Technology Law Review 2018, 129 (174 ff.); sowie die Nachweise in den folgenden Abschnitten.

a) Verbesserungsmöglichkeiten

Seit es Datenschutzerklärungen gibt, wird nach Wegen gesucht, diese transparenter zu gestalten. Maßgeblich sind hierbei zwei Kategorien: die kognitive Optimierung des Inhalts (aa)); und das Timing (bb)).

aa) Kognitive Optimierung des Inhalts

Kognitive Optimierung von Pflichtinformationen hat zum Ziel, Informationen so zu gestalten, dass ihre Verarbeitung möglichst wenig kognitive Ressourcen erfordert, zugleich aber ein hinreichender Informationsgehalt vermittelt wird. Gerade zu diesem Thema sind (auch durch den Verfasser[196]) bereits umfangreiche Studien veröffentlicht worden,[197] sodass einige Hinweise genügen mögen.

(1) Verständlichkeit der Sprache

Ein erster wichtiger Faktor ist die Verständlichkeit der Sprache.[198] Art. 12 Abs. 1 S. 1 DS-GVO schreibt bereits heute vor, dass datenschutzrechtliche Pflichtinformationen in einer verständlichen Form und in einer klaren und einfachen Sprache übermittelt werden müssen. Dies wird jedoch durch bestehende Datenschutzerklärungen bislang nur unzureichend umgesetzt. Eine 2017 veröffentlichte Studie von 50.000 Datenschutzerklärungen zeigt, dass deren Lesbarkeit nach Maßgabe verschiedener Lesbarkeitsmaße im Schnitt niedrig ist.[199] Während eine weitere Studie suggeriert, dass sich die visuelle Darstellung der Datenschutzerklärungen nach Geltungsbeginn der DS-GVO verbessert hat,[200] gilt dies nicht für die Lesbarkeit: Hier bestätigt eine nach Geltungsbeginn der DS-GVO an 300 Datenschutzerklärungen durchgeführte Analyse im Wesentlichen die Erkenntnisse der Arbeit von 2017 zur geringen Lesbarkeit.[201]

---

[196] *Hacker*, Verhaltensökonomik und Normativität, 2017, 444 ff.

[197] Siehe nur *Sunstein*, Memorandum for the Heads of Executive Departments and Agencies: Informing Consumers through Smart Disclosure, 2011; *Bar-Gill*, Seduction by Contract, 2012, 105 ff.; *Sunstein*, Simpler: The Future of Government, 2013; *Bar-Gill*, 11 Jerusalem Review of Legal Studies 2015, 75; *Federal Trade Commission*, Putting Disclosures to the Test: Staff Summary, 2016; *Policy and Research Group of the Office of the Privacy Commissioner of Canada*, Consent and privacy – A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act, 2016, 11 ff.; kritisch *Ben-Shahar/Schneider*, More Than You Wanted to Know, 2014, Kapitel 8.

[198] Siehe ausführlich *Schendera*, in: Lerch (Hrsg.), Die Sprache des Rechts, Bd. 1, 2004, 321; *Charrow/Charrow*, 79 Columbia Law Review 1979, 1306; *Hacker*, Verhaltensökonomik und Normativität, 2017, 461 ff.

[199] *Fabian/Ermakova/Lentz*, Proceedings of the International Conference on Web Intelligence 2017, 18.

[200] *Linden et al.* The privacy policy landscape after the GDPR, Working Paper, 2019, https://arxiv.org/abs/1809.08396, 6.

[201] *Becher/Benoliel*, in: Mathis/Tor (Hrsg.), Consumer Law & Economics, 2020, (im Escheinen).

Sicherlich ist die erhöhte Lesbarkeit von Datenschutzerklärungen weiterhin ein Desiderat,[202] schon deshalb, weil sie Informationsintermediären bei ihrer Analysearbeit hilft.[203] Allerdings zeigt eine weitere Studie, dass man von einer besseren sprachlichen Verständlichkeit nicht unbedingt eine Verbesserung der tatsächlichen Informationslage der Nutzer erwarten sollte.[204] Obwohl die Autoren der Studie verschiedene *best practices*, die von Datenschutzaufsichtsbehörden zur Erhöhung der Lesbarkeit empfohlen wurden, umsetzten,[205] zeigte sich fast kein Unterschied gegenüber den nicht verbesserten Datenschutzerklärungen: Die Nutzer verbrachten kaum mehr Zeit mit den Erklärungen und im Schnitt viel zu wenig, um sie auch nur ansatzweise zu erfassen.[206] Ferner verbesserte sich die Informationsaufnahme durch Nutzer nicht einmal in statistisch signifikanter Weise.[207] Eine technische Ausdrucksweise (konkret die Rede von „Cookies") kann sogar die Interaktion mit einem Hinweis auf Privatsphäreeinstellungen leicht erhöhen,[208] auch wenn Fachtermini grundsätzlich die Verständlichkeit[209] und die Bereitschaft zur Befassung mit den Informationen reduzieren.[210] Insgesamt zeigt sich damit, dass eine erhöhte Verständlichkeit der Sprache von Datenschutzerklärungen kaum zu einer informierten Entscheidung führt, da auch sprachlich einfachere Erklärungen in praktisch demselben Umfang wie komplexere ignoriert werden.

(2) Staffelung der Information auf mehreren Ebenen (*multi-layered notices*)

Ein zentrales Desiderat für die Verbesserung der Informiertheit der Einwilligung ist ferner seit einigen Jahren die Aufteilung der Datenschutzerklärung

---

[202] *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (455 f.); *Waldman*, 21 Stanford Technology Law Review 2018, 129 (176).

[203] Siehe oben, § 4 B.I.5.b).

[204] *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S41.

[205] Die verbesserten sechs Punkte waren: „*Titles.* Use clear titles and headers for the specific provisions. *Layered Information.* Provide a short-form summary for each provision, followed by the more comprehensive information. The long form should appear in smaller font and may even be posted elsewhere, but in such cases a clear reference or link to it must accompany the short-form summary. *Font.* Use easily readable type in a legible size and in a distinct color that contrasts distinctly with the background. *Literary Style.* Use active, not passive, language and short sentences with plain, straightforward language. *Examples.* When listing categories of personal information that is being collected or shared, give concrete examples, rather than ambiguous statements, of the type of information in each category. *Names.* If the notice refers to partner and affiliated companies, provide their names." (*Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S41 [S46]).

[206] *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S41 (S52): Durchschnitt 19 Sekunden, Median 6 Sekunden, bei einer geschätzten Lesedauer von mindestens 90 Sekunden.

[207] *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S41 (S54).

[208] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (10).

[209] *Charrow/Charrow*, 79 Columbia Law Review 1979, 1306 (1336); *Schendera*, in: Lerch (Hrsg.), Die Sprache des Rechts, Bd. 1, 2004, 321 (356).

[210] *Milne/Culnan*, 18 Journal of Interactive Marketing 2004, 15 (23 f.).

in mehrere, nach Komplexität gestaffelte Schichten: neben eine Basisaufklärung treten dann ausführliche Informationen in einem oder mehreren weiteren, verlinkten Dokument(en) (sog. Mehrebenen-Datenschutzerklärungen, *multilayered notices*).[211] Eine derartige Aufteilung von Pflichtinformationen in eine kurze Zusammenfassung und ausführlichere Hintergrundinformationen soll heterogene Adressatenkreise selektiv ansprechen[212] und wird auch in anderen Bereichen des Informationsmodells, etwa im Kapitalmarktrecht (*key investor document*),[213] mittlerweile gepflogen.

(a) Empirischer Nutzen

Die empirischen Ergebnisse zu gestuften Formaten der Informationsvermittlung sind gemischt,[214] jedoch in der Tendenz positiv. Zwar wird die komplexere Ebene durchaus nicht jedes Mal zurate gezogen, wenn die gesuchten Informationen in der Basisaufklärung nicht zu finden sind.[215] Auch führt eine gestufte Datenschutzerklärung nicht notwendig zu einer besseren Informa-

[211] *Hintze*, 76 Maryland Law Review 2017, 1044 (1083 f.); *Policy and Research Group of the Office of the Privacy Commissioner of Canada*, Consent and privacy – A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act, 2016, 12; *Kampert*, Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, 2016, 191 f.; *Schaub et al.*, Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 2015, 1 (5); *Cranor*, 10 Journal on Telecommunications & High Technology Law 2012, 273 (287); *Timpson/Troutman*, 4 International Journal of Mobile Marketing 2009, 57; *Menzel*,, DuD 2008, 400 (408); *Center for Information Policy Leadership*, Ten steps to develop a multilayered privacy notice, 2006; *Good et al.*, Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS) 2005, 43 (45); *Abrams/Crompton*, 2(1) Privacy Law Bulletin 2005, 1; *Center for Information Policy Leadership*, Multi-Layered Notices Explained, First Data Privacy Subgroup Meeting, 2005; *Article 29 Data Protection Working Party*, Opinion 10/2004 on More Harmonised Information Provisions, WP 100, 2004, 8 f.; Entschließung der 25. Internationalen Konferenz der Datenschutzbeauftragten, Sydney, 2003, zur Verbesserung der Bekanntmachung der Praktiken zum Datenschutz, in: LDA/BBDI, Dokumente zu Datenschutz und Informationsfreiheit 2003, 2004, 91.

[212] *Hacker*, Verhaltensökonomik und Normativität, 2017, 457.

[213] Art. 78 der Richtlinie 2009/65/EG des Europäischen Parlaments und des Rates vom 13. Juli 2009 zur Koordinierung der Rechts- und Verwaltungsvorschriften betreffend bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (OGAW), ABl. 2009 L 302/32; Art. 7 der Verordnung (EU) 2017/1129 des Europäischen Parlaments und des Rates vom 14. Juni 2017 über den Prospekt, der beim öffentlichen Angebot von Wertpapieren oder bei deren Zulassung zum Handel an einem geregelten Markt zu veröffentlichen ist und zur Aufhebung der Richtlinie 2003/71/EG, ABl. 2017 L 168/12; Art. 5 ff. der Verordnung (EU) Nr. 1286/2014 des Europäischen Parlaments und des Rates vom 26. November 2014 über Basisinformationsblätter für verpackte Anlageprodukte für Kleinanleger und Versicherungsanlageprodukte (PRIIP), ABl. 2014 L 352/1, § 64 Abs. 2 WpHG.

[214] Überblick bei *Hacker*, Verhaltensökonomik und Normativität, 2017, 454 ff.

[215] *Kelley et al.*, Proceedings of the 28th International Conference on Human Factors in Computing Systems 2010, 1573 (1579); *McDonald et al.*, Proceedings of the 9th Symposium on Usable Privacy and Security 2009, 37 (43, 50).

tionsvermittlung[216] oder einem sorgsameren Umgang mit sensitiven Informationen,[217] was jedoch hauptsächlich daran liegen dürfte, dass auch auf mehreren Ebenen gestufte Informationen nicht zu einer höheren Motivation führen, die Datenschutzerklärungen überhaupt sinnvoll zur Kenntnis zu nehmen.[218] Grundsätzlich bevorzugen Nutzer jedoch gestufte Formate gegenüber ungestuftem Fließtext[219] und brauchen weniger Zeit, um darin korrekte Antworten zu finden.[220] Hierarchisch strukturierte Information kann auch besser memorisiert werden[221] und führt daher tendenziell zu geringerer Informationsüberlastung.[222]

Insgesamt sollte man die empirische Wirksamkeit von gestuften Formaten der Datenschutzerklärung jedoch nicht überbewerten. Die Informationsvermittlung wird nicht unbedingt verbessert und auch in einer Studie mit Cookie Banners führte ein Link auf weiterführende Informationen nicht zu einer größeren Interaktion der Nutzer mit dem Hinweis.[223] Für die Abstufung spricht daher vor allem, dass solche Nutzer, die ohnehin motiviert sind, bestimmte Informationen ausfindig zu machen, dies in der Regel schneller erledigen können als bei einem einzigen Fließtextdokument. Zumindest eine Studie weist jedoch darauf hin, dass sich mit einem standardisierten Tabellenformat, in dem die Durchführung oder Nichtdurchführung bestimmter Verarbeitungen farblich kodiert wird (*privacy nutrition label*), noch bessere Ergebnisse erzielen ließen als mit einer gestuften Datenschutzerklärung.[224] Angesichts der Vielzahl der möglichen Verarbeitungsformen ist jedoch die Ausarbeitung eines standardisierten Tabellenformats für Datenschutzerklärungen bislang nicht gelungen.[225] Daher ist, trotz der gemischten empirischen Resultate, der Einsatz von gestuften Datenschutzerklärungen grundsätzlich wünschenswert.

---

[216] *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S41 (S54); *Kelley et al.*, Proceedings of the 28th International Conference on Human Factors in Computing Systems 2010, 1573 (1577); *McDonald et al.*, Proceedings of the 9th Symposium on Usable Privacy and Security 2009, 37 (50); für gekürzte Datenschutzerklärungen *Gluck et al.*, Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016, 321.

[217] *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S41 (S56).

[218] *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S41 (S52).

[219] *Kelley et al.*, Proceedings of the 28th International Conference on Human Factors in Computing Systems 2010, 1573 (1580).

[220] *Kelley et al.*, Proceedings of the 28th International Conference on Human Factors in Computing Systems 2010, 1573 (1580); *McDonald et al.*, Proceedings of the 9th Symposium on Usable Privacy and Security 2009, 37 (49f.); so auch, zum vereinfachten Kapitalmarktprospekt, *Beshears et al.*, in: Wise (Hrsg.), Explorations in the Economics of Aging, 2011, 75 (90).

[221] *Reed*, Cognition. Theory and Applications, 7. Aufl., 2006, 211–213.

[222] *Hacker*, Verhaltensökonomik und Normativität, 2017, 457.

[223] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (2).

[224] *Kelley et al.*, Proceedings of the 28th International Conference on Human Factors in Computing Systems 2010, 1573 (1580f.); vgl. auch *Kleimann Communication Group*, Know Before You Owe: Evolution of the Integrated TILA-RESPA Disclosures, 2012.

[225] Vgl. *Hacker*, Verhaltensökonomik und Normativität, 2017, 456.

Welche Informationen in die Basisinformationen aufgenommen werden sollten, wird damit zwar zentral,[226] lässt sich jedoch schwerlich allgemein beantworten.[227] Informationen zu den im zweiten Teil dieser Arbeit im Fokus stehenden drei Leitfällen – Datenweiterleitung an Dritte, Datenerhebung durch Dritte, Datenerhebung bei Dritten – sollten jedoch aufgrund ihrer besonderen Sensitivität und Relevanz für die datenschutzrechtlichen Risiken standardmäßig Teil der kurzen Basisaufklärung sein.

(b) Pflicht nach der DS-GVO?

Wenn gestufte Datenschutzerklärungen grundsätzlich aus Gründen der Verständlichkeit empfehlenswert sind, erhebt sich die Frage, ob bereits *de lege lata* eine Verpflichtung zu ihrer Nutzung besteht. Für das Regime der DSRL hatte die Artikel-29-Datenschutzgruppe bereits 2004 die Verwendung von gestuften Erklärungen angeregt und dargelegt, dass ihre Nutzung legal sei, wenn in der Summe auf allen Dokumenten jedenfalls die Pflichtinformationen abgebildet sind.[228] Dies wurde in der Stellungnahme zu Smartphone Apps noch einmal bestätigt.[229] Das LG Frankfurt a. M. verschärfte diese Hinweise in einem Urteil aus dem Jahr 2016 dahingehend, dass eine gestufte Darbietung nicht nur möglich, sondern für die Informiertheit der Einwilligung sogar notwendig ist, wenn der Nutzer andernfalls über 50 Bildschirmseiten auf einem Smart TV durchblättern müsste.[230]

Diese Einschätzung wird man situationsspezifisch auf die DS-GVO übertragen können. Art. 12 Abs. 1 S. 1 DS-GVO verlangt nunmehr die Übermittlung von Pflichtinformationen in „transparenter, verständlicher und leicht zugänglicher Form". Daraus dürfte bereits jetzt folgen, dass eine gestufte oder anderweitig optimierte Informationsvermittlung notwendig ist, wenn die

[226] *Schaub et al.*, Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 2015, 1 (5).

[227] Siehe den 39. Erwägungsgrund der DS-GVO sowie *Article 29 Data Protection Working Party*, Opinion 10/2004 on More Harmonised Information Provisions, WP 100, 2004, 8: „the identity of the controller and the purposes of processing – except when individuals are already aware – and any additional information which in view of the particular circumstances of the case must be provided beforehand to ensure a fair processing"; nunmehr *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 1, 2018, 22 Rn. 36: „Einzelheiten zu den Verarbeitungszwecken, die Identität des Verantwortlichen sowie eine Beschreibung der Rechte der betroffenen Person […] zusätzlich […] Angaben über die Verarbeitung, welche sich am stärksten auf die betroffene Person auswirkt, und die Verarbeitungsvorgänge, mit denen Letztere ggf. nicht gerechnet hat"; Ansätze für gestufte Produktinformationen bei *Hacker*, Verhaltensökonomik und Normativität, 2017, 466 ff.

[228] *Article 29 Data Protection Working Party*, Opinion 10/2004 on More Harmonised Information Provisions, WP 100, 2004, 8 f.

[229] *Article 29 Data Protection Working Party*, Opinion 02/2013 on apps on smart devices, WP 202, 2013, 23 f.

[230] LG Frankfurt a. M. ZD 2016, 494 (497) (zu § 4a BDSG aF); siehe auch BGH GRUR 2020, 891 Rn. 31–35.

Pflichtinformationen andernfalls einen Umfang annehmen würden, bei dem die Verständlichkeit erheblich leiden würde.[231] Wo hier die Grenze verläuft, muss jeweils im Einzelfall bestimmt werden. Allerdings wird man kaum sagen können, dass etwa eine Datenschutzerklärung, die fünf DIN A4-Seiten umfasst, nicht mehr transparent oder verständlich wäre. Insofern muss *de lege lata*, wie bereits bemerkt, nach herrschender Meinung auf den dem Durchschnittsverbraucher angenäherten Durchschnittsnutzer abgestellt werden,[232] für den mehrere Seiten Text nicht prinzipiell intransparent oder unverständlich sind.[233] Dieser Befund wird gestützt durch die Leitlinien der Artikel-29-Datenschutzgruppe zur Transparenz nach der DS-GVO, die Mehrebenen-Datenschutzerklärungen wie schon unter der DSRL lediglich empfehlen und für legal, nicht jedoch für notwendig erklären.[234] Demgegenüber ist nach hier vertretener Auffassung eine gestufte Datenschutzerklärung oder eine andere verständlichkeitsfördernde Übermittlungsmodalität (Tabellenformat, *privacy nutrition label*) bei Überschreitung der soeben angesprochenen, einzelfallabhängigen Grenze bereits jetzt zwingend notwendig.[235] Nur so lässt sich das in Art. 12–14 DS-GVO angelegte Spannungsverhältnis von Vollständigkeit und Verständlichkeit bei größeren Datenschutzerklärungen sinnvoll auflösen.[236]

Noch weitergehend ergibt sich aus der tendenziell positiven empirischen Wirkung eines Mehrebenenformats auf die Verständlichkeit, dass Art. 12 Abs. 1 DS-GVO *de lege ferenda* dahingehend abgeändert werden sollte, dass Datenschutzerklärungen, welche die Länge einer DIN A4-Seite (500 Wörter) überschreiten, zwingend eine Zusammenfassung der wesentlichen Punkte[237] auf einer DIN A4-Seite bieten müssen (sog. One-Pager).[238] Dabei könnte sich der Verantwortliche auch eines Tabellenformats (*privacy nutrition label*)[239] oder

---

[231] Vgl. *Dix*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 12 DS-GVO Rn. 20.

[232] Siehe oben, § 4, Fn. 490.

[233] Vgl. *Bäcker*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 12 DS-GVO Rn. 12: Verletzung von Art. 12 Abs. 1 S. 1 DS-GVO erst bei „grob […] unverständlichen Informationen".

[234] *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 1, 2018, 22 f.

[235] Ähnlich *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 DS-GVO Rn. 60; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 74.

[236] *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 74; vgl. auch *Bäcker*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 12 DS-GVO Rn. 12; *Franck*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 12 DS-GVO Rn. 23.

[237] Vgl. dazu den 39. Erwägungsgrund der DS-GVO.

[238] So bereits die *Fokusgruppe Verbrauchersouveränität und Transparenz*, Nationaler IT-Gipfel 2015, One-Pager Datenschutzhinweise, 2015; für die Darstellung von AGB und Datenschutzvorgaben, Sachverständigenrat für Verbraucherfragen, Verbraucherrecht 2.0, 2016, 46 f.; *Micklitz*, VuR 2017, 43 (44).

[239] Siehe *Cranor*, 10 Journal on Telecommunications & High Technology Law 2012, 273

Icons (dazu sogleich) bedienen.[240] Die Verbesserungen sind jedoch auch beim One-Pager nur inkrementell: Eine Studie ergab, dass er zwar häufiger wahrgenommen wird als traditionelle Datenschutzerklärungen, die Informiertheit der betroffenen Personen jedoch nur geringfügig anstieg.[241]

(3) Icons

Dass die DS-GVO, anders als noch die DSRL, die Verständlichkeit und Gestaltung der Pflichtinformationen selbst in den Blick nimmt, zeigt insbesondere die Regelung zu standardisierten Bildsymbolen (Icons) in Art. 12 Abs. 7 und 8 DS-GVO. Danach können die nach Art. 13 und 14 DS-GVO erforderlichen Pflichtinformationen in Kombination mit Icons bereitgestellt werden, Art. 12 Abs. 7 S. 1 DS-GVO. Ihre Nutzung ist daher rein fakultativ, in elektronischer Form müssen sie jedoch maschinenlesbar sein, Art. 12 Abs. 7 S. 2 DS-GVO. Die Kommission kann Durchführungsrechtsakte erlassen zu den Informationen, die durch Icons dargestellt werden, sowie zu dem Verfahren ihrer Bereitstellung, Art. 12 Abs. 8 DS-GVO. Derartige Rechtsetzung wurde jedoch zur Zeit der Abfassung dieser Arbeit noch nicht in Angriff genommen. Auch eine nach Art. 70 Abs. 1 lit. r DS-GVO mögliche Stellungnahme des europäischen Datenschutzausschusses lag noch nicht vor.

Icons können eine durchaus sinnvolle Ergänzung des Informationsregimes darstellen.[242] In den Passagen der DS-GVO, die sich damit beschäftigen, sind sie als Teil der Pflichtinformationen konzipiert, die *vor* einer Datenverarbeitung übermittelt werden müssen. Gedacht ist daher vor allem an ihre Integration in die Datenschutzerklärung, bei einer mehrstufigen Erklärung dann konsequenterweise auch auf der ersten Ebene.

---

(288); *Kleimann Communication Group*, Know Before You Owe: Evolution of the Integrated TILA-RESPA Disclosures, 2012.

[240] *Pinnick*, Privacy Short Notice Design, TrustArc Blog (17.2.2011), https://www.trustarc.com/blog/2011/02/17/privacy-short-notice-design/.

[241] *ConPolicy*, Wege zur besseren Informiertheit im Datenschutz, 2018, 2, 48, 51.

[242] *Holtz/Nocun/Hansen*, IFIP PrimeLife International Summer School on Privacy and Identity Management for Life, 2011, 338; *Pinnick*, Privacy Short Notice Design, TrustArc Blog (17.2.2011), https://www.trustarc.com/blog/2011/02/17/privacy-short-notice-design/; *Cranor*, 10 Journal on Telecommunications & High Technology Law 2012, 273 (293 f.); *Policy and Research Group of the Office of the Privacy Commissioner of Canada*, Consent and privacy – A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act, 2016, 12; *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (415); *Hacker*, Verhaltensökonomik und Normativität, 2017, 451 ff., besonders 464 f.; *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (455); *Efroni et al.*, 5 European Data Protection Law Review 2019, 352 (358 ff.); *Reidenberg et al.*, 96 Washington University Law Review 2019, 1409 (1422 ff.); *Dix*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 12 DS-GVO Rn. 38; *Metzger*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen), unter III.2.; für den urheberrechtlichen Bereich ausführlich *Specht*, Diktat der Technik, 2019, 416 ff.

Grundsätzlich können Icons jedoch in unterschiedlicher Form angezeigt werden: einmalig vor der Datenverarbeitung, oder auch periodisch oder persistent während derselben auf dem Gerät des Nutzers.[243] Diese Verwendungsarten von Icons haben gänzlich verschiedene Funktionen. Icons in einer Datenschutzerklärung versuchen deren Inhalt schnell verständlich zu machen. Sie sollen so die Informiertheit der Einwilligung stärken und zu einem effektiveren Wettbewerb der Anbieter um Bedingungen der Datenverarbeitung führen.[244] Periodische oder persistente Icons hingegen können dem Nutzer in einer konkreten Situation schnell vor Augen führen, welche Daten gesammelt werden. Bekannt sind etwa Symbole auf dem Bildschirm von Smartphones, die anzeigen, dass eine Lokalisierung mittels GPS-Daten erfolgt.[245] Dauerhaft eingeblendete Icons unterliegen jedoch grundsätzlich einem rapiden Wahrnehmungsschwund (*wear out*).[246]

Damit Icons, gleich ob einmalig, periodisch oder persistent, zu einer Verbesserung der Informationslage und damit zu präferenzkonformen Entscheidungen beitragen können, ist jedoch ein Umstand entscheidend, der gegenwärtig noch nicht hinreichend gewährleistet wird: Icons müssen zumindest EU-weit standardisiert werden,[247] damit sie nicht nur von den Anbietern rechtssicher verwendet, sondern von den Nutzern auch einfach wiedererkannt werden.[248] Die Kommission sollte daher zügig ihre delegierte Rechtsetzungsbefugnis wahrnehmen, allerdings erst nach einer empirischen Evaluierung des nutzerfreundlichsten Designs der Icons.[249] Erste Ansätze hierfür bestehen be-

[243] *Schaub et al.*, Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 2015, 1 (5).

[244] *Efroni et al.*, 5 European Data Protection Law Review 2019, 352 (359); *Franck*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 12 DS-GVO Rn. 46.

[245] *Federal Trade Commission*, Mobile Privacy Disclosures, 2013, 17 f.

[246] *Schaub et al.*, Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 2015, 1 (7); vgl. auch *Calo*, 87 Notre Dame Law Review 2012, 1027 (1030 f.); *Efroni et al.*, 5 European Data Protection Law Review 2019, 352 (359); allgemein zum *wear out* bei häufig wahrgenommenen Informationen *Hacker*, Verhaltensökonomik und Normativität, 2017, 612 f.

[247] Zu Vorschlägen für die Gestaltung von Icons, siehe *Pinnick*, Privacy Short Notice Design, TrustArc Blog (17.2.2011), https://www.trustarc.com/blog/2011/02/17/privacy-short-notice-design/; *Cranor*, 10 Journal on Telecommunications & High Technology Law 2012, 273 (293 ff.); ferner die Übersicht bei *ConPolicy*, Wege zur besseren Informiertheit im Datenschutz, 2018, 63–66; weiterhin *Efroni et al.*, 5 European Data Protection Law Review 2019, 352.

[248] *Auer-Reindsorff*, MMR 2019, 209 (209 f.); *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (455); *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 1, 2018, 30.

[249] Zur Notwendigkeit empirischer Tests *Federal Trade Commission*, Mobile Privacy Disclosures, 2013, 18; *Dimitropoulos/Hacker*, 25 Journal of Law and Policy 2017, 473 (besonders 528 ff.); *Hacker*, Verhaltensökonomik und Normativität, 2017, 927; *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 1, 2018, 30; *Efroni et al.*, 5 European Data Protection Law Review 2019, 352 (359 f.); *Waldman*, 21 Stanford Technology Law Review 2018, 129 (181); siehe etwa das umfangreiche *pre-*

reits,[250] sie ergeben jedoch noch kein einheitliches Bild hinsichtlich der Wirksamkeit,[251] die insgesamt überschaubar ist.[252]

Problematisch ist ferner, dass sich die Rechtsetzungskompetenz der Kommission nach dem Wortlaut von Art. 12 Abs. 8 DS-GVO lediglich auf die darzustellenden Informationen und das Verfahren der Bereitstellung, nicht jedoch auf die Gestaltung der Icons selbst erstreckt.[253] Man wird hier jedoch eine Annexkompetenz der Kommission annehmen können, da sowohl in Abs. 7 als auch Abs. 8 jeweils von „standardisierten" Bildsymbolen die Rede ist, außer der Kommission jedoch bei jetzigem Regelungsstand keine Institution zur Standardisierung infrage kommt.[254] Die Rechtsetzungsbefugnis der Kommission erstreckt sich allerdings bei systematischer Auslegung jedenfalls nur auf einmalige Icons zur Ergänzung der Pflichtinformationen, also vor der Datenverarbeitung. Für andere Icons muss daher der EU-Gesetzgeber noch tätig werden, wenn auch diese vereinheitlicht werden sollen.

bb) Timing: Kontextualisierung und Zeitabhängigkeit

Eine weitere Verbesserung der Informiertheit von Einwilligungen lässt sich möglicherweise dadurch erzielen, dass diese nicht lediglich einmal zu Beginn eines Nutzungsverhältnisses, sondern jeweils in der Verarbeitungssituation für einen ganz konkreten Anlass oder Kontext erteilt werden (sog. Just-in-time-Hinweise, *just-in-time notices*).[255] Dabei kann sowohl ein bloßer Hinweis seitens des Verarbeiters erfolgen[256] oder aber eine situationsspezifische Einwil-

testing bei *Kleimann Communication Group*, Know Before You Owe: Evolution of the Integrated TILA-RESPA Disclosures, 2012.

[250] *Fischer-Hübner/Wästlund/Zwingelberg*, UI prototypes: Policy administration and presentation, Version 1, Deliverable D4. 3.1 of the EC FP7 project PrimeLife, 2009; *Holtz/Nocun/Hansen*, IFIP PrimeLife International Summer School on Privacy and Identity Management for Life, 2010, 338; *Gluck et al.*, Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016, 321.

[251] *ConPolicy*, Wege zur besseren Informiertheit im Datenschutz, 2018, 69 f.

[252] *ConPolicy*, Wege zur besseren Informiertheit im Datenschutz, 2018, 71.

[253] *Pohle/Spittka*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 12 DS-GVO Rn. 29; *Bäcker*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 12 DS-GVO Rn. 24; *Dix*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 12 DS-GVO Rn. 41.

[254] Wie hier *Pollmann/Kipker*, DuD 2016, 378 (381); *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 1, 2018, 30; wohl auch *Heckmann/Paschke*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 12 Rn. 57; für einen weiteren Anwendungsbereich von Art. 12 Abs. 8 DS-GVO auch *Efroni et al.*, 5 European Data Protection Law Review 2019, 352 (360).

[255] Grundlegend *Patrick/Kenny*, in: Dingledine (Hrsg.), Privacy Enhancing Technologies, 2003, 107; siehe ferner *Schaub et al.*, Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 2015, 1 (5–7); *Federal Trade Commission*, Mobile Privacy Disclosures, 2013, 15 f.; *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 1, 2018, 24.

[256] *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 1, 2018, 24.

ligung von der betroffenen Person abgegeben werden.[257] Eine Einwilligung kann zum Beispiel gerade zu dem Zeitpunkt abgefragt werden, zu dem Daten tatsächlich in einer bestimmten, sensitiven Weise verarbeitet werden sollen.[258] Damit lässt sich die Informationsvermittlung signifikant verbessern.[259] So kann etwa die Frage nach einer Berechtigung der Verwendung von Lokalisierungsdaten für lokalisierungsbasierte Werbung unmittelbar in der Situation, in welcher die Werbung geschaltet werden soll, erfolgen.[260]

Problematisch erscheint hieran jedoch, dass dies zwar das Bewusstsein für spezifische Datenverarbeitungsvorgänge erhöht und Kontrollmöglichkeiten schafft, zugleich aber die Nutzer einer irritierenden und ressourcenintensiven Flut von Einwilligungen in ihrem Alltag ausgesetzt sind. Angesichts des Umstandes, dass die Mehrzahl der Nutzer nicht einmal willens ist, auch nur einmal zu Beginn eines Nutzungsverhältnisses Datenschutzerklärungen zur Kenntnis zu nehmen, dürfte die Erhöhung der Frequenz von Einwilligungsnotwendigkeiten der Präferenz der meisten Nutzer zuwiderlaufen. Der gleiche Vorbehalt begegnet Vorschlägen, Einwilligungen in festen Zeitabständen periodisch einzuholen.[261]

Möglich und begrüßenswert wäre einerseits, Just-in-time-Hinweise und Einwilligungen obligatorisch für besonders sensitive oder intrusive Verarbeitungssituationen zu etablieren, etwa für Datenverlagerungen ins EU-Ausland oder für Tracking durch Drittanbieter (*third-party tracking*). Ferner sollte es möglich sein, dass Nutzer die Möglichkeit erhalten, generell derartige Hinweise zu erhalten – so sie denn wollen (Opt-In). Dies würde es denjenigen Nutzern, die gering ausgeprägte Datenschutzpräferenzen haben, ermöglichen, von hochfrequenten Hinweisen und der Notwendigkeit wiederholter Einwilligungen verschont zu bleiben. Diejenigen Nutzer, welche stark ausgeprägte Datenschutzpräferenzen haben, könnten hingegen Just-in-time-Hinweise und -Einwilligungen zur Regel machen und so eine stärkere Kontrolle über ihre Daten ausüben.

b) Bewertung

Transparenz und Verständlichkeit der Datenschutzerklärung sind essenziell, wenn eine residuale Chance auf eine informierte Entscheidung wenigstens einer Minderheit der Nutzer bestehen soll. Dies hat auch der europäische Ge-

[257] Vgl. *Acquisti*, 50(3) ACM Computing Surveys (CSUR) 2017, Article 44, 24.

[258] Siehe *Balebako et al.*, Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices 2015, 63.

[259] *Balebako et al.*, Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices 2015, 63 (72); *Acquisti*, 50(3) ACM Computing Surveys (CSUR) 2017, Article 44, 24 f.

[260] *Rosner/Kenneally*, Clearly Opaque. Privacy Risks of the Internet of Things, Bericht, 2018, 109.

[261] Zu diesem Vorschlag etwa *Schaub et al.*, Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 2015, 1 (7).

setzgeber erkannt, der in Art. 12 DS-GVO nunmehr detaillierte Vorgaben für die Gestaltung der Datenschutzerklärung macht. Die soeben besprochenen Techniken, von verständlicher Sprache über Mehrebenen-Datenschutzerklärungen, One-Pager und Icons bis hin zu Just-in-time-Hinweisen, hat gezeigt, dass transparenzbasierte Ansätze durchaus bislang noch nicht ausgeschöpfte Möglichkeiten der Steigerung der Verständlichkeit von datenschutzbezogenen Pflichtinformationen bereithalten.

Nichtsdestoweniger zeigen die bislang empirisch getesteten Formate auch die Grenzen dieses Ansatzes auf. Weder durch ein Mehrebenenformat, verständliche Sprache oder One-Pager ließ sich die Zahl derer, die sich mit Datenschutzerklärungen beschäftigen, oder die Informationsvermittlung signifikant erhöhen. Nicht einmal drastische, hervorgehoben platzierte Warnhinweise hatten einen nennenswerten Effekt.[262] Dies legt den Schluss nahe, dass informierte Entscheidungen über datenschutzrechtlich relevante Aspekte von datenbasierten Austauschprozessen auch bei Ausschöpfung der dargestellten, transparenzorientierten Mittel immer einer kleinen Minderheit vorbehalten bleiben werden.[263] Ob diese Minderheit dereinst groß genug wird, um marktdisziplinierend zu wirken, wie es ökonomische Modelle zur *informed minority* vorsehen,[264] ist jedoch zu bezweifeln. Denn neben einem signifikanten Anstieg der informierten Nutzer gegenüber dem gegenwärtigen Niveau[265] setzt der Disziplinierungseffekt voraus, dass Anbieter nicht zwischen informierten und weniger informierten Nutzern unterscheiden können.[266] Gerade diese Differenzierung ist jedoch durch den Einsatz maschinellen Lernens immer einfacher möglich.[267]

Transparenzbasierte Ansätze behalten daher zwar durchaus ihre Berechtigung, da sie für diejenigen, denen die Durchsetzung ihrer grundrechtlich geschützten Datenschutzpräferenzen ein Anliegen ist, die Informationskosten erheblich senkt. Zudem profitieren auch Intermediäre, welche die Informationen aus Datenschutzerklärungen für weitere Nutzer aufbereiten. Schließlich stellt die in der DS-GVO zum Teil vorgeschriebene Maschinenlesbarkeit der Pflichtinformationen eine erhebliche Erleichterung für die Entwicklung von technologischen Analysewerkzeugen dar,[268] die weiter oben behandelt wurden.[269] Zugleich müssen transparenzbasierte Ansätze jedoch gekoppelt werden mit weiteren Strategien, damit die Erfüllung der materiellen Voraussetzungen für

---

[262] *Ben-Shahar/Chilton*, 45 Journal of Legal Studies 2016, S41 (S64 f.).
[263] Vgl. *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 35 f.
[264] *Schwartz/Wilde*, 127 University of Pennsylvania Law Review 1979, 630 (637 f.).
[265] *Bakos/Marotta-Wurgler/Trossen*, 43 The Journal of Legal Studies 2014, 1 (3).
[266] *Schwartz/Wilde*, 127 University of Pennsylvania Law Review 1979, 630 (638).
[267] Siehe bereits die Diskussion oben, bei § 3, Fn. 82.
[268] *Schaub et al.*, Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 2015, 1 (10).
[269] Siehe oben, § 6 B.

die wirksame Ausübung von Privatautonomie im digitalen Austauschbereich nicht die Ausnahme bleibt.

2. *Verhaltensbasierte Ansätze:* privacy nudges

Im Gefolge der zunehmenden Rezeption der Verhaltenswissenschaften, insbesondere der Verhaltensökonomik,[270] für regulatorische Zwecke[271] sind für eine Effektivierung des Datenschutzes in den vergangenen Jahren verstärkt *privacy nudges* diskutiert worden.[272] Im Rahmen dieser regulatorischen Technik wird versucht, verhaltensbezogenes Wissen fruchtbar zu machen, um eine Lenkungswirkung hin zu datenschutzfreundlichem Verhalten zu erzielen. Bei einem weiteren, letztlich jedoch diffusen, Verständnis des Begriffs *nudge*[273] fallen auch die bereits genannten transparenzbasierten Ansätze unter diese Kategorie.[274]

a) Interventionsmöglichkeiten

Den rechtlichen Hauptanwendungsfall von *privacy nudges* stellt freilich der bereits umfänglich erörterte[275] Grundsatz des *privacy by default* dar.[276] Wie bereits gesehen, hat die Wahl der Voreinstellung zum Beispiel bei Cookie-Einwilligungen dramatische Wirkungen: Im Gegensatz zum selten manifestierten Opt-Out erlauben weniger als 0,1 % der Nutzer Cookies für alle Zwecke, und weniger als 4 % für die Zwecke von *third-party tracking*, wenn sie aktiv selbst

---

[270] Siehe etwa den Überblick bei *Camerer/Loewenstein/Rabin* (Hrsg.), Advances in Behavioral Economics, 2004; Thaler (Hrsg.), Advances in Behavioral Finance, 2005; *Altman* (Hrsg.), Handbook of Contemporary Behavioral Economics: Foundations and Developments, 2006.

[271] Siehe nur *Jolls/Sunstein/Thaler*, 50 Stanford Law Review 1998, 1471; *Korobkin/Ulen*, 88 California Law Review 2000, 1051; *Sunstein/Thaler*, Nudge: Improving Decisions About Health, Wealth, and Happiness, 2008; *Eidenmüller*, JZ 2005, 216; *Schmolke*, Grenzen der Selbstbindung im Privatrecht, 2014; *Alemanno/Sibony* (Hrsg.), Nudge and the Law: A European Perspective, 2015; *Hacker*, Verhaltensökonomik und Normativität, 2017; *Zamir/Teichmann*, Behavioral Law and Economics, 2018.

[272] Siehe etwa *Acquisti*, 7(6) IEEE Security & Privacy 2009, 82; *Wang et al.*, Proceedings of the 22nd International Conference on World Wide Web 2013, 763; *Monteleone et al.*, Nudges to privacy behaviour: Exploring an alternative approach to privacy notices, JRC Science and Policy Report, 2015; *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 359 ff.; *Acquisti*, 50(3) ACM Computing Surveys (CSUR) 2017, Article 44.

[273] So etwa bei *Thaler/Sunstein*, Nudge: Improving Decisions About Health, Wealth, and Happiness, 2008, 6: „A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid."; dagegen treffend, mit nuancierterem Begriffsverständnis, *Alemanno/Sibony*, in: Alemanno/Sibony (Hrsg.), Nudge and the Law: A European Perspective, 2015, 1 (10 f.); siehe auch *Hacker*, 24 European Review of Private Law 2016, 297 (304).

[274] *Acquisti*, 50(3) ACM Computing Surveys (CSUR) 2017, Article 44, 3.

[275] Siehe oben, § 4 C.III.

[276] *Acquisti*, 50(3) ACM Computing Surveys (CSUR) 2017, Article 44, 21.

einwilligen müssen.[277] Neben der durch Art. 4 Nr. 11 DS-GVO ausdrücklich zum gesetzlichen Standard erhobenen aktiven Einwilligung, die freilich nach dem späten Urteil des EuGH auch unter der DSRL bereits verpflichtend gewesen wäre,[278] lassen sich auch bei der Gestaltung einer ganzen Reihe weiterer Parameter Verhaltenseffekte für datenschutzfreundliche Ergebnisse nutzen. Zu nennen sind hier insbesondere[279] das *framing* einer Einwilligung,[280] die Reihenfolge von Optionen,[281] die Hervorhebung bestimmter Schaltflächen[282] oder auch die Wahl der bereits angesprochenen Icons.[283]

Ferner ist es denkbar, verhaltensökonomische Effekte nicht (nur) für eine Lenkungswirkung zu nutzen (*nudge*), sondern Interventionen so zu gestalten, dass kognitive Verzerrungen der Informationsverarbeitung durch Nutzer reduziert oder gar eliminiert werden (*debiasing*).[284] Dabei existiert durchaus eine Schnittmenge zwischen beiden Techniken: Werden verhaltensökonomische Effekte (zum Beispiel durch Salienz erzeugte mentale Verfügbarkeit, *availability heuristic*[285]) eingesetzt, um kognitive Verzerrungen zu verringern[286] (zum Beispiel die Unterschätzung von datenschutzrechtlichen Risiken infolge von Überoptimismus, *optimism bias*[287]), so spricht man bisweilen von *rebiasing*.[288]

b) Bewertung

Der Verfasser hat sich an anderer Stelle bereits ausführlich mit den Vorzügen und Nachteilen verhaltensbasierter Regulierung auseinandergesetzt.[289] Daher mögen auch an dieser Stelle einige Hinweise genügen. *Debiasing* ist zwar grund-

[277] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (2, 9).

[278] Siehe oben, § 4 B.4.b)bb)(1)(b).

[279] Siehe den Überblick bei *Acquisti*, 50(3) ACM Computing Surveys (CSUR) 2017, Article 44, 13 ff.

[280] Siehe oben, § 3, Fn. 88.

[281] *Wang et al.*, Proceedings of the 32nd annual ACM conference on human factors in computing systems 2014, 2367.

[282] Hier zeigte sich ein erheblicher Effekt in *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (9).

[283] Für eine Einordnung als *nudge Krönke*, Der Staat 55 (2016), 319 (329 f.); treffend differenzierend nach der Rechtfertigungsgrundlage *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 61 ff.

[284] Zu Begriff und Wirkung von *debiasing* ausführlich *Larrick*, in: Koehler/Harvey (Hrsg.), Blackwell Handbook of Judgment and Decision Making, 2004, 316; *Jolls/Sunstein*, 35 The Journal of Legal Studies 2006, 199; *Hacker*, Verhaltensökonomik und Normativität, 2017, 574 ff.

[285] Dazu grundlegend *Tversky/Kahneman*, 5 Cognitive Psychology 1973, 207; siehe auch *N. Schwarz/Vaughn*, in: Gilovich et al. (Hrsg.), Heuristics and Biases: The Psychology of Intuitive Judgment, 2002, 103.

[286] *Hacker*, Verhaltensökonomik und Normativität, 2017, 585 ff.

[287] Dazu etwa *DeJoy*, 21 Accident Analysis & Prevention, 1989, 333; *Weinstein*, 246 Science, 1989, 1232; *Sharot*, 21 Current Biology 2011, R941.

[288] *Larrick*, in: Koehler/Harvey (Hrsg.), Blackwell Handbook of Judgment and Decision Making, 2004, 316 (317); *Hacker*, Verhaltensökonomik und Normativität, 2017, 585.

[289] *Hacker*, Verhaltensökonomik und Normativität, 2017, Zweiter und Dritter Teil.

sätzlich wünschenswert, um Nutzern eine rationale Wahl hinsichtlich der Vor- und Nachteile von Datenverarbeitung zu ermöglichen. Allerdings ist dabei im Blick zu behalten, dass rationales Handeln die negativen Externalitäten der Datenverarbeitung verstärken kann, wenn sich nämlich, wie gesehen,[290] die Einwilligung in Datenverarbeitung als rational dominante Strategie erweist, durch diesen Effekt jedoch das soziale Optimum an Datenverarbeitung überschritten wird.[291] Zwar ist nicht gesagt, dass jede Form von rationalitätsstärkender Maßnahme diesen Effekt haben wird; vielmehr können insbesondere Nutzer mit stark ausgeprägten Datenschutzpräferenzen zu dem Schluss kommen, dass für sie bei rationaler Betrachtung eine Verweigerung der Einwilligung gerade individuell nutzenmaximierend ist. Allerdings sind *debiasing*-Strategien regelmäßig äußerst schwer zu kalibrieren: Da das Ausmaß an kognitiven Verzerrungen individuell und auch kontextuell stark variiert,[292] können Maßnahmen mit rationalitätsfördernder Intention schnell über das Ziel hinausschießen und kognitive Verzerrungen in die entgegengesetzte Richtung induzieren.[293] Wenn etwa salient vor den Gefahren der Datenverarbeitung gewarnt wird, mag dies dazu führen, dass ein signifikanter Anteil der Nutzer die Risiken der Datenverarbeitung nicht mehr unter-, sondern überschätzt. Insofern sind vor derartigen Interventionen umfassende empirische Tests ratsam.

Bezüglich *privacy by default* wurde bereits oben im Rahmen der Diskussion von Art. 25 DS-GVO festgestellt,[294] dass diese Regel als *penalty default* angesehen werden kann, die gegenüber der entgegengesetzten Regelung eines *tracking by default* eine signifikante Verbesserung der Informationslage und der Möglichkeit der Ausübung von Wahlfreiheit erwarten lässt. Zudem lassen sich dergestalt negative Externalitäten reduzieren. Nichtsdestoweniger bleibt festzustellen, dass jede dispositive Regelung, für oder gegen Datenschutz, den Präferenzen jedenfalls einer größeren Nutzergruppe widerspricht. Dies deutet, wie die Diskussion der datenschonenden Option noch im Einzelnen zeigen wird,[295] auf die Überlegenheit einer aktiven Wahl hin.

Schließlich ist zu bemerken, dass für die Zwecke der vorliegenden Untersuchung der Nutzen von über *data protection by default* hinausgehenden *privacy nudges* beschränkt ist. Erstens können Anbieter versuchen, so auf Nutzer einzuwirken, dass die Lenkungswirkung verpufft.[296] Zweitens kommt es zu einer Stärkung autonomer Nutzerentscheidungen nur dann, wenn Transparenz hinsichtlich der Lenkungswirkung sichergestellt ist und diese auch ef-

[290] Siehe oben, Text bei § 3, Fn. 96.
[291] *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 28, 72.
[292] *Stanovich/West*, 23 Behavioral and Brain Sciences, 2000, 645; *Stanovich/West/Toplak*, The Rationality Quotient: Toward a Test of Rational Thinking, 2016.
[293] Ausführlich *Hacker*, Verhaltensökonomik und Normativität, 2017, 605 ff.
[294] Siehe oben, § 4 C.III.2.
[295] Siehe unten, § 6 C.II.
[296] *Willis*, 29 Berkeley Technology Law Journal 2014, 61 (131): „Nudges can be powerful when no one is pushing back. But a push can easily overwhelm a nudge."

fektiv durch die Adressaten konterkariert werden kann.[297] Dies verringert jedoch zugleich typischerweise, wenngleich nicht notwendig,[298] die Wirksamkeit der Intervention. Nichttransparente staatliche Verhaltenslenkung kann denn vor allem dadurch gerechtfertigt werden, dass durch die Maßnahme negative Externalitäten der Preisgabe personenbezogener Daten verringert werden.[299] Dies ist zwar immer eine Frage des Einzelfalls, infolge des erhöhten Risikos negativer Externalitäten durch Anwendungen maschinellen Lernens[300] jedoch eine zunehmend relevante Rechtfertigungsstrategie.

3. Technologiebasierte Ansätze: Wege zu einer automatisierten Kommunikation von Datenschutzpräferenzen

Neben transparenz- und verhaltensbasierten bilden die technologiebasierten Ansätze die dritte Gruppe der Vorschläge zur Verbesserung der wirksamen Ausübung privatautonomer Gestaltungsmacht im datenschutzrechtlichen Kontext. Dabei ergibt sich zwar eine gewisse Schnittmenge mit den bereits diskutierten Technologien zur Minimierung von Datenschutzrisiken wie *privacy-enhancing technologies* und Verfahren maschinellen Lernens zur Rechtmäßigkeitskontrolle. Der besondere Akzent der nunmehr zu erörternden technologiebasierten Ansätze liegt jedoch darin, dass sie nicht lediglich durch technische Instrumente Transparenz hinsichtlich des Inhalts und der Rechtmäßigkeit der Datenverarbeitung herstellen oder einseitig die Erhebung von Daten minimieren, sondern Möglichkeiten zur direkten technologischen Kommunikation und Implementierung eigener datenschutzrechtlicher Präferenzen bieten sollen – ohne dass der einzelne Nutzer die jeweiligen konkreten Formen der Datenverarbeitung überhaupt notwendig zur Kenntnis nehmen müsste. Darin läge ein entscheidender Vorzug: Wie gesehen können transparenzbasierte Ansätze nur zu einem geringen Grad rationale oder beschränkt rationale Ignoranz überwinden. Nur durch technische Unterstützung lässt sich daher ein effektives Datenermöglichungsrecht aufbauen.

Technologische Systeme zur Durchsetzung eigener Datenschutzpräferenzen werden in jüngerer Zeit häufiger sowohl in der rechtlichen als auch der informatischen Literatur vorgeschlagen.[301] Zunächst ist hier die technische

---

[297] *Hacker*, Verhaltensökonomik und Normativität, 2017, 265 ff., 273 ff.

[298] *Loewenstein et al.*, 1 Behavioral Science & Policy 2015, 35 (keine negative Wirkung der Transparenz bei dispositiven Regeln [*default rules*]); ebenso *Bruns et al.*, 65 Journal of Economic Psychology 2018, 41.

[299] *Kesan/Shah*, 82 Notre Dame Law Review 2006, 583 (621); *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 365.

[300] Siehe oben, § 3 B.II.1.c).

[301] *Efroni et al.*, 5 European Data Protection Law Review 2019, 352 (357); *Ziegler/Menon/Annichino*, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 149 (165 f.); *ConPolicy*, Wege zur besseren Informiertheit im Datenschutz, 2018, 71 ff.; *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (457); *Stiftung Datenschutz*, Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische

Machbarkeit darzustellen (a)) und eine Bewertung mit Blick auf die Möglichkeit der Förderung von Autonomieressourcen vorzunehmen (b)), bevor die bislang zum Teil mangelnde rechtliche Bindungswirkung und Durchsetzbarkeit thematisiert und rechtliche Reformvorschläge unterbreitet werden können (c)).

a) Technische Möglichkeiten

Technische Applikationen zur Durchsetzung datenschutzrechtlicher Präferenzen lassen sich in zwei Kategorien einteilen. Bereits seit längerer Zeit wird an Datenschutz-Dashboards geforscht, die manuell verwaltet werden (aa)). Zunehmend werden jedoch auch Instrumente für eine automatisierte Implementierung von Präferenzen entwickelt (bb)).

aa) Manuelles Datenschutz-Dashboard

Ein Datenschutz-Dashboard ist eine zentrale digitale Anlaufstelle, „über welche die betroffenen Personen die ‚Datenschutzinformationen' einsehen und ihre Datenschutzpräferenzen verwalten können, indem sie ihre Einwilligung zu der Nutzung ihrer Daten auf gewisse Weise durch den besagten Dienst geben oder dieser widersprechen."[302] Die FTC[303] und die Artikel-29-Datenschutzgruppe befürworten ihre Einrichtung,[304] ebenso wie viele Stimmen in der Literatur.[305] Wichtig ist dabei, dass das Dashboard die Möglichkeit bietet,

Herausforderungen, 2017, 35; *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 44, 59 f.; *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (415 ff.); *European Commission*, An emerging offer of „personal information management services". Current state of service offers and challenges, Report, 2016, 1 f.; *European Data Protection Supervisor*, Opinion on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data, Opinion 9/2016, 2016, 5; *Policy and Research Group of the Office of the Privacy Commissioner of Canada*, Consent and privacy – A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act, 2016, 12 f.; *Edwards*, 2 European Data Protection Law Review 2016, 28 (57); *Hall/Hans/Henry*, Comments for November 2013 Workshop on the „Internet of Things" (1.6.2013), https://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00028-86211.pdf, 4.

[302] *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 1, 2018, 24; siehe auch *Zimmermann/Accorsi/Müller*, Ninth International Conference on Availability, Reliability and Security 2014, 152 (153).

[303] *Federal Trade Commission*, Mobile Privacy Disclosures, 2013, 16 f.

[304] *Artikel-29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 1, 2018, 24.

[305] *Reidenberg et al.*, 96 Washington University Law Review 2019, 1409 (1426 ff.); *Rosner/Kenneally*, Clearly Opaque. Privacy Risks of the Internet of Things, Bericht, 2018, 5; *Raschke et al.*, Proceedings of the IFIP International Summer School on Privacy and Identity Management 2017, 221; *Bier/Kühne/Beyerer*, Proceedings of the 4th Annual Privacy Forum 2016, 135; *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (416); *Schaub et al.*, Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 2015, 1 (8, 10); *Zimmermann/Accorsi/Müller*, Ninth International Conference on Availability, Reliability and Security 2014, 152; *Satyanarayanan*, IEEE Pervasive Computing 2003, 2 (2).

die Berechtigungen vieler oder gar aller auf einem Gerät laufenden Dienste einzusehen *und* zu ändern.[306]

Einen Vorläufer zu solchen umfassenderen Dashboards stellt die Browser-Erweiterung PrivacyBird dar,[307] die von dem Platform for Privacy Preferences (P3P) Project entwickelt wurde.[308] Der Nutzer kann darin Präferenzen hinsichtlich seines gewünschten Datenschutzniveaus festlegen; das Tool untersucht dann automatisiert, ob die Datenschutzerklärungen der Webseiten, die besucht werden, diesen Einstellungen entsprechen und meldet das Ergebnis an den Nutzer.[309] Allerdings kann mit dem PrivacyBird nur Transparenz hergestellt, nicht jedoch können Privatsphäreeinstellungen in Webseiten oder Apps verändert werden. Diese sog. Intervenienz wiederum ermöglichen neuere Instrumente, von denen bereits mehrere verfügbar sind.[310] Die App und Browser-Erweiterung PrivacyFix ermöglicht es Nutzern etwa, die Privatsphäreeinstellungen verschiedener sozialer Netzwerke zu visualisieren und Änderungen vorzunehmen.[311] Ebenfalls als App und Browser-Erweiterung steht PlusPrivacy bereit.[312] Mit diesem von der Europäischen Kommission geförderten Projekt lässt sich einerseits in ausgewählten sozialen Netzwerken (Facebook, Twitter und LinkedIn) sowie bei Google das Datenschutzniveau einstellen.[313] Soweit es die jeweiligen, durch das Dashboard unterstützten Anbieter erlauben, können damit die Privatsphäreeinstellungen mit einem Klick auf das datenschutzfreundlichste Niveau gebracht werden, auch jeweils wieder nach Updates der jeweiligen Netzwerke (sog. *single click privacy*).[314] Wollte man dies von Hand bewerkstelligen, so müsste man bei jedem Anbieter bis zu sechs verschiedene

---

306 Frühere Dashboards fungieren als reine Transparenzwerkzeuge, siehe den Überblick bei *Bier/Kühne/Beyerer*, Proceedings of the 4th Annual Privacy Forum 2016, 135 (136 f.); Betonung der Änderungsmöglichkeiten bei *Zimmermann/Accorsi/Müller*, Ninth International Conference on Availability, Reliability and Security 2014, 152 (153); *Cabinakova/Zimmermann/Mueller*, 24th European Conference on Information Systems (ECIS) 2016, 1 (2 f.); siehe auch *Federal Trade Commission*, Mobile Privacy Disclosures, 2013, 16.

307 http://privacybird.com/; siehe auch *Cranor*, 10 Journal on Telecommunications & High Technology Law 2012, 273 (280 f.); *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (415 f.).

308 https://www.w3.org/P3P/.

309 http://privacybird.com/.

310 Überblick über ältere Modelle bei *Bier/Kühne/Beyerer*, Proceedings of the 4th Annual Privacy Forum 2016, 135 (137); siehe auch *Raschke et al.*, Proceedings of the IFIP International Summer School on Privacy and Identity Management 2017, 221.

311 LegalCommDesign, PrivacyFix: Online Privacy Dashboard for social networks, http://www.legaltechdesign.com/communication-design/privacyfix-online-privacy-dashboard-for-social-networks/.

312 https://plusprivacy.com/.

313 PlusPrivacy, PlusPrivacy adds management of Google privacy (22.2.2018), https://plusprivacy.com/2018/02/22/plusprivacy-adds-automatic-management-of-google-privacy-settings/.

314 PlusPrivacy, PlusPrivacy adds management of Google privacy (22.2.2018), https://plusprivacy.com/2018/02/22/plusprivacy-adds-automatic-management-of-google-privacy-settings/.

Webseiten aufsuchen.[315] Modifikationen der einzelnen Einstellungen bei den verschiedenen unterstützten Anbietern sind auch möglich, sodass das Datenschutzniveau nach individuellen Vorlieben gewählt werden kann. Ferner bietet das Instrument auch Identitätsschutz im E-Mail-Verkehr[316] und fungiert als Ad-Blocker.[317] Schließlich vermag es Berechtigungen von Apps und Browser-Erweiterungen für den Zugriff auf Daten anzuzeigen und zu kappen.[318] Aufgebaut werden soll noch eine Rechtmäßigkeitskontrolle nach der DS-GVO.[319] Damit vereint PlusPrivacy bereits jetzt signifikante Funktionalitäten aus dem Bereich der *privacy-enhancing technologies* und der Präferenzkontrollinstrumente, mit einer möglichen Erweiterung auf die Rechtmäßigkeitskontrolle. Auch andere Instrumente setzen nunmehr verstärkt darauf, im Rahmen eines Dashboards die Ausübung von Betroffenenrechten nach der DS-GVO (zum Beispiel das Recht auf Löschung) zu automatisieren.[320] Damit werden Dashboards zunehmend zu einer umfassenden Schaltstelle für die eigenverantwortliche Wahrnehmung von datenbezogenen Interessen.

Für den Bereich sozialer Netzwerke und Suchmaschinen sind daher bereits leistungsstarke Angebote am Markt vorhanden. Demgegenüber hinken die Entwicklungen eines IoT-Dashboards deutlich hinterher,[321] auch wenn einige Prototypen existieren.[322] Gerade im Internet der Dinge wäre es aufgrund der zunehmenden Anzahl vernetzter Geräte essenziell, Privatsphäreeinstellungen gebündelt vornehmen zu können.[323] Gegenwärtig beziehen sich technische Access-Systeme im Bereich des IoT jedoch häufig nur auf die unmittelbare Pro-

[315] PlusPrivacy, PlusPrivacy adds management of Google privacy (22.2.2018), https://plusprivacy.com/2018/02/22/plusprivacy-adds-automatic-management-of-google-privacy-settings/; siehe auch die Untersuchung der norwegischen Verbraucherbehörde *Forbrukerrådet*, Deceived by Design, 2018.

[316] PlusPrivacy, PlusPrivacy feature – email identity management (28.11.2017), https://plusprivacy.com/2017/11/28/plusprivacy-feature-email-identity-management/.

[317] https://plusprivacy.com/faq/.

[318] PlusPrivacy, Making sense of connected apps and browser extensions using PlusPrivacy (7.12.2017), https://plusprivacy.com/2017/12/07/making-sense-of-connected-apps-and-browser-extensions-using-plusprivacy/.

[319] https://plusprivacy.com/.

[320] *Raschke et al.*, Proceedings of the IFIP International Summer School on Privacy and Identity Management 2017, 221; *Zibuschka/Horsch/Kubach*, Open Identity Summit 2019, 119 (126).

[321] *Zibuschka/Horsch/Kubach*, Open Identity Summit 2019, 119 (125).

[322] Siehe *Ebinger et al.*, 1st International Workshop on Smart Grid Security 2012, 120, für *smart meters*; *Seitz/Selander/Gehrmann*, IEEE 14th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013, 1; umfassendere Entwicklung eines Dashboards mit Interventionsfunktion *Zibuschka/Horsch/Kubach*, Open Identity Summit 2019, 119 (125 f.); http://www.entourage-projekt.de/.

[323] *Satyanarayanan*, IEEE Pervasive Computing 2003, 2 (2); *Zibuschka/Nofer/Hinz*, Multikonferenz Wirtschaftsinformatik (MKWI) 2016, 1391 (1398 f.); *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (36).

duktfunktionalität und bieten typischerweise keine Möglichkeit, die Weiterleitung von Daten oder deren Analyse spezifisch zu unterbinden.[324]

bb) Automatisierte Kontrollinstrumente

Die bislang vorgestellten Dashboards werden manuell verwaltet. Sie bieten zwar die Möglichkeit zur Intervention, die jedoch von den Nutzern jeweils in eigener Regie veranlasst werden muss. Gegenwärtig werden jedoch zunehmend Anwendungen entwickelt, welche die Kontrolle über datenschutzrechtlich relevante Prozesse automatisieren.[325] Diese neue Generation von Datenschutzassistenten (*privacy assistants*) kann entweder extern vorgegebene Datenschutzpräferenzen selbstständig umsetzen oder gar das gewünschte Informations- und Datenschutzniveau, nach einer initialen Konfiguration, selbst aus den Handlungen des Nutzers erlernen (*personalized privacy assistant*).[326] Empirische Studien zeigen, dass die Nutzung der Intelligenz eines technischen Systems auch für die automatisierte Steuerung der Datenschutzoptionen bei Nutzern beliebter ist als die individuell-manuelle Intervention.[327]

Intelligente Datenschutzassistenten können die Grundlage sein für ein Regime der technologischen Einwilligung durch personalisierte Mastereinwilligungen:[328] die automatisierte Kommunikation mit Webseiten, Apps und IoT-Geräten, bei der bereits prospektiv, und nicht lediglich nachträglich, Kontrolle über die Datenverarbeitung durch die Kommunikation von Datenschutzpräferenzen ausgeübt wird.[329] Gerade für stark vernetzte Umgebungen sind solche Werkzeuge essenziell, um selektiv relevante Datenschutzinformationen anzuzeigen und insbesondere weitgehend automatisiert diejenigen Optionen zu

---

[324] Siehe *Madaan/Ahad/Sastry*, 34 Computer Law & Security Review 2018, 125 (130).

[325] *Alpers et al.*, 3rd IEEE International Conference on Computer and Communications (ICCC) 2017, 1460; *Pappachan*, IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW) 2017, 193; *Das et al.*, IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) 2017, 1387; *Das et al.*, 17 (3) IEEE Pervasive Computing 2018, 35; *Cunche/Le Métayer/Morel*, A Generic Information and Consent Framework for the IoT (Extended Version), Research Report 9234, 2018; *Lu et al.*, Proceedings of 5th International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications 2019; für einen *legal assistant*, siehe *Joshi et al.*, 2016 AAAI Fall Symposium Series 2016, 149.

[326] *ConPolicy*, Wege zur besseren Informiertheit im Datenschutz, 2018, 71 f.; *Zibuschka/Nofer/Hinz*, Multikonferenz Wirtschaftsinformatik (MKWI) 2016, 1391 (1394 f.); *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (36).

[327] *Zibuschka/Nofer/Hinz*, Multikonferenz Wirtschaftsinformatik (MKWI) 2016, 1391 (1398 f.); *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (2); siehe auch *Emami-Naeini et al.*, Thirteenth Symposium on Usable Privacy and Security (SOUPS) 2017, 399 (410).

[328] Siehe zu einem personalisierten Einwilligungsrechtsregime auch *Busch*, 86 The University of Chicago Law Review 2019, 309 (323); *Hacker*, 7 International Data Privacy Law 2017, 266 (280).

[329] Frühe Vorschläge bei *Langheinrich*, International Conference on Ubiquitous Computing 2002, 237; *Sadeh/Chan/Van*, Proceedings of UBIAGENTS 2002, 34.

wählen, die mit den (manuell oder durch maschinelles Lernen erstellten) Master-Einstellungen übereinstimmen. Zugleich sollte es Nutzern möglich sein, ihre Master-Einstellungen im Einzelfall abzuändern.

Ein Vorläufer für ein solches System ist ein von Forschern an der Carnegie Mellon University entwickeltes Instrument, das Nutzern adaptiv hilft, Berechtigungen von Applikationen auf ihren Smartphones zu konfigurieren.[330] Dabei wird eine Empfehlung auf Grundlage eines Vergleichs mit den Entscheidungen ähnlicher Nutzer, bei denen kontrolliert Präferenzen erhoben wurden, generiert (*clustering*).[331] Ein Prototyp kann bereits auf Android Smartphones verwendet werden. In einer Feldstudie wurden 79 % der Empfehlungen von den Nutzern übernommen.[332]

Im Rahmen des Internets der Dinge liegt eine zentrale Herausforderung jedoch darin, dass Datenschutzassistenten überhaupt die Präsenz und Form der Datenverarbeitung von IoT-Geräten erkennen müssen.[333] Dies ist bei der Nutzung passiver Sensoren durch die Daten verarbeitenden Geräte nicht trivial. Gearbeitet wird daher etwa an einem *IoT Resource Registry* (IRR), in dem Eigentümer von IoT-Geräten mit minimalem Aufwand die Existenz, die Formen der Datenverarbeitung sowie etwaige Interventionsmöglichkeiten (Opt-In, Opt-Out etc.) vermerken können.[334] Anreize für Eigentümer, ihre Geräte, Dienste und Applikationen in ein IRR einzutragen, ergeben sich unter zwei Gesichtspunkten:[335] Erstens werden diese Gerätenutzern aktiv angezeigt, sodass sie auf die Funktionalität, womöglich auch gegen Entgelt, zugreifen können. Das IRR hat damit auch einen werblichen Aspekt. Zweitens ermöglicht erst die Information über die Datenverarbeitung datenschutzrechtliche Compliance mit Blick auf Art. 12 ff. DS-GVO. Die notwendigen Informationen können im IRR hinterlegt werden. Datenschutzassistenten können das IRR dann ansteuern, um relevante Geräte und Kontrollmöglichkeiten in der Umgebung des Nutzers ausfindig zu machen.[336] Die Präferenzen des Nutzers werden sodann über Schnittstellen am jeweiligen Gerät durchgesetzt, soweit dies

---

330 *Liu et al.*, Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016, 27; ein ähnliches System stellen vor *Oglaza et al.*, 11th International Conference on Availability, Reliability and Security (ARES) 2016, 1.

331 *Liu et al.*, Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016, 27 (30 f.); zum *clustering* der Nutzer genauer *Lin et al.*, 10th Symposium on Usable Privacy and Security (SOUPS) 2014, 199 (204 f.).

332 *Liu et al.*, Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016, 27 (35).

333 Vgl. *Cunche/Le Métayer/Morel*, A Generic Information and Consent Framework for the IoT (Extended Version), Research Report 9234, 2018, 5 ff.

334 *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (38 f.); *Pappachan*, IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW) 2017, 193 (193 f.); *Cunche/Le Métayer/Morel*, A Generic Information and Consent Framework for the IoT (Extended Version), Research Report 9234, 2018, 10 f.

335 *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (38).

336 *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (36, 41).

der Eigentümer zulässt.[337] Ein derartiges Assistenzsystem wurde als Pilotprojekt am Campus der Carnegie Mellon University eingerichtet, ein weiteres am Campus der University of California, Irvine.[338] Über eine Smartphone-App können sich Nutzer datenverarbeitende IoT-Geräte, Dienste und Apps anzeigen lassen und ihre spezifischen Verarbeitungspraktiken, soweit möglich, konfigurieren.[339] An der Nutzung von Techniken maschinellen Lernens für die automatisierte Selektion relevanter Informationen und die automatisierte Konfiguration wird zur Zeit der Abfassung dieses Manuskripts gearbeitet.[340] Wo eine präferenzkonforme Konfiguration nicht möglich ist, können Warnungen ausgesprochen werden.[341]

Eine besondere Möglichkeit, Datenschutzpräferenzen durchzusetzen, bietet insbesondere bei IoT-Geräten schließlich das bereits erwähnte *edge computing*.[342] Dabei werden die für das Gerät notwendigen Rechenoperationen nicht auf einem externen Server, etwa einer Cloud, sondern lokal auf dem Gerät selbst oder im Heimnetzwerk durchgeführt. Dadurch lassen sich individuell konfigurierte Datenschutzeinstellungen deutlich besser durchsetzen, da noch im Gerät oder Heimnetzwerk entschieden werden kann, welche Daten überhaupt wie verarbeitet werden sollen.[343] Auch dem Grundsatz der Datenminimierung kann damit Genüge getan werden.[344]

b) Bewertung

Technologiebasierte Ansätze bieten daher die vielversprechendste Möglichkeit zur Verbesserung der empirischen Einwilligungsvoraussetzungen. Zugleich stehen auch sie jedoch unter signifikanten Vorbehalten.

aa) Potenzial

Die vorgestellten technologiebasierten Ansätze haben erhebliches Potenzial.[345] Wenn informationsbasierter Datenschutz überhaupt eine Zukunft haben soll, werden sie unumgänglich sein. Datenschutz ist für die meisten Nutzer lediglich ein Konsumaspekt unter vielen. Die wirksame Ausübung von Privatautonomie im datenschutzrechtlichen Bereich kann daher letztlich nur über

[337] *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (41).
[338] *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (43 f.); *Pappachan*, IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW) 2017, 193.
[339] *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (40 f.).
[340] *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (41); *Pappachan*, IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW) 2017, 193 (193).
[341] *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (41).
[342] Siehe oben, Text bei § 2, Fn. 123.
[343] *Satyanarayanan*, 50 Computer 2017, 30 (32).
[344] *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (409 f.).
[345] Siehe die Nachweise in § 6, Fn. 301.

radikale Vereinfachung von Informationsvermittlung und Wahlmöglichkeiten sowie technische Hilfestellungen gelingen. Die vom Nutzer zu erbringende Eigeninitiative muss gegen null tendieren, da wie gesehen selbst kognitive Optimierungsverfahren der Informationsbereitstellung bislang nicht zu einer signifikant verstärkten Befassung des Durchschnittsnutzers mit datenschutzrechtlichen Belangen von Austauschprozessen geführt haben. Die Durchsetzung von Datenschutzpräferenzen muss daher zentralisiert (*single click privacy*)[346] oder automatisiert werden (*personalized privacy assistant*).

Gerade für das Internet der Dinge ist dies von eminenter Wichtigkeit.[347] IoT-Geräte erfassen bereits jetzt standardmäßig Daten von Dritten, wie der dritte Leitfall der Arbeit zeigt.[348] Dritte werden jedoch noch weniger Neigung verspüren, sich mit den Datenschutzkonfigurationen von Geräten anderer Personen zu beschäftigen als mit denen ihrer eigenen Geräte. Die Angaben, mit welchen Datenverarbeitungsvorgängen betroffene Personen einverstanden und nicht einverstanden sind, müssen daher durch IoT-Geräte und andere datensammelnde Dienste und Apps lesbar und automatisch zu verarbeiten sein, wie es etwa an den beiden Pilotprojekten an US-amerikanischen Universitäten der Fall ist. Die Nutzung technischer Hilfsmittel ist dabei weder hinsichtlich der technischen Bereitstellung noch der Nutzungs- und Zahlungsbereitschaft utopische Theorie: Nutzer von IoT-Geräten befürworten in einer empirischen Studie die Einrichtung von Dashboards und Assistenten, die Transparenz und Kontrollmöglichkeiten bieten, und geben an, für einen intelligent den Datenschutz umsetzenden persönlichen Assistenten, der IoT-Geräte steuert, im Schnitt knapp 20 € pro Monat ausgeben zu wollen.[349] Für ein Smart Home Gerät, das 49 $ kostet, waren Nutzer im Schnitt bereit, etwa 14 $ für zusätzlichen Datenschutz auszugeben.[350] Dies muss sich in Feldversuchen und im Konsumalltag erst noch bewähren, erste Kooperationen mit namhaften Herstellern laufen jedoch bereits.[351] Nur so können heterogene Datenschutzpräferenzen in der Realität letztlich in vernetzte Umgebungen eingespielt werden.

bb) Limitationen

Das genannte Potenzial technologiebasierter Ansätze lässt sich jedoch nur realisieren, wenn die noch bestehenden Beschränkungen sowohl auf technischer

[346] *Stiftung Datenschutz*, Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, 2017, 36.

[347] *Satyanarayanan*, IEEE Pervasive Computing 2003, 2 (2); *Zibuschka/Nofer/Hinz*, Multikonferenz Wirtschaftsinformatik (MKWI) 2016, 1391 (1398 f.); *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (36).

[348] Siehe oben, § 3 D.I.3.

[349] *Zibuschka/Nofer/Hinz*, Multikonferenz Wirtschaftsinformatik (MKWI) 2016, 1391 (1398).

[350] *Barbosa et al.*, Proceedings on Privacy Enhancing Technologies 2019, 211 (220).

[351] Siehe etwa die Kooperation mit Bosch im Rahmen des Entourage-Projekts, http://www.entourage-projekt.de/, unter Konsortium.

(1) als auch ökonomischer Ebene (2) überwunden werden. Hinzu kommt eine regulatorische Ebene, die das rechtskonforme Funktionieren von Datenschutzassistenten, die mit sensiblen Daten umgehen, sicherstellen muss (3).

(1) Technische Ebene: Technikreife

In technischer Hinsicht ist festzustellen, dass die Entwicklung sowohl von Datenschutz-Dashboards als auch von Datenschutzassistenten, die durch maschinelles Lernen unterstützt werden, zwar Gegenstand aktueller Forschung ist, aber einsatzfähige Instrumente noch nicht in allen Bereichen ausgereift oder gar am Markt etabliert sind.[352] Insbesondere im Rahmen des Internets der Dinge sind technische Applikationen zur Durchsetzung von Datenschutzpräferenzen erst in der Erprobungsphase.[353] Wegen der Vielzahl der Anbieter stellt die koordinierte, zentralisierte Abbildung von Informationen und Konfiguration von Geräten hier eine deutlich größere Herausforderung dar als in anderen Kontexten, in denen man sich (etwa bei sozialen Netzwerken oder Suchmaschinen) auf wenige, führende Anbieter konzentrieren kann.[354] In diesen zuletzt genannten Bereichen ist denn auch die Technikreife für Instrumente zur Durchsetzung von Datenschutzpräferenzen deutlich höher. Allerdings können sie auch dort immer nur soweit fruchten, wie anbieterseitig Optionen zur Verfügung gestellt werden, die den kommunizierten Datenschutzpräferenzen entsprechen.[355] Bei sozialen Netzwerken und Suchmaschinen ist dies gerade für Nutzer mit stark ausgeprägten Datenschutzpräferenzen häufig nur eingeschränkt der Fall. Insgesamt fehlt es für bereichsübergreifende Datenschutz-Dashboards oder Assistenten an einheitlichen Schnittstellen, über welche die Instrumente Informationen abfragen und Konfigurationen einspielen können. Hier besteht rechtlicher Reformbedarf, wie gleich noch zu thematisieren ist (siehe unter § 6 C.I.3.c)bb)).

(2) Ökonomische Ebene: Anreize und Präferenzen

Auf ökonomischer Ebene sind einerseits die mit einer erhöhten Kontrollmöglichkeit einhergehenden Anreize und Folgen zu bedenken, muss andererseits aber auch die rationale Formung von Präferenzen, die mithilfe technischer Applikationen durchgesetzt werden sollen, generell kritisch hinterfragt werden.

---

352 Siehe *Stiftung Datenschutz*, Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, 2017, 36.

353 *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (36).

354 *Emami-Naeini et al.*, Thirteenth Symposium on Usable Privacy and Security (SOUPS) 2017, 399 (410); *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (44).

355 Siehe *Rhahla et al.*, IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE) 2019, 170; *Hall/Hans/Henry*, Comments for November 2013 Workshop on the „Internet of Things" (1.6.2013), https://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00028-86211.pdf, 4.

(a) Kontrolle und Veröffentlichungsbereitschaft

Empirische Studien weisen darauf hin, dass die Gewährung von Kontrolle über Privatsphäreeinstellungen kontraintuitive Folgen für das Verhalten der Betroffenen haben kann: So kann mehr Kontrolle dazu führen, dass die Akteure im Schnitt mehr Informationen über sich selbst veröffentlichen als in einer Umgebung, in der es an Kontrolle fehlt.[356] Dies weist darauf hin, dass unabgestimmte Versuche zur Wiederherstellung der Datensouveränität jedenfalls insoweit untauglich sind, als das normative Ziel in einer Minimierung des absolut zur Verfügung gestellten Volumens personenbezogener Daten besteht. Demgegenüber ist jedoch zweierlei zu bemerken. Erstens ist die Minimierung der Veröffentlichung personenbezogener Daten kein Selbstzweck. Ein regulatorisches Problem besteht lediglich dann, wenn die Akteure entweder die Konsequenzen der Veröffentlichung nicht überblicken oder negative Externalitäten bestehen. Wie die Ausführungen in § 3 gezeigt haben, liegen für beide Problembereiche durchaus empirische Anknüpfungspunkte vor.

Dies legt jedoch zweitens nicht den Schluss nahe, dass die Zurverfügungstellung von Kontrollmöglichkeiten gar kein lohnendes Ziel sein könne. Vielmehr müssen die damit einhergehenden regulatorischen Probleme der möglicherweise stärkeren Bereitschaft der Nutzer zur Informationsveröffentlichung durch geeignete rechtliche Antworten eingefangen werden. Die vorangegangenen Teile der Arbeit liefern dafür Vorschläge: Unreflektierten Formen der Informationsveröffentlichung kann durch transparenzbasierte Ansätze, die ohnehin typischerweise mit den technologiebasierten Formen der Durchsetzung von Datenschutzpräferenzen verknüpft werden, entgegengewirkt werden. Verhaltensbasierte Ansätze adressieren kognitive Verzerrungen. Externalitäten wiederum erfordern spezifische Formen der Regulierung; Art. 25 DS-GVO weist hier in die richtige Richtung.[357] Daran erweist sich einmal mehr, dass es nicht die eine, einfache Lösung gibt, um den verschiedenen Typen von Marktversagen und sozialen Risiken im Bereich datenbasierter Austauschprozesse zu begegnen. Notwendig ist vielmehr ein integrierter Mix an Maßnahmen, mit dem soweit als möglich die verschiedenen Problembereiche adressiert werden.

Sofern autonomiefördernde Maßnahmen daher mit den genannten weiteren regulatorischen Interventionen verknüpft werden, erscheint das Ziel der Erhöhung einer Kontrolle über die Datenverarbeitung legitim, auch wenn dies in der Summe zu einer erhöhten Veröffentlichung personenbezogener Daten führen sollte: Wo Kontrollmöglichkeiten und Transparenz auf technisch vereinfachten

[356] *Brandimarte/Acquisti/Loewenstein*, 4 Social Psychological and Personality Science, 2013, 340; *Cabinakova/Zimmermann/Mueller*, 24th European Conference on Information Systems (ECIS) 2016, 1 (12); siehe auch *Xu et al.*, 26 Journal of Management Information Systems 2009, 135 (160).

[357] Siehe oben, Text bei § 4, Fn. 1080.

Wege bereitgestellt werden, beginnt letztlich der Bereich der datenschutzrechtlichen Eigenverantwortung, den die Ausübung von Privatautonomie immer voraussetzt.

(b) Formung und Modellierung von Präferenzen

Ein weiterer Einwand gegen Instrumente zur Durchsetzung von Datenschutzpräferenzen hinterfragt den Begriff der Datenschutzpräferenz an sich. Denn Heterogenität herrscht nicht nur hinsichtlich der Präferenzen zwischen verschiedenen Akteuren; auch die Präferenzen einzelner Akteure sind, wie empirische Studien zeigen, stark kontextabhängig.[358] Sie differieren zum Beispiel nachvollziehbarer Weise zwischen öffentlichem und privatem Raum.[359] Wenn jedoch individuelle Nutzer gar keine stabilen Datenschutzpräferenzen aufweisen, wie sollen diese sinnvoll durchgesetzt werden?

Hierauf lassen sich drei Antworten geben. Trotz kontextspezifischer Differenzen dürfte erstens die grundsätzliche Ausrichtung von Datenschutzpräferenzen bei den einzelnen Nutzern verhältnismäßig stabil sein. Auch wenn hierzu, soweit ersichtlich, empirische Erhebungen fehlen, so steht doch zu erwarten, dass Nutzer, die der Verarbeitung ihrer personenbezogenen Daten grundsätzlich kritisch gegenüberstehen, über verschiedene Kontexte hinweg stärker ausgeprägte Datenschutzpräferenzen haben werden als solche Nutzer, denen der Umgang mit ihren Daten gleichgültig ist. Diese grundsätzliche Ausrichtung lässt sich aber bereits in sinnvoller Weise zum Beispiel durch Datenschutzassistenten umsetzen.

Zweitens ist gerade die Modellierung und kontextbezogene Vorhersage von Datenschutzpräferenzen ein Feld aktiver Forschung. Auch insoweit wird auf Modelle maschinellen Lernens zurückgegriffen, um Datenschutzpräferenzen zu approximieren.[360] In einer bereits genannten Feldstudie wurden 79 % der Empfehlungen eines Datenschutzassistenten, die mithilfe prädiktiver Modellierung von Präferenzen erstellt wurden, angenommen.[361] Ein anderes Modell konnte Präferenzen mit einer Genauigkeit (*accuracy*) von 88 % vorhersagen, nachdem es in lediglich drei unterschiedlichen Situationen individuelle Privatsphäreentscheidungen beobachtet hatte;[362] ein weiteres kam bei Nutzern, über

[358] *Acquisti/Brandimarte/Loewenstein*, 347 Science 2015, 509 (511 f.); *Acquisti/Taylor/Wagman*, 54 Journal of Economic Literature 2016, 442 (476–478); *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (37); *Barbosa et al.*, Proceedings on Privacy Enhancing Technologies 2019, 211 (212); *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 30; siehe zudem die Nachweise in § 3, Fn. 88.

[359] *Emami-Naeini et al.*, Thirteenth Symposium on Usable Privacy and Security (SOUPS) 2017, 399 (409).

[360] *Barbosa et al.*, Proceedings on Privacy Enhancing Technologies 2019, 211 (213 f.).

[361] *Liu et al.*, Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016, 27 (27, 30 f.).

[362] *Emami-Naeini et al.*, Thirteenth Symposium on Usable Privacy and Security (SOUPS) 2017, 399 (410).

die gar keine Vorinformationen vorlagen, auf eine *accuracy* von 87 %.[363] In reellen Nutzungsanwendungen dürften die Zahl der beobachtbaren Entscheidungen und damit auch die Vorhersagegenauigkeit noch deutlich höher liegen.[364] Ein weiteres Instrument erreichte bei der Vorhersage von kontextbezogenen Präferenzen hinsichtlich des Zugriffs von Apps auf Smartphone-Daten sogar eine Genauigkeit von 97 %.[365] Auch für den Einsatz von IoT-Geräten in Smart Homes ließen sich gute Ergebnisse bei der kontextbasierten Präferenzmodellierung erzielen.[366] Der Einsatz von personalisierten Datenschutzassistenten, welche die durchzusetzenden Einstellungen adaptiv durch Untersuchung des Nutzerverhaltens anpassen, verspricht daher, die Kontextgebundenheit von Präferenzen immer besser abzubilden. Wichtig ist dabei neben der Genauigkeit der Vorhersage dann vor allem, dass die Assistenten selbst die gewonnenen Daten lediglich zur Konfiguration der Datenschutzeinstellungen und nicht anderweitig verwenden.

Drittens bieten die bislang entwickelten Datenschutzassistenten Nutzern die Möglichkeit, Einstellungen für konkrete Situationen oder auch generell abzuändern, wenn sich Präferenzen ändern. Die Technik kann dem Nutzer auch insoweit nicht alles abnehmen. Es verbleibt ein irreduzibler Bereich der Eigenverantwortung, den die Betroffenen jeweils wahrnehmen müssen. Auch ausgereifte technische Lösungen werden daher nicht zu einem vollständig präferenzkonformen Verhalten aller Akteure führen, aber sie können dazu zumindest einen signifikanten Beitrag leisten.

(3) Regulatorische Ebene

Aufgrund der Verarbeitung potenziell sensibler, jedenfalls personenbezogener Daten speziell durch präferenzmodellierende Assistenten spielt schließlich deren Regulierung eine bedeutende Rolle,[367] die hier nur angeschnitten werden kann. So wird man, im Bereich der Aufsicht durch die Datenschutzbehörden, durch konsequentes Enforcement darauf achten müssen, dass die Vorgaben der DS-GVO hinsichtlich des Umgangs mit den durch die Assistenten notwendig zu erhebenden und zu verarbeitenden Nutzerdaten der Nutzer strikt eingehalten werden. Zudem mag man an spezifische Regelungen für Interessenkonflikte denken, die insbesondere bei Modellen entstehen können, die mit entgeltlichen *White Lists* von bestimmten Unternehmen arbeiten.[368]

[363] *Rosni et al.*, Proceedings of the PAL: Privacy-Enhancing Artificial Intelligence and Language Technologies 2019, 53 (58).

[364] *Emami-Naeini et al.*, Thirteenth Symposium on Usable Privacy and Security (SOUPS) 2017, 399 (410).

[365] *Wijesekera et al.*, IEEE Symposium on Security and Privacy (SP) 2017, 1077.

[366] *Barbosa et al.*, Proceedings on Privacy Enhancing Technologies 2019, 211 (214).

[367] Siehe etwa *Gal*, 25 Michigan Technology Law Review 2018, 59 (91 ff.); *Gal/Elkin-Koren*, 30 Harvard Journal of Law and Technology 2016, 309 (339 ff.).

[368] Diese Praxis ist z. B. bei AdBlockern weit verbreitet, siehe nur BGH, NJW 2018, 3640 Rn. 18, 26 – Werbeblocker II; BGH NJW 2020, 64 Rn. 25 f. – Werbeblocker III.

c) Eingeschränkter rechtlicher Reformbedarf

Die technischen Limitationen technologiebasierter Ansätze werden aller Voraussicht nach mit zunehmender Reife der Applikationen geringer werden. Die ökonomischen Beschränkungen lassen sich ebenfalls zum Teil durch technische Ansätze überwinden, weisen jedoch zudem verstärkt auf die Notwendigkeit koordinierter und integrierter Bemühungen zur Adressierung der verschiedenen Typen von Marktversagen im Bereich der digitalen Wirtschaft hin. Die regulatorischen Herausforderungen schließlich stellen sich zuvorderst als solche der konsequenten Durchsetzung des bestehenden Datenschutzrechts dar. Die vielleicht zentrale Limitation für technologiebasierte Ansätze hingegen erwächst aus der Rechtsordnung selbst.

Denn es muss erstens sichergestellt sein, dass die automatisierte Kommunikation von Datenschutzpräferenzen überhaupt als Wahl der betroffenen Person im Rechtssinne eingestuft wird (aa)). Zweitens müssen die technischen Grundlagen für eine Kommunikation zwischen Datenschutz-Dashboards oder -Assistenten einerseits und datenverarbeitenden Geräten, Diensten oder Applikationen andererseits gewährleistet sein (bb)).

aa) Rechtssichere automatisierte und autonome Kommunikation von Präferenzen

Die automatisierte Verwaltung, Kommunikation und Durchsetzung von Datenschutzpräferenzen ist, wie gesehen, nicht nur zunehmend technisch möglich, sondern auch für viele Nutzer in Befragungen gegenüber einer manuellen, tendenziell mühsamen Einzelverwaltung vorzugswürdig. Zugleich stellt sich damit jedoch die Frage, ob das geltende Datenschutzrecht für derartige automatisierte Ansätze schon bereit ist, sowohl im Regime der Einwilligung (1) als auch beim Widerspruch gegen bestimmte Formen der Datenverarbeitung (2).

(1) Einwilligungsregime nach der DS-GVO

Bei der Verwendung von intelligenten Systemen erhebt sich ganz allgemein die Frage, inwiefern von diesen generierte Erklärungen dem Nutzer zugerechnet werden können. Im allgemeinen Vertragsrecht hat sich daran anknüpfend eine Diskussion über Vertragsschlüsse unter Verwendung von mit künstlicher Intelligenz ausgestatteten Agenten entsponnen.[369] Für die soeben behandelten Datenschutzassistenten ist nun insbesondere relevant, inwiefern datenschutzrechtliche Einwilligungen nach der DS-GVO automatisiert, ggf. auch autonom,[370] abgegeben werden können.[371] Die (wohl) herrschende Literatur sieht

[369] Siehe oben die Nachweise in § 5, Fn. 348.

[370] Zum Unterschied von Automatisierung und Autonomie etwa *Hacker*, RW 9 (2018), 243 (251 ff.); *Specht*, Diktat der Technik, 2019, 45.

dies bislang kritisch.[372] Zwar entscheide sich der Nutzer bewusst und unmissverständlich zur Nutzung eines Datenschutzassistenten. Die Einwilligung in eine Datenverarbeitung müsse jedoch im konkreten Fall erteilt werden. Übernimmt dies allerdings ein Datenschutzassistent, so habe die betroffene Person weder zu einem bestimmten Zweck[373] noch informiert die Einwilligung erteilt.[374]

Nach hier vertretener Auffassung ist hingegen bereits nach geltendem Recht die Delegation von Einwilligungserklärungen an Datenschutzassistenten weitestgehend möglich. Dabei muss jedoch analytisch zwischen zwei Fällen unterschieden werden: der inhaltlichen Determination der Erklärung sowie der Abgabebedingungen *durch den Nutzer* einerseits (a) und der inhaltlichen Erstellung der Einwilligungserklärung sowie der Entscheidung über die Bedingungen ihrer Übermittlung *durch den Assistenten* andererseits (b). In beiden Fällen können allerdings im Ergebnis, nach hier vertretener Auffassung, die Bestimmtheit und Informiertheit der Einwilligung ebenso wie eine dem Nutzer zurechenbare Abgabe in der Regel bejaht werden. Es müssen jedoch (natürlich) auch die übrigen Anforderungen des Datenschutzrechts an die Einwilligungserklärung, insbesondere auch die Grenze des Art. 7 Abs. 4 DS-GVO, beachtet werden.[375]

(a) Automatisierte Einwilligung

Der Nutzer selbst kann Inhalt und Bedingungen für die Abgabe der Erklärung einmal über einen Datenschutzassistenten oder auch über Browser-Spezifikationen determinieren. Insofern kann man, parallel zur automatisierten Willenserklärung,[376] von einer automatisierten Einwilligung sprechen.

(aa) Schwach autonome Datenschutzassistenten

Werden der Inhalt der Einwilligungserklärung und die Bedingungen ihrer Abgabe im Wesentlichen durch den Nutzer determiniert, so handelt der Assistent nur schwach autonom[377] und setzt lediglich die Vorgaben des Nutzers automatisiert und zeitlich gestreckt um. In diesem Fall ist die automatisierte Er-

---

371 Zu Tatbestand und Abgabe der Einwilligungserklärung allgemein oben, § 5 B.II.2.b) und c).

372 *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 71.

373 *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 71.

374 *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 71.

375 *Stiftung Datenschutz*, Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, 2017, 40.

376 Siehe dazu die Übersicht bei *Paulus*, JuS 2019, 960.

377 Zur schwachen Autonomie näher *Hacker*, RW 9 (2018), 243 (253).

klärung nach allgemeinen zivilrechtlichen Grundsätzen gem. §§ 133, 157 BGB dem Nutzer zuzurechnen, weil sie von seinem Willen umfasst ist und er sich des Assistenten lediglich als eines Kommunikationswerkzeugs bedient.[378] Allerdings muss die Vorgabe, damit die Erklärung bestimmt im Sinne von Art. 4 Nr. 11 DS-GVO ist, einen hinreichenden Grad an Granularität aufweisen; sie darf insbesondere nicht vollkommen pauschal sein.[379]

Dabei dürfen jedoch keine hohen Anforderungen gestellt werden. Es wäre nachgerade paradox, wenn die DS-GVO die technisch unterstützte Ausübung von Datenschutzpräferenzen unterminierte, indem sie Nutzer für die Wirksamkeit der Einwilligung zu einem Grad der Beschäftigung mit datenschutzrechtlichen Belangen zwänge, den praktisch niemand erreichen kann noch will. Damit würde die gegenwärtig beste Möglichkeit einer residualen Kontrolle der Datenverarbeitung durch den Nutzer selbst, die doch ausweislich des siebten Erwägungsgrunds gerade Ziel der DS-GVO ist, konterkariert. Dies kann bei teleologischer Auslegung von Art. 4 Nr. 11 DS-GVO nicht überzeugen.

Ähnliche Erwägungen gelten für die Informiertheit der Einwilligung. Hier wurde bereits im datenschutzrechtlichen Teil der Arbeit nachgewiesen, dass die bloße Möglichkeit der Kenntnisnahme von Informationen genügt, ohne dass der Nutzer die Informationen tatsächlich rezipieren müsste.[380] Daher muss es genügen, wenn die zumutbare Möglichkeit besteht, im Einzelfall vor der Datenverarbeitung an die Informationen zu gelangen, etwa über Links oder Push-Hinweise im Assistenten. Wenn der Nutzer auf deren Kenntnisnahme aus freien Stücken verzichtet, macht dies die Einwilligung nicht unwirksam.

Günstig ist in jedem Fall, dass gegenwärtig künstliche Sprachen für Einwilligungserklärungen entwickelt werden, deren Semantik sowohl die Anforderungen der DS-GVO erfüllen soll als auch maschinenlesbar ist, so dass sie automatisiert von datenverarbeitenden Geräten, Diensten oder Applikationen angewandt werden können.[381] So kann ein Nutzer beispielsweise spezifizieren, dass von einem Gerät aufgezeichnete personenbezogene Daten nur zu

---

[378] *Wettig*, Vertragsabschluss mittels elektronischer Agenten, 2010, 151–155.; *Specht/Herold*, MMR 2018, 40 (41); *Paulus/Matzke*, ZfPW 2018, 431 (440 f.); *Spindler*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Vorbemerkung zu §§ 116 ff. Rn. 6 (dort als Computererklärung bezeichnet); *Paulus*, JuS 2019, 960 (963); *Specht*, Diktat der Technik, 2019, 44.

[379] *Stiftung Datenschutz*, Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, 2017, 38 f.; siehe auch *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 71; *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 20; siehe auch oben, § 4 B.I.3.a)bb).

[380] Siehe oben, § 4 B.I.3.a)cc)(2).

[381] *Pardo/Le Métayer*, Analysis of Privacy Policies to Enhance Informed Consent, Working Paper, 2019, https://arxiv.org/abs/1903.06068; *Cunche/Le Métayer/Morel*, A Generic Information and Consent Framework for the IoT (Extended Version), Research Report 9234, 2018, 11 f.; *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (419 f.).

Forschungszwecken benutzt werden dürfen und auch dies nur bis zu einem bestimmten Verfallsdatum.[382] In diesem Umfang sollte dann auch von einer wirksamen Einwilligung ausgegangen werden.[383]

(bb) Browser-Spezifikationen

Als wirksame Einwilligungserklärung nach Art. 4 Nr. 11 DS-GVO stellt es sich ferner dar, wenn nicht durch Datenschutzassistenten, sondern durch eine einfache, manuell konfigurierte Browser-Erweiterungen Präferenzen kommuniziert werden, zum Beispiel hinsichtlich der Cookies, in deren Speicherung man einwilligt.[384] Solches leistet etwa die Browser-Erweiterung „I don't care about cookies".[385] Darin kann spezifiziert werden, in die Nutzung welcher Formen von Cookies die betroffene Person einwilligt und in welche nicht. Dies wird als *request header* an die jeweiligen Webseiten, mit denen der Browser kommuniziert, übertragen.[386] Auch hier wird man die notwendige Eingrenzung des Zwecks der Datenverarbeitung nicht überspannen dürfen. Dies zeigt bereits der 32. Erwägungsgrund der DS-GVO, in dem ausdrücklich darauf hingewiesen wird, dass eine Einwilligung auch durch „die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft", also etwa Browser-Spezifikationen, erteilt werden kann.[387] Entscheidet sich der Nutzer beispielsweise frei dafür, Marketing-Cookies grundsätzlich zuzulassen, so muss diese Entscheidung ausreichen.[388] Denn die Zweckbeschränkung dient in erster Linie dem Nutzer selbst, sodass nicht ersichtlich ist, weshalb er nicht aus freien Stücken einen breiten Zweck sollte wählen können. Dagegen spricht allenfalls die Möglichkeit negativer Externalitäten, die jedoch, wie gesehen,[389] durch andere Formen der Regulierung adressiert werden sollte (z. B. Datenschutz durch Technikgestaltung).

(b) Autonome Einwilligung

Ein zusätzliches Problem tritt jedoch dann auf, wenn der Datenschutzassistent über den Inhalt und die Bedingungen der Übermittlung der Einwilligung in

[382] Siehe das Beispiel von *Pardo/Le Métayer*, Analysis of Privacy Policies to Enhance Informed Consent, Working Paper, 2019, https://arxiv.org/abs/1903.06068, 5.

[383] Siehe auch den 33. Erwägungsgrund der DS-GVO.

[384] Siehe auch bereits oben, § 4 B.I.4.c)aa) und sogleich unten, unter (3).

[385] https://www.i-dont-care-about-cookies.eu/notices/3.0.2/.

[386] Zur technischen Funktionsweise https://www.i-dont-care-about-cookies.eu/cookie-installing-permission-header/.

[387] So auch *Artikel-29-Datenschutzgruppe*, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, 2018, 20; *Stemmer*, in: BeckOK DatenschutzR, 28. Ed. 2018, Art. 7 DS-GVO Rn. 81; *Schantz*, NJW 2016, 1841 (1844); zweifelnd *Spindler*, DB 2016, 937.

[388] Zweifelnd, ob Browser-Spezifikationen das Bestimmtheitsgebot erfüllen, *Arning/Rothkegel*, in: Taeger/Gabel, DSGVO BDSG, 3. Aufl. 2019, Art. 4 DS-GVO Rn. 286.

[389] Siehe oben, § 6 C.I.3.b)bb)(2)(a).

stark autonomer Weise selbst entscheidet.[390] Handelt es sich dabei lediglich um eine Empfehlung, die der Nutzer jeweils bestätigen muss, so verwirklicht der Nutzer unstrittig selbst den objektiven und subjektiven Tatbestand der Einwilligung und gibt diese selbst ab. Rechtlich problematisch ist jedoch die Verwendung von Assistenten, welche die Datenschutzpräferenzen von Nutzern prädiktiv modellieren und daran angepasste, eigenständige Entscheidungen hinsichtlich der Übermittlung von Einwilligungserklärungen treffen, welche die Nutzer lediglich nachträglich abändern können. Umstritten ist hier zunächst, inwieweit eine eigenständige Erklärung des Assistenten dem Nutzer zugerechnet werden kann, die Erklärung also für und gegen die betroffene Person als Einwilligung im Sinne von Art. 4 Nr. 11 DS-GVO Wirkung entfaltet.[391]

(aa) Grundsätze der Zurechnung der Erklärung zum Nutzer

Die Interessenlage spricht dabei nach hier vertretener Ansicht für die Lösung dieser Fälle nach Maßgabe von zwei Prinzipien. Erstens muss die autonome Einwilligung, die der Datenschutzassistent eigenständig erstellt und übermittelt, dem Nutzer grundsätzlich zugerechnet werden (zur dogmatischen Konstruktion sogleich, unter [bb]). Dies impliziert insbesondere, dass die Einwilligung jedenfalls im Grundsatz auch dann Wirkung für und gegen den Nutzer entfalten muss, wenn sie auf Grundlage eines prädiktiven Fehlers des Datenschutzassistenten erstellt wurde, der Nutzer in der fraglichen Situation die Einwilligung also gar nicht abgegeben hätte. Dafür lässt sich zunächst die Korrelation von Nutzen und Risiko anführen:[392] *qui habet commoda ferre debet onera*.[393] Allerdings ist die Anwendung dieses Rechtssatzes hier nicht gänzlich überzeugend, da zwar der Einsatz des Datenschutzassistenten unbestritten für den Nutzer vorteilhaft ist, jedoch auch der Anbieter einer Leistung in einem datenbasierten Austauschverhältnis davon regelmäßig profitiert.[394] Einerseits kann so der Aushandlungsprozess deutlich effizienter gestaltet und andererseits, sofern die rechtlichen Wirkungen der Einwilligung eintreten, datenschutzrechtliche Compliance gefördert werden. Entscheidend ist daher der Gedanke der Risikobeherrschung: Beim Einsatz eines hinreichend autonomen Datenschutzassistenten geht es nicht mehr um die Zuweisung eines Produkt-, sondern eines Personalrisikos. Dieses ist auch in anderen rechtlichen Bereichen, etwa bei der Haftung nach § 278 BGB, in auf privatautonomer Gestaltung basierenden Verhältnissen dem Verwender stark autonomer Systeme zugewie-

[390] Zu starker Autonomie *Sartor*, in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, 263 (267 ff.); *Hacker*, RW 9 (2018), 243 (252); zum autonomen Vertragsschluss noch unten, § 6 C.II.3.b).

[391] Siehe die Nachweise oben, § 5, Fn. 348.

[392] *Paulus/Matzke*, ZfPW 2018, 431 (443); *Paulus*, Jus 2019, 960 (965).

[393] Zu diesem Rechtssatz bereits oben, § 4, Fn. 250.

[394] Vgl. zur parallelen Problematik im Vertragsrecht *Möschel*, AcP 186 (1986), 187 (199 f.); *Hacker*, RW 9 (2018), 243 (254).

sen.[395] Denn die richtige Auswahl, Instruktion (Voreinstellungen) und Überwachung (Fehlerdetektion und -korrektur, Feedback) des Assistenten kann der Nutzer viel effizienter leisten als der Anbieter.[396] Hinzu kommt, dass bei einem Fehlschlag der Zurechnung der Anbieter den Intermediär (den Datenschutzassistenten) *de lege lata* mangels Rechtspersönlichkeit und Haftungsmasse nicht selbst in Haftung nehmen kann. Bei dogmatischer Konstruktion über ein Stellvertretungsmodell läuft damit etwa § 179 BGB leer.[397] All dies spricht klar dafür, autonome Erklärungen des Assistenten nicht nur im vertraglichen,[398] sondern auch im datenschutzrechtlichen Bereich dem Nutzer zuzurechnen.

Eine Grenze muss diese Zurechnung zweitens jedoch dann finden, wenn der Anbieter Kenntnis davon hat, dass der Assistent die Vorgaben des „Innenverhältnisses" überschritten oder einen sonstigen prädiktiven Fehler gemacht hat. Denn dann ist der Anbieter nicht mehr schutzwürdig und die soeben genannten Argumente für eine Zurechnung zum Nutzer greifen nicht mehr.

(bb) Dogmatische Umsetzung: §§ 164 ff. BGB analog

In dogmatischer Hinsicht lassen sich diese Prinzipien *de lege lata* auf zwei Wegen umsetzen; beide offenbaren jedoch noch dogmatische Schwächen. Erstens kann dem Nutzer eine autonome Erklärung des Datenschutzassistenten wie eine automatisierte Einwilligungserklärung analog §§ 133, 157 BGB strikt zugerechnet werden.[399] Zur Begründung muss dann angeführt werden, dass durch die Inbetriebnahme und Konfiguration des Assistenten der objektive und subjektive Tatbestand der Einwilligungserklärung in hinreichender Weise erfüllt und die Abgabe autorisiert wurde.[400] Der Assistent würde dann wie ein schwach autonomer Computer (Werkzeug) oder wie ein menschlicher Bote behandelt.[401] Durchbrochen würde diese Zurechnung bei Kenntnis des Anbieters von einem Fehler nach § 242 BGB. Der Schwachpunkt dieser Lösung ist jedoch die Radizierung der autonomen Erklärung in der Willensbildung des Nutzers selbst: Mit zunehmender Autonomie des Assistenten fehlt es gerade an der Rückbindung der Erklärung an einen hinreichend konkretisierten Willen des Nutzers.[402]

---

[395] Dazu ausführlich *Hacker*, RW 9 (2018), 243 (255 ff.).

[396] Siehe *Hacker*, RW 9 (2018), 243 (255) m. w. N.

[397] Dies kritisieren *Foerster*, ZfPW 2019, 418 (426); *Spindler*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Vorbemerkung zu §§ 116 ff. Rn. 7; *Paulus/Matzke*, ZfPW 2018, 431 (443 f.); *Günther*, Roboter und rechtliche Verantwortung, 2016, 54; *Bräutigam/Klindt*, NJW 2015, 1137 (1138); *Wettig*, Vertragsabschluss mittels elektronischer Agenten, 2010, 180 f.; *Sorge*, Softwareagenten, 2006, 118; *Cornelius*, MMR 2002, 353 (355).

[398] Siehe nochmals die Nachweise in § 5, Fn. 348.

[399] *Paulus/Matzke*, ZfPW 2018, 431 (443 f.); *Paulus*, Jus 2019, 960 (965); *Pieper*, GRUR-Prax 2019, 298 (300).

[400] *Paulus/Matzke*, ZfPW 2018, 431 (444); *Leyens/Böttcher*, JuS 2019, 133 (135).

[401] *Spindler*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Vorbemerkung zu §§ 116 ff. Rn. 7; wohl auch *Keßler*, MMR 2017, 589 (592).

[402] *Specht/Herold*, MMR 2018, 40 (43); *Leyens/Böttcher*, JuS 2019, 133 (135).

Diese Verselbstständigung der Entscheidungskompetenz des Assistenten nimmt eine zweite dogmatische Lösung auf, die eine Zurechnung nach den Regeln des Stellvertretungsrechts gewährleistet. Zwar sind die §§ 164 ff. BGB mangels Rechtspersönlichkeit des Assistenten nicht direkt anwendbar,[403] sie können jedoch aus den oben genannten Erwägungen, die grundsätzlich für eine Zurechnung der Erklärung zum Nutzer sprechen, analog angewandt werden.[404] Der Schwachpunkt dieser Lösung liegt nach hier vertretener Auffassung vor allem darin, dass eine *strikte* Zurechnung zum Nutzer angesichts eines möglicherweise beschränkten Umfangs der „Vollmacht" nur schwer zu gewährleisten ist. Zwar ließe sich argumentieren, dass die Nutzung des (bekanntermaßen probabilistisch operierenden und daher fehlbaren) Assistenten grundsätzlich auch die Möglichkeit von Fehlprognosen einschließt, so dass derartige Fehler, bei Auslegung der „Vollmacht" analog §§ 133, 157 BGB, zumeist keine Überschreitung der Vertretungsmacht darstellen dürften.[405] Damit dürften Fälle des Handelns ohne Vertretungsmacht zumindest selten sein.[406] Ganz auszuschließen sind sie freilich nicht, wenn man den Gedanken der quasi-rechtsgeschäftlichen Vollmacht, die dem Datenschutzassistenten erteilt wird, ernst nimmt. Dann jedoch stellt sich in voller Schärfe das Problem des Fehlens einer Haftung des vollmachtlosen Vertreters analog § 179 BGB. Daher läge eine interessengerechte Lösung in einer im Außenverhältnis unbeschränkbaren Vollmacht.[407] Die Wirkung für und gegen den Nutzer entfiele nur bei einem erkannten oder evidenten Überschreiten der Vertre-

[403] *Cornelius*, MMR 2002, 353 (354); *Sester/Nitschke*, CR 2004, 548 (550 f.); *Keßler*, MMR 2017, 589 (592); *Specht/Herold*, MMR 2018, 40 (43).

[404] Ebenso im Ergebnis *Teubner*, AcP 182 (2018), 155 (181 f.); *Specht/Herold*, MMR 2018, 40 (43); *Sartor*, in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, 263 (272 ff.); *Schirmer*, JZ 2016, 660 (664); *Grundmann/Hacker*, 13 European Review of Contract Law 2017, 255 (283); *Kersten*, JZ 2015, 1 (7); *Surden*, 46 UC Davis Law Review 2012, 629 (694); dies erwägend auch *Specht*, Diktat der Technik, 2019, 46; explizit gegen eine analoge Anwendung der §§ 164 ff. BGB *Spindler*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Vorbemerkung zu §§ 116 ff. Rn. 7; *Paulus*, JuS 2019, 960 (965); *Leyens/Böttcher*, JuS 2019, 133 (135); *Günther*, Roboter und rechtliche Verantwortung, 2016, 54; *Wettig*, Vertragsabschluss mittels elektronischer Agenten, 2010, 178–183, der aber eine Analogie zum Wissensvertreter nach § 166 Abs. 1 BGB befürwortet, ebd., 188 f.; *Wiebe*, Die elektronische Willenserklärung, 2002, 130 ff.; für eine direkte Zurechnung zu demjenigen, der autonome Systeme im eigenen Interesse einsetzt, *Foerster*, ZfPW 2019, 418 (426); *Sosnitza*, CR 2016, 764 (767).

[405] Denkbar wäre daher für diese Fälle lediglich ein (eingeschränktes, siehe oben § 5 B.II.2.e): Fall des § 142 Abs. 2 BGB) Anfechtungsrecht, mit der Folge des § 122 BGB, siehe *Schirmer*, JZ 2016, 660 (664); *Leyens/Böttcher*, JuS 2019, 133 (136 f.). Allerdings entfällt bei positiver Kenntnis des Anbieters die Zurechnung ohnehin (dazu sogleich), so dass lediglich in Fällen des Kennenmüssens ein Anfechtungsrecht bestünde. Dieses ist jedoch gesperrt, wenn man, wie hier (unten, Text bei § 6, Fn. 412), eine Rechtsscheinshaftung analog § 172 Abs. 2 BGB bejaht, siehe BGH NJW 1964, 654 (656).

[406] *Sorge*, Softwareagenten, 2006, 61.

[407] *Schirmer*, JZ 2016, 660 (664); *Grundmann/Hacker*, 13 European Review of Contract Law 2017, 255 (283); *Foerster*, ZfPW 2019, 418 (427).

tungsmacht,[408] zum Beispiel wenn durch Attributzertifikate, gemeinsam mit der Einwilligungserklärung, klare Grenzen der Bevollmächtigung kommuniziert werden, die der Anbieter automatisiert verarbeiten kann.[409] Allerdings müsste die im Außenverhältnis unbeschränkbare Vollmacht gesetzlich angeordnet werden, wie auch in § 50 HGB, § 37 Abs. 2 GmbHG und § 82 Abs. 1 AktG. Sinnvoll wäre es dabei, unterschiedliche, standarisierte Grade der Vollmacht vorzusehen, zwischen denen sich Nutzer entscheiden und die den Assistenten salient, z. B. durch farbliches Coding („Vollmachtsampel"), zugeordnet werden könnten.[410] Besser erscheint es *de lege lata* jedoch, den Schutz des Rechtsverkehrs durch Rechtsscheinstatbestände zu gewährleisten, konkret wie bei der Blanketterklärung[411] durch § 172 Abs. 2 BGB analog.[412]

Dogmatisch vorzugswürdig ist daher das Stellvertretungsregime. Einerseits nimmt es die technische Autonomie des Assistenten ernst und muss die Zurechnung zum Willen des Nutzers nicht mittels einer Fiktion überwinden. Andererseits lassen sich damit auch sachgerechte Lösungen für die seltenen Fälle der Überschreitung der Vollmacht finden. Denn selbst wenn man eine Analogie zu § 172 Abs. 2 BGB ablehnt, liegt eine Erlaubnis der Datenverarbeitung nach Art. 6 Abs. 1 lit. f DS-GVO aus dem Gedanken der sachgerechten Risikoverteilung sehr nahe.[413]

Wie im datenschutzrechtlichen Teil der Arbeit gezeigt, ist eine Stellvertretung bei der Einwilligungserklärung nach hier vertretener Auffassung grundsätzlich zulässig und folgt mangels Vorgaben in der DS-GVO den Regeln nationalen Rechts.[414] Auf diesem Wege lässt sich auch das Problem der *de lege lata* notwendigen Zweckbeschränkung der Einwilligungserklärung lösen. Der Assistent selbst muss eine hinreichend beschränkte Erklärung abgeben. Dies ist etwa durch Bezugnahme auf die in dem IRR hinterlegten Verarbeitungszwecke des jeweiligen IoT-Geräts möglich. Die Zweckbeschränkung ist dann Teil der Erklärung selbst und wirkt analog § 164 Abs. 1 S. 1 BGB für und wider den Nutzer.

Hinsichtlich der Informiertheit der Erklärung ist zu bemerken, dass sich zwar die Kenntnis eines autonomen Assistenten analog § 166 BGB (unter gewissen Umständen) dem Nutzer zurechnen ließe.[415] Allerdings wurde im

---

[408] Vgl. dazu etwa BGH NJW 2006, 2776 (zum Missbrauch der Vertretungsmacht durch GmbH-Geschäftsführer); BGH BB 1976, 852 (zur Evidenz).

[409] Dazu *Sorge*, Softwareagenten, 2006, 61 ff.

[410] *Grundmann/Hacker*, 13 European Review of Contract Law 2017, 255 (283).

[411] Siehe etwa zu den Grundsätzen der Blanketterklärung in diesem Zusammenhang *Sester/Nitschke*, CR 2004, 548 (549 f.); *Groß/Gressel*, NZA 2016, 990 (992); *Specht/Herold*, MMR 2018, 40 (43); *Paulus/Matzke*, ZfPW 2018, 431 (444); kritisch insoweit *Sorge*, Softwareagenten, 2006, 25 f.; *Leyens/Böttcher*, JuS 2019, 133 (135).

[412] Zu dessen Anwendung auf die Blanketterklärung BGH NJW 1963, 1971; BGH NJW 1991, 487 (488).

[413] Vgl. die Ausführungen oben, § 6 E.I.2.c)bb)(2).

[414] Siehe oben, § 5 B.II.2.d).

[415] *Hacker*, RW 9 (2018), 243 (277 ff.).

Rahmen der Ausführungen zur Stellvertretung hinsichtlich der Einwilligungserklärung bereits ausgeführt, dass die Voraussetzungen der Informiertheit der Einwilligung in der Person des Vertretenen selbst vorliegen müssen.[416] Auch hier gilt jedoch wiederum, dass die bloße Möglichkeit der Information genügt, die etwa durch einen Push-Hinweis auf dem Gerät des Nutzers erfolgen kann.

(2) Automatisierter und autonomer Widerspruch gegen bestimmte Formen der Datenverarbeitung, Art. 21 f. DS-GVO

Das zur Einwilligung Gesagte gilt, *mutatis mutandis*, auch für die Widerspruchsrechte nach Art. 21 DS-GVO. Wie die Einwilligungserklärung ist der Widerspruch geschäftsähnliche Handlung, da seine Rechtsfolgen kraft Gesetzes eintreten.[417]

(a) Art. 21 Abs. 2 DS-GVO

Verhältnismäßig klar zu beurteilen ist das Widerspruchsrecht nach Art. 21 Abs. 2 DS-GVO. Danach kann die betroffene Person anlasslos der Verarbeitung personenbezogener Daten zu Zwecken der Direktwerbung widersprechen. Dies betrifft nicht nur unmittelbar an die betroffene Person adressierte Werbung mittels E-Mail oder SMS,[418] sondern nach hier vertretener Auffassung auch mithilfe von Geräte-Identifiern personalisierte Werbung im Onlinebereich.[419] Da der Widerspruch nach Art. 21 Abs. 2 DS-GVO weder dem Zweck nach beschränkt noch informiert abgegeben werden muss, können dafür zumindest alle Techniken verwendet werden, die auch für eine wirksame Einwilligungserklärung genutzt werden können. Zwar wird in der Literatur zum Teil bestritten, dass der https-Header *do not track* einen wirksamen Widerspruch gegen Direktwerbung darstelle.[420] Dies kann jedoch jedenfalls seit Geltungsbeginn der DS-GVO kaum noch bezweifelt werden, wenn der Nutzer die Einrichtung des Headers selbst aktiv vornimmt, zurechenbar durch einen Datenschutzassistenten vornehmen lässt oder selbst eine Voreinstellung bestätigt. Denn eine derartige Einbindung eines *do not track*-Headers ist unmissverständlich auf das Unterlassen von Tracking-Maßnahmen gerichtet.[421]

[416] Siehe oben, § 5 B.II.2.d).

[417] Siehe zur Rechtsnatur der Einwilligung oben, § 5 B.II.1.a); für eine Einordnung des Widerspruchs als einseitige, empfangsbedürftige Willenserklärung *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 21 DS-GVO Rn. 31.

[418] *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 21 DS-GVO Rn. 26.

[419] *Caspar*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 21 DS-GVO Rn. 21; *Helfrich*, in: Sydow, Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 21 Rn. 77; *Tavanti*, RDV 2016, 295 (297 mit Fn. 18); *Piltz*, K&R 2016, 557 (565); wohl auch *Ehmann*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Anhang 3 zu Artikel 6: Datenverarbeitung für Zwecke der Werbung Rn. 18.

[420] Siehe insbesondere *Tavanti*, RDV 2016, 295 (302) und die Nachweise in § 4, Fn. 880.

[421] Streit kann sich allenfalls an der Frage entzünden, ob nur Direktwerbung durch

Jedenfalls die im Rahmen dieser Arbeit interessierenden Formen von Direktwerbung, etwa personalisierte Werbung, ruhen unmittelbar auf Tracking auf.

An der Notwendigkeit, die Einrichtung des automatisierten Widerspruchs zurechenbar aktiv vorzunehmen, ändert jedoch auch Art. 21 Abs. 5 DS-GVO nichts.[422] Danach kann im „Zusammenhang mit der Nutzung von Diensten der Informationsgesellschaft […] die betroffene Person […] ihr Widerspruchsrecht mittels automatisierter Verfahren ausüben, bei denen technische Spezifikationen verwendet werden." Dieser Absatz bestätigt, dass Browser-Spezifikationen zur Einlegung des Widerspruchs verwendet werden können, also auch im Fall von *do not track*;[423] er regelt jedoch nur die Zulässigkeit dieser Form, entscheidet aber nicht über das „Ob" der auch nach diesem Absatz erforderlichen Ausübung des Widerspruchs.[424]

(b) Art. 21 Abs. 1 S. 1 und Abs. 6 DS-GVO

Anders verhält es sich jedoch hinsichtlich des Widerspruchrechts nach Art. 21 Abs. 1 S. 1 DS-GVO. Danach kann die betroffene Person gegen die Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 lit. e oder f DS-GVO Widerspruch einlegen aus Gründen, die sich aus ihrer besonderen Situation ergeben. Diese Gründe müssen jedoch im Einzelfall kommuniziert werden.[425] Dies ist schon allein deshalb erforderlich, damit der Verantwortliche entscheiden kann, ob der Widerspruch nach Art. 21 Abs. 1 S. 2 DS-GVO durch zwingende schutzwürdige Gründe überwunden werden kann, was eine Abwägung mit den für die betroffene Person ausschlaggebenden Gründen notwendig

Drittanbieter oder auch durch Erstanbieter erfasst ist. Rein technisch betrachtet richtet sich *do not track* nur gegen Tracking durch erstere, siehe *Le Métayer*, in: Wright/De Hert (Hrsg.), Enforcing Privacy, 2016, 395 (421). Diese Unterscheidung dürfte den meisten Nutzern jedoch nicht geläufig sein. Letztlich ist daher die Verwendung eines klareren https-Headers (z. B. *do not send ads*) oder die Verwendung eines umfassenden AdBlockers zu empfehlen, die beide klar und unmissverständlich einen Widerspruch gegen Direktwerbung implizieren.

[422] aA *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 21 Rn. 74; *Caspar*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 21 DS-GVO Rn. 35.

[423] *Albrecht*, CR 2016, 88 (93); *Spindler*, DB 2016, 937; *Schantz*, NJW 2016, 1841 (1846); *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 21 DS-GVO Rn. 31; *Herbst*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 21 DS-GVO Rn. 43; *Caspar*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 21 DS-GVO Rn. 33; *Spindler/Dalby*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 21 DS-GVO Rn. 16.

[424] Siehe den Wortlaut von Art. 21 Abs. 2 („einzulegen") und Abs. 5 („ausüben"); ebenso *Kamann/Braun*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018, Art. 21 Rn. 61; wohl auch *Forgó*, in: BeckOK DatenschutzR, 29. Ed. 2018, Art. 21 DS-GVO Rn. 29; *Spindler/Dalby*, in: Spindler/Schuster, Recht der elektronischen Medien, 4. Aufl. 2019, Art. 21 DS-GVO Rn. 16.

[425] *Caspar*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 21 DS-GVO Rn. 7.

macht. Sofern diese für die betroffene Person maßgeblichen Gründe spezifiziert werden, spricht jedoch wiederum nichts gegen eine Verwendung schwach oder stark autonomer Datenschutzassistenten für die Ausübung des Widerspruchs.[426] Lediglich ein pauschaler Widerspruch, etwa in einem https-Header (*do not process based on Art. 6[1][f] GDPR*), wäre unwirksam.[427] Dasselbe gilt für das Widerspruchsrecht nach Art. 21 Abs. 6 DS-GVO, für das ebenfalls besondere situative Gründe angeführt werden müssen.

(c) Art. 22 Abs. 1 DS-GVO

Wie im Fall von Art. 21 Abs. 2 DS-GVO wäre wiederum ein Widerspruch gegen eine automatisierte Entscheidung im Einzelfall nach Art. 22 Abs. 1 DS-GVO zu beurteilen (*do not automatically process*), sofern man in dieser Vorschrift – unzutreffender Weise[428] – lediglich ein Widerspruchsrecht und nicht ein Verbot sieht.[429] Denn selbst wenn man von einem bloßen Widerspruchsrecht ausgeht, wäre dieses jedenfalls ebenso anlasslos wie das nach Art. 21 Abs. 2 DS-GVO gewährt.[430]

(3) Entwicklungsperspektiven

Nach hier vertretener Auffassung sind daher Einwilligungserklärungen, die durch Datenschutzassistenten generiert werden, in weitem Umfang bereits jetzt datenschutzrechtlich zulässig, unabhängig davon, inwieweit Inhalt und Bedingungen der Übermittlung der Erklärungen durch den Nutzer im Einzelnen determiniert oder durch den Assistenten selbstständig erstellt bzw. bewertet werden. Allerdings ist diese Lösung angesichts erheblicher Gegenstimmen in der Literatur keineswegs rechtssicher. Hinzu kommt, dass der Weg über das Stellvertretungsrecht nach hier vertretener Auffassung ins nationale Recht führt und eine interessengerechte unbeschränkbare Außenvollmacht gesetzlich angeordnet werden sollte. Für die künftig bedeutsame Frage der DS-GVO-kompatiblen Nutzung von Datenschutzassistenten wäre daher eine europäische Lösung vorzugswürdig.[431] Gleiches gilt für die umstrittene Frage, inwiefern ein *do not track*-Header einen wirksamen Widerspruch gegen Direktwerbung dar-

[426] Vgl. *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 21 DS-GVO Rn. 36.

[427] Vgl. *Caspar*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 21 DS-GVO Rn. 7 (unspezifische Einwände nicht ausreichend); zweifelnd *Forgó*, in: BeckOK DatenschutzR, 29. Ed. 2018, Art. 21 DS-GVO Rn. 28.

[428] *Buchner*, in: Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 22 DS-GVO Rn. 12; *Martini*, in: Paal/Pauly, DS-GVO BDSG, 2. Aufl. 2018, Art. 22 Rn. 29; zum internationalen Schrifttum und Begründung des Verbotscharakters *Hacker*, 7 International Data Privacy Law 2017, 266 (275 Fn. 7).

[429] *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 22 DS-GVO Rn. 5.

[430] Vgl. *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 22 DS-GVO Rn. 5, wonach das Widerspruchsrecht nicht einmal aktiv ausgeübt werden muss.

[431] So im Ergebnis auch *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 7 DS-GVO Rn. 71.

stellen kann, wenn er in die Voreinstellungen eines Browsers standardmäßig integriert ist und nicht aktiv durch den Nutzer bestätigt wurde. Die ePrivacy-Verordnung bietet sich für diese Fragen als einziger in näherer Zukunft realistisch denkbarer Regelungsort an.

Die bisherige Regelung in Art. 9 Abs. 2 des Kommissionsentwurfs der ePrivacy-Verordnung ist jedoch noch nicht hinreichend.[432] Danach wird lediglich festgestellt, dass eine nach der ePrivacy-Verordnung erforderliche Einwilligung (zum Beispiel in Geräte-Identifier) auch durch Browser-Einstellungen gegeben werden kann. Damit ist jedoch weder die Frage des passiven Belassens der Voreinstellungen noch die Zurechnung von Erklärungen, die durch Datenschutzassistenten außerhalb von Browser-Spezifikationen gegeben werden, beantwortet. Sinnvoll erscheint hier zweierlei: Erstens sollte klargestellt werden, dass Einwilligungserklärungen auch durch Datenschutzassistenten, unabhängig von ihrem Autonomiegrad, abgegeben werden können, und dass an die Bestimmtheit und Informiertheit dieser technisch unterstützten Einwilligungserklärungen keine hohen Anforderungen gestellt werden können. Nur so lässt sich wenigstens eine Schwundstufe individueller Datensouveränität erhalten. Zweitens sollte verankert werden, dass auch die passive Hinnahme von Datenschutz-Voreinstellungen in Browser-Spezifikationen als Widerspruch im Sinne von Art. 21 Abs. 2 DS-GVO gedeutet werden muss. Dies entspricht dem in Art. 25 Abs. 2 DS-GVO enthaltenen Gebot datenschutzfreundlicher Voreinstellungen,[433] das in diesem Bereich nur so mit Leben gefüllt werden kann.

bb) Interoperabilität durch Datenschutz-Schnittstelle

Ein zweiter Bereich, in dem rechtliche Reformen notwendig sind, ist die Frage der Interoperabilität von Datenschutzassistenten und datenverarbeitenden Geräten, Diensten und Applikationen. Wie gesehen ist die Verwendung von Datenschutzassistenten unumgänglich für die Ausübung residualer Datensouveränität in vernetzten Umgebungen. Allerdings ist für die Kommunikation zwischen datenverarbeitenden Geräten, Diensten oder Applikationen einerseits und Datenschutzassistenten andererseits eine Zugriffsmöglichkeit letzterer auf erstere notwendig. Daran mangelt es jedoch gerade im Internet der Dinge gegenwärtig noch häufig. Sowohl für die Herstellung von Transparenz als auch die Konfiguration von datenverarbeitenden Geräten nach Maßgabe der Nutzervorgaben muss eine interoperable Datenschutz-Schnittstelle (API)[434] daher verbindlich sein und nach Möglichkeit technisch standardisiert werden, damit ein Datenschutzassistent auf alle relevanten Applikationen zugreifen

[432] Dazu bereits oben, § 4 B.I.4.c)aa).

[433] Aus diesem Grund bereits *de lege lata* für einen wirksamen Widerspruch durch unbestätigte *do not track*-Voreinstellungen *Caspar*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 21 DS-GVO Rn. 35.

[434] Zum Begriff der API oben, § 4, Fn. 1118.

kann.[435] Die technischen und rechtlichen, insbesondere kartellrechtlichen,[436] Details der Standardisierung müssen allerdings einer gesonderten Untersuchung vorbehalten bleiben. Dass die Bereitstellung einer Schnittstelle technisch und rechtlich durchführbar ist, zeigt jedoch das Gebot einer Schnittstelle für Zahlungsdienstleistungsapplikationen in der PSD 2-Richtlinie[437] (Art. 66 Abs. 1, 67 Abs. 1 PSD 2-Richtlinie, § 675f Abs. 3 BGB, § 48 ZAG).[438]

Im Bereich des Internets der Dinge erscheint eine Datenschutz-Schnittstelle mindestens ebenso grundlegend wie eine Zugangsmöglichkeit für Drittdienstleister im Zahlungsverkehr. Dabei geht es im datenschutzrechtlichen Bereich nicht darum, die Möglichkeit zu schaffen, Datenschutzpräferenzen von betroffenen Personen in jedem Einzelfall durchzusetzen; dies widerspräche Art. 6 Abs. 1 lit. c-f DS-GVO. Die Existenz einer Schnittstelle ist jedoch Voraussetzung dafür, dass die Präferenzen überhaupt wirksam kommuniziert werden können. Der Inhaber des datenverarbeitenden Gerätes, Dienstes oder der Applikation muss dann innerhalb des geltenden rechtlichen Rahmens entscheiden, inwiefern er diese Präferenzen honorieren möchte.

Dies lässt sich abschließend am Besuch eines Gasts in einem Smart Home veranschaulichen. So mag die Türklingel mit einer Kamera ausgestattet sein, die dem Hausbesitzer durch die Verwendung von Gesichtserkennungssoftware melden kann, welcher Gast vor der Tür steht. Der Datenschutzassistent würde der Kamera über die Datenschutz-Schnittstelle automatisiert signalisieren, ob der Inhaber des Assistenten der Gesichtserkennung zustimmt oder nicht.[439] In besonders dringenden Fällen, etwa zur Verhinderung von strafrechtlich relevanten Handlungen, könnte der Hausbesitzer eine Gesichtserkennung entgegen den Präferenzen des (ungebetenen) Gastes autorisieren. Im Wohnzimmer des Hauses wiederum kann der Datenschutzassistent den *smart speakers* des Hausherrn kommunizieren, dass die Stimme des Gastes für Aufnahmen tabu ist, in der Küche dafür sorgen, dass der *smart fridge* nicht den Konsum alkoholischer Getränke durch den Gast erfasst. Die Beispiele ließen sich beliebig erweitern. Sie zeigen einmal mehr: Nur durch derartig automatisierte Kom-

---

[435] Vgl. *Datenethikkommission*, Gutachten der Datenethikkommission, 2019, 133; *Alpers et al.*, 3rd IEEE International Conference on Computer and Communications (ICCC) 2017, 1460 (1466); *Stiftung Datenschutz*, Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, 2017, 23; *Hall/Hans/Henry*, Comments for November 2013 Workshop on the „Internet of Things" (1.6.2013), https://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00028-86211.pdf, 4.

[436] Siehe etwa *Koenig/Neumann*, WuW 2009, 382; *Weck*, NJOZ 2009, 1177 (1184 ff.).

[437] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG, ABl. 2015 L 337/35.

[438] Dazu etwa *Zahrte*, NJW 2018, 337 (338, 341); *Schmalenbach*, in: BeckOK BGB, 51. Ed. 2019, § 675f Rn. 50.

[439] Vgl. die Anwendungen in *Das et al.*, 17(3) IEEE Pervasive Computing 2018, 35 (40, 44).

munikation lässt sich in einer zunehmend vernetzten Welt ein gewisser Grad der Souveränität über die Verwendung der eigenen Daten erhalten.

4. Zusammenfassung zur Verbesserung der Einwilligung und der Präferenzkommunikation

Die verschiedenen zur Verbesserung des Einwilligungsregimes diskutierten Strategien belegen, dass es zur Unterstützung informierter und autonomer Entscheidungen im Bereich datenbasierter Austauschprozesse kein Allheilmittel gibt.[440] Vielmehr müssen unterschiedliche Maßnahmen ineinandergreifen, damit verschiedene Typen von Marktversagen adressiert werden können. Insoweit lassen sich transparenzbasierte, verhaltensbasierte und technologiebasierte Ansätze unterscheiden. Übergreifend lässt sich jedoch konstatieren: Die informierte Einwilligung muss von der *technologischen Einwilligung* abgelöst werden, in deren Rahmen Techniken maschinellen Lernens den Einwilligenden unterstützen.

a) Bewertung der verschiedenen Ansätze

Transparenzbasierte Ansätze sollen Informationen einfacher und wirksamer an einzelne Nutzer vermitteln durch eine bewusste Gestaltung der Pflichtinformationen selbst. Dadurch soll Informationsasymmetrie und Informationsüberlastung entgegengewirkt werden. Empirische Erhebungen zeigen jedoch, dass hier lediglich inkrementelle Verbesserungen zu erwarten sind. Zwar können etwa mit Mehrebenen-Datenschutzerklärungen, einer Kurzzusammenfassung der Datenschutzerklärung auf einer Seite (One-Pager), mit Icons oder Warnhinweisen die Informationen gebündelt und kognitiv optimiert werden. Sie wirken empirisch bislang jedoch nur in geringem Umfang, da die Nutzer trotz kognitiver Optimierung die Informationen kaum zur Kenntnis nehmen. Es zeigt sich bei vielen Nutzern eine persistente Präferenz, möglichst wenig mit Informationen über Einwilligungserklärungen belästigt zu werden. Transparenzbasierte Ansätze wirken sich daher positiv lediglich für eine verschwindende Minderheit sowie für Dritte aus, die Informationen als Intermediäre aufbereiten oder zur Durchsetzung des Datenschutzrechts berufen sind. Insofern macht es Sinn, diese Ansätze weiterzuentwickeln, auch wenn der Effekt für den Großteil der Nutzer gering sein wird.

Bereits hier zeigt sich, dass es zum Teil sinnvoll ist, unterschiedliche Wege zu beschreiten für Nutzer mit heterogen ausgeprägten Datenschutzpräferenzen. Dies gilt insbesondere für das Timing von Pflichtinformationen. Hier lassen sich empirisch tatsächlich erhebliche Effekte auf die Informiertheit der Nutzer feststellen. Jene Nutzer mit hohen Datenschutzpräferenzen sollten daher die Möglichkeit erhalten, Just-in-time-Hinweise zu erhalten und Just-in-time-

[440] Vgl. *Calo*, 82 George Washington Law Review, 2014, 995 (1048).

Einwilligungen zu erteilen. Alle anderen jedoch sollten von hochfrequenten Hinweisen verschont bleiben.

Neben den transparenzbasierten stehen die verhaltensbasierten Ansätze. Sie schöpfen ihre Legitimation nicht lediglich, wie man meinen könnte, aus der Reduzierung von kognitiven Verzerrungen, sondern auch aus der Minimierung negativer Externalitäten. Diese Ansätze umfassen ein weites Spektrum von *privacy nudges* bis hin zu *debiasing*. Besonders prominent ist der Grundsatz von *privacy by design*, der sich nun in spezifischer Form auch in Art. 25 DS-GVO wiederfindet. Damit können insgesamt die Menge an veröffentlichten Informationen und in der Folge auch negative Externalitäten der Datenverarbeitung vermindert werden. Vor der Implementierung von – davon zu unterscheiden – *debiasing*-Strategien, die zumindest theoretisch verhaltensökonomische Effekte reduzieren können, sind jedoch umfangreiche empirische Tests notwendig. Für das im Rahmen dieses Kapitels zentral verfolgte Ziel, informierte und autonome Entscheidungen zu stärken, sind schließlich all jene Maßnahmen wenig brauchbar, die auf intransparenten Lenkungseffekten basieren.

Von herausragender Bedeutung für die partielle Rückgewinnung von Datensouveränität sind schließlich technologiebasierte Ansätze wie etwa ein Datenschutz-Dashboard oder (personalisierte) Datenschutzassistenten. Diesen Unterstützungswerkzeugen gehört mit großer Wahrscheinlichkeit die Zukunft: Dadurch lässt sich nicht nur Transparenz herstellen, sondern auch die aktive Durchsetzung von Datenschutzpräferenzen zentralisieren oder sogar schrittweise automatisieren. Besonders vielversprechend sind dabei Datenschutzassistenten, welche die Präferenzen der Nutzer adaptiv modellieren und so nur noch ein Minimum an Eigeninitiative der Nutzer erfordern. Diese technologiebasierten Ansätze müssen aber rechtlich begleitet werden, um ihre volle Wirksamkeit zu entfalten.

b) Rechtlicher Reformbedarf

Insgesamt zeigt sich bei den verschiedenen Ansätzen rechtlicher Reformbedarf in unterschiedlicher Ausprägung. Bei den transparenzbasierten Techniken ist dieser überschaubar, da nach hier vertretener Auffassung viele Strategien bereits jetzt durch Art. 12 DS-GVO geboten sind. Nachbesserungsbedarf besteht vor allem bei einem obligatorischen One-Pager sowie bei der Möglichkeit der Auswahl von Just-in-time-Hinweisen und -Einwilligungen. Hinsichtlich der verhaltensbasierten Ansätze besteht gegenwärtig kaum Reformbedarf, da Datenschutz durch Technikgestaltung und Voreinstellungen bereits in Art. 25 DS-GVO verankert ist und für weitere Maßnahmen zunächst empirische Tests erforderlich wären.

Deutlich höherer Reformbedarf besteht hingegen bei den technologiebasierten Ansätzen. Hier stechen zwei Desiderate heraus: Erstens muss die automatisierte Kommunikation von Datenschutzpräferenzen, insbesondere durch

Datenschutzassistenten, die selbstständig Erklärungen erstellen und übermitteln, rechtssicher gestaltet werden. Nach hier vertretener, in der Literatur aber umstrittener Auffassung ist dies bereits jetzt unter dem Regime der DS-GVO weitestgehend möglich. Es würde Sinn und Zweck der Verordnung nachgerade auf den Kopf stellen, wenn diejenige Form der Kommunikation von Präferenzen, die am ehesten eine residuale Form der Nutzerkontrolle gewährleistet, an Vorschriften zum vermeintlichen Schutze der Nutzer selbst scheitern würde. Nichtsdestoweniger sollte hier eine europäische Lösung gefunden werden, bei der insbesondere auch die Möglichkeit des Widerspruchs nach Art. 21 DS-GVO durch voreingestellte Spezifikationen gewährleistet sein muss. Die Vorschläge der ePrivacy-Verordnung gehen insoweit noch nicht weit genug.

Zweitens ist die Kommunikation von Datenschutzpräferenzen auf einen sicheren Kommunikationskanal zwischen Datenschutz-Dashboards oder -Assistenten einerseits und datenverarbeitenden Geräten, Diensten oder Applikationen andererseits angewiesen. Der Zugriff auf letztere muss daher durch eine verpflichtende, standardisierte Datenschutz-Schnittstelle gewährleistet werden.

Insgesamt spricht daher vieles dafür, sich vom Primat der individuellen, informierten Einwilligung zu lösen und die rechtlichen Grundlagen für eine technologische, personalisierte Mastereinwilligung zu legen, die im Einzelfall durch den Nutzer spezifiziert werden kann, aber nicht muss. Zuletzt ist jedoch zu konstatieren, dass verbesserte Transparenz und Kommunikation von Präferenzen immer nur dann neue Möglichkeiten zur Verwirklichung bestimmter Datenschutzpräferenzen eröffnen, wenn darauf abgestimmte Leistungen von Anbietern auch zur Verfügung gestellt werden. Dem widmet sich der folgende, letzte Abschnitt dieses Kapitels.

II. Verbesserung reeller Wahlmöglichkeiten: Das Recht auf eine datenschonende Option

Durch die am Ende des vorangegangenen Abschnitts diskutierten technologiebasierten Ansätze lassen sich Datenschutzpräferenzen effektiv kommunizieren. Durchgesetzt werden können diese jedoch nur, sofern durch den jeweiligen Anbieter entsprechende Wahlmöglichkeiten vorgesehen sind. Genau daran mangelt es jedoch gegenwärtig bei vielen datenverarbeitenden Geräten, Diensten und Applikationen. Empirische Studien zeigen insbesondere, dass auch diejenigen Apps, die monetär bezahlt werden, häufig in ähnlicher Weise Daten erheben und verarbeiten wie monetär kostenfreie Apps.[441]

[441] *Bamberger et al.*, 35 Berkeley Technology Law Journal 2020 (im Erscheinen); tendenziell invasivere Datenverarbeitung durch monetär kostenlose Apps stellen hingegen *Kummer/Schulte* 65 Management Science 2019, 3470 (3480) fest.

1. Grundidee: Datenschonende Option und privacy score

Daher mehren sich in der Literatur die Stimmen, die ein Recht der Nutzer auf eine datenschonende Vertrags- oder Nutzungsoption befürworten, in deren Rahmen nur die absolut vertraglich oder technisch notwendigen Daten verarbeitet werden.[442] Auch der Verfasser hat dies bereits an anderer Stelle angeregt.[443] Im Rahmen des folgenden Abschnitts sollen diese Überlegungen aufgegriffen und zugleich in zweifacher Hinsicht entscheidend fortentwickelt werden: erstens durch die Verbindung der Wahlmöglichkeit einer datenschonenden Option mit einem verpflichtenden *privacy score*, der zu einer Vergleichbarkeit des Datenpreises unterschiedlicher Optionen führt; und zweitens durch die sektorspezifische Beschränkung des Rechts auf eine datenschonende Option, welche die Vorrangigkeit der Bereitstellung solcher Optionen durch den Markt unterstreicht. Erst durch diese zusätzlichen rechtlichen Stützmechanismen wird aus dem im vorigen Abschnitt entwickelten Recht der Präferenzkommunikation ein effektives Datenermöglichungsrecht.

Bevor die Grundzüge des hier unterbreiteten Vorschlags (b)) und die dafür sprechenden Argumente (c)) vorgestellt werden, muss jedoch noch präzisiert werden, inwiefern in diesem Bereich überhaupt rechtlicher Reformbedarf besteht (a)).

a) Datenschonende Option *de lege lata* und *de lege ferenda*

Nach der im vierten Kapitel dieser Arbeit vertretenen Auffassung folgt die Notwendigkeit, eine zumutbare datenschonende Option anzubieten, be-

[442] *Traung*, CRi 2012, 33 (42); *Novotny/Spiekermann*, Personal Information Markets AND Privacy: A New Model to Solve the Controversy, in: Hildebrandt et al. (Hrsg.), Digital Enlightenment Yearbook 2013, 2013, 102 (107 f.); *Strandburg*, University of Chicago Legal Forum, 2013, 95 (170); *Irion/Luchetta*, Online Personal Data Processing and EU Data Protection Reform, CEPS Task Force Report, 2013, 38; *Hoofnagle/Whittington*, 61 UCLA Law Review 2014, 606 (661 f.); *Calo*, 82 George Washington Law Review, 2014, 995 (1047 f.); *Monopolkommission*, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015, Rn. 338; *Kerber*, GRUR Int. 2016, 639 (644); *European Data Protection Supervisor*, EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), Opinion 6/2017, 2017, 17; *Becker*, JZ 2017, 171 (175 ff.); siehe auch *Jarovsky*, 4 European Data Protection Law Review 2018, 447 (456 f.); *Ezrachi/Stucke*, Is Your Digital Assistant Devious?, Oxford Legal Studies Research Paper No. 52/2016, University of Tennessee Legal Studies Research Paper No. 304, https://ssrn.com/abstract=2828117, 20 (bei persönlichen digitalen Assistenten); *Metzger*, in: Festschrift Basedow, 2018, 131 (137 f.); *Wagner/Eidenmüller*, 86 University of Chicago Law Review 2019, 581 (605 ff.) (*right to anonymity*); *Gal*, 25 Michigan Technology Law Review 2018, 59 (95 f.) (*stop button* für persönliche digitale Assistenten); kritisch zu einem Recht auf eine datenschonende Option *Malgieri/Custers*, 34 Computer Law & Security Review 2018, 289 (297 f.); *Härting*, CR 2016, 646 (648 f.); *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 7 DS-GVO Rn. 30; tendenziell als zu als wenig weitgehend bewertet von *Zuiderveen Borgesius*, in: Alemanno/Sibony (Hrsg.), Nudge and the Law: A European Perspective, 2015, 179 (201 f.).

[443] *Hacker/Petkova*, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1 (20 ff.); *Hacker*, 7 International Data Privacy Law 2017, 266 (280 ff.).

reits in weiten Teilen aus der Auslegung von Art. 7 Abs. 4, Art. 6 Abs. 1 lit. b und f DS-GVO. Denn eine Einwilligung in die Verarbeitung nicht vertragserforderlicher Daten scheitert danach, sofern keine vergleichbaren Angebote am Markt bestehen, am Kopplungsverbot des Art. 7 Abs. 4 DS-GVO.[444] Jedenfalls für den Fall personalisierter Werbung scheidet danach weiterhin eine Rechtfertigung nach Art. 6 Abs. 1 lit. f DS-GVO in der Regel aus.[445] Ferner sind Nutzerpflichten für Art. 6 Abs. 1 lit. b DS-GVO irrelevant[446] und artifiziell weite Leistungspflichten des Verantwortlichen, die grundsätzlich datenschutzrechtlich beachtlich wären, scheitern in der Regel an der AGB-Kontrolle.[447] Daher lässt sich eine datenschutzrechtskonforme Verarbeitung von Daten, die nicht für die Erfüllung der Leistungspflichten des Anbieters erforderlich sind, in der Regel nur über eine Einwilligung gewährleisten, hinsichtlich derer das Kopplungsverbot durch das Bestehen von datenschonenden Alternativen, die durch den Anbieter selbst oder funktional vergleichbare andere Anbieter gewährt werden, ausgeschaltet wurde. Durch diese Schlusskette wird mittelbar bereits *de lege lata* ein Recht auf eine datenschonende Option etabliert.

Allerdings sind die einzelnen Glieder dieser Schlusskette in hohem Maße umstritten und mit rechtlicher Unsicherheit behaftet. Zudem hat sich diese Sichtweise unter den Anbietern gegenwärtig noch nicht mehrheitlich durchgesetzt. Schließlich umfasst die gegenwärtige Rechtslage jedenfalls nicht die Etablierung eines *privacy score*. Daher erscheint es sinnvoll, auf europäischer Ebene, zum Beispiel im Rahmen der ePrivacy-Verordnung, ein subjektives Recht auf eine datenschonende Option, gekoppelt mit der Ausweisung eines *privacy score*, explizit zu verankern.[448] Damit muss eine objektiv-rechtliche Pflicht der erfassten Anbieter zum Angebot einer derartigen Option korrespondieren, die auch durch Aufsichtsbehörden durchgesetzt und sanktioniert werden kann.[449] Ferner bedarf es einer Klagebefugnis von qualifizierten Einrichtungen, wie auch sonst im Bereich des Datenschutzrechts.[450]

b) Grundlegender Inhalt des Vorschlags: Drei Weichenstellungen

Der hier unterbreitete Vorschlag enthält drei zentrale Weichenstellungen, die im weiteren Verlauf der Untersuchung genauer expliziert werden.

---

[444] Siehe oben, § 4 B.I.3.a)dd)(6).
[445] Siehe oben, § 4 C.I.5.
[446] Siehe oben, § 4 B.II.2.b)bb).
[447] Siehe oben, § 5 C.II.1.cc)(1)(b)(cc).
[448] Siehe auch *European Data Protection Supervisor*, EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), Opinion 6/2017, 2017, 17.
[449] Vgl. *Becker*, JZ 2017, 171 (179).
[450] Siehe § 2 Abs. 1 S. 1 i. V. m. Abs. 2 S. 1 Nr. 11, § 3 UKlaG.

aa) Pflichtangebot der datenschonenden Option

Erstens werden erfasste Anbieter verpflichtet, zumindest eine datenschonende Option anzubieten. In der Praxis wird dies regelmäßig darauf hinauslaufen, dass Anbieter mindestens zwei Vertrags- oder Nutzungsoptionen zur Verfügung stellen: eine datenschonende und eine datenintensive. Die datenintensive Option entspricht im Wesentlichen den gegenwärtigen monetär kostenfreien Angeboten, bei denen die Bezahlung im ökonomischen Sinne über Daten erfolgt. Auch für diese Option gilt das bestehende Datenschutzrecht unverändert fort. Hinsichtlich der datenschonenden Option dürfen die Anbieter jedoch nur bestimmte, technisch erforderliche Datenverarbeitungen vornehmen.[451] Eine Erlaubnis nach Art. 6 Abs. 1 lit. a, b und f DS-GVO ist damit ausgeschlossen.[452] Würde man insbesondere den Rückgriff auf die Einwilligung nach Art. 6 Abs. 1 lit. a DS-GVO nicht sperren, so stünde zu befürchten, dass manche Anbieter die Nutzer unmittelbar nach Wahl der datenschonenden Option mit Einwilligungsersuchen konfrontieren, die ein signifikanter Teil angesichts rationaler Ignoranz, Informationsüberlastung, verhaltensökonomischer oder persuasiver Effekte annehmen würde,[453] so dass auf diesem Weg die Wirkung der datenschonenden Option konterkariert würde. Für die Nutzung einer personalisierten Produkterfahrung müssen Nutzer stattdessen grundsätzlich in die datenintensive Option wechseln.[454] Lediglich eine Anpassung des Designs auf persönliche Bedürfnisse (z. B. Schriftgröße) und eine dahingehende Speicherung und Verarbeitung von Daten sollte auch in der datenschonenden Option möglich sein.[455] Sofern in deren Rahmen eine weitergehende Datenverarbeitung vorgenommen wird, muss dies einem DS-GVO-Verstoß gleichgestellt werden, mit den üblichen Sanktionsfolgen. Die Bezahlung erfolgt dann in dieser Option ganz überwiegend monetär.

bb) Verbindung mit *privacy scores*

Zweitens müssen alle Optionen mit EU-weit vereinheitlichten *privacy scores* versehen werden. Damit wird die Höhe des datenschutzrechtlichen Risikos mit einem Blick, zum Beispiel durch eine Zahl zwischen null und 100, erfassbar. Die Verwendung derartiger Scores sollte, nach eingehenden empirischen Tests, ebenfalls vereinheitlicht und zwingend ausgestaltet werden. Wie der effektive Jahreszins bei der Kreditvergabe können sie einen erheblichen Beitrag zur Preistransparenz leisten, da, wie gesehen, die Möglichkeit der Datenverarbei-

[451] Dazu genauer unten, § 6 C.II.3.a).

[452] Art. 6 Abs. 1 lit. c-e DS-GVO stünden damit weiterhin als Erlaubnistatbestände zur Verfügung, um gesellschaftlich oder im Einzelfall individuell besonders dringliche Formen der Verarbeitung zu ermöglichen; vgl. *Becker*, JZ 2017, 171 (177).

[453] *Willis*, 29 Berkeley Technology Law Journal 2014, 61 (111 ff.).

[454] Siehe unten, § 6 C.II.5.c).

[455] Siehe unten, § 6 C.II.3.a)bb).

tung regelmäßig einen (zusätzlichen) Produktpreis darstellt.[456] Solange keine verlässlichen, vereinheitlichten Scores existieren, muss zumindest ein Link auf einen Datenschutz-One-Pager für jede Option aufgenommen werden.[457]

cc) Sektorspezifizität

Drittens werden diese beiden Verpflichtungen, zum Angebot einer datenschonenden Option und zur Ausweisung eines *privacy scores*, sektorspezifisch etabliert. Voraussetzung ist, dass in einem bestimmten Wirtschaftssektor keine hinreichenden datenschutzfreundlichen Modelle am Markt verfügbar sind, sodass Nutzer mit stark ausgeprägten Datenschutzpräferenzen keine Möglichkeit zur Verwirklichung ihrer Präferenzen haben.

c) Argumente

Für diese Ausgestaltung sprechen vier Argumente, die sich aus den bisherigen Ergebnissen zu heterogenen Datenschutzpräferenzen und den unterschiedlichen Typen von Marktversagen bei digitalen Austauschprozessen speisen.[458]

aa) Marktergänzende Alternativen zur Durchsetzung von Datenschutzpräferenzen

Erstens schaffen verbesserte Information (transparenzbasierte Ansätze), Handlungslenkung (verhaltensbasierte Ansätze) und klarere Kommunikation von Datenschutzpräferenzen (technologiebasierte Ansätze) keine Möglichkeiten zur Durchsetzung von Datenschutzpräferenzen. Sie schaffen keine vertraglichen Alternativen.[459] Einfach auszuwählende, datenschonende Optionen sind jedoch heute, jedenfalls in vielen zentralen Bereichen der digitalen Wirtschaft, nicht anzutreffen.[460] Dies liegt auch daran, dass Datenschutz in vielen Sektoren (noch) kein wirksamer Wettbewerbsparameter ist.[461]

---

[456] Siehe oben, § 3 A.II.

[457] Zum One-Pager oben, § 6 C.I.1.a)aa)(2).

[458] Siehe zu den Typen von Marktversagen oben, § 3 B.II.1.

[459] *Worms/Gusy*, DuD 2012, 92 (97); *Becker*, JZ 2017, 171 (175); *Hacker*, 7 International Data Privacy Law 2017, 266 (281).

[460] *Warner/Sloan*, 15 Vanderbilt Journal of Entertainment and Technology Law 2012, 49 (59 f.); *Strandburg*, University of Chicago Legal Forum, 2013, 95 (164 f.); *Custers et al.*, 10 SCRIPTed 2013, 435 (456 f.); *European Data Protection Supervisor*, Opinion on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data, Opinion 9/2016, 2016, 13 f.; *Becker*, JZ 2017, 171 (174); *Botta/Wiedemann*, The Antitrust Bulletin 2019, 428 (432); vgl. auch *Künzler*, Direct Consumer Influence – The Missing Strategy to Integrate Data Privacy Preferences into the Market, Working Paper, 2019, https://ssrn.com/abstract=3395928, 7; siehe dazu noch unten, § 6 C.II.4.

[461] *Warner/Sloan*, 15 Vanderbilt Journal of Entertainment and Technology Law 2012, 49 (60 f., 63 f.); *Autorité de la Concurrence/Bundeskartellamt*, Competition Law and Data, Joint Report (10.5.2016), 24 f.; *Kerber*, GRUR Int. 2016, 639 (642); *Botta/Wiedemann*, The Antitrust Bulletin 2019, 428 (433).

Dieser empirische Befund wird gestützt durch spieltheoretische Analysen: Wenn Anbieter antizipieren, dass nur wenige Nutzer eine Einwilligung in weitreichendere Datenverarbeitung ablehnen, stellt das Angebot einer *take it or leave it*-Option mit weitreichender Datenverarbeitung die dominante Strategie dar (einseitiges Feiglingsspiel, *hawk-dove game*).[462] Denn die wenigen Nutzer, die diese Option ablehnen, generieren nicht hinreichende Opportunitätskosten, als dass ein zweispuriges System der Datenverarbeitung (für solche mit hohen und solche mit niedrigen Datenschutzpräferenzen) sich für Anbieter lohnen würde.[463] Die Nutzer wissen daher, dass die Anbieter nicht einknicken werden, und müssen selbst strategisch einlenken (in die Datenverarbeitung einwilligen), wenn sie in den Genuss der Leistung kommen wollen.

In der Konsequenz bedeutet dies, dass heterogene Datenschutzpräferenzen nur äußerst ungleich befriedigt werden: Jene mit wenig ausgeprägten Präferenzen erhalten passende, datenintensive Angebote, bei denen sie ihre Daten zur Budgeterweiterung einsetzen können. Jene mit stark ausgeprägten Präferenzen jedoch finden, zumindest in vielen Bereichen, keine adäquaten Angebote zur Verwirklichung ihrer Präferenzen am Markt vor. Nun gibt es sicherlich kein grundsätzliches Recht darauf, alle eigenen Präferenzen lückenlos durch marktgängige Angebote abgedeckt zu sehen. Hinsichtlich stark ausgeprägter Datenschutzpräferenzen werden diese subjektiven Interessen jedoch entscheidend verstärkt durch das Datenschutzgrundrecht, das, wie gesehen,[464] auch horizontale Wirkung entfaltet. Dies verleiht den auf das Angebot datenschonender Optionen gerichteten Präferenzen ein besonderes Gewicht und streitet letztlich auch in der Abwägung mit den Grundrechten der Anbieter für datenschonende Optionen.[465] Besonders greifbar wird deren Dringlichkeit im Rahmen der zunehmenden Vernetzung des Internets der Dinge: Wie gesehen ist die Datenerhebung dort in steigendem Maße durch Unentrinnbarkeit gekennzeichnet.[466] Verzicht ist dann keine Handlungsalternative mehr. Insoweit erscheint die gesetzliche Verankerung einer datenschonenden Option in vielen Bereichen der digitalen Wirtschaft unumgänglich, wenn auch stark ausgeprägte Datenschutzpräferenzen honoriert werden sollen. Nur so kann letztlich heterogenen Datenschutzpräferenzen Genüge getan werden.[467]

---

[462] *Warner/Sloan*, 15 Vanderbilt Journal of Entertainment and Technology Law 2012, 49 (61 ff.); *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 170 ff., 383; *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 16; optimistischer hinsichtlich möglicher Anreize zur Bereitstellung von datenschutzfreundlichen Alternativen *Hetcher*, Norms in a Wired World, 2004, 299 f. (Analyse als wiederholtes Gefangenendilemma).

[463] *Warner/Sloan*, 15 Vanderbilt Journal of Entertainment and Technology Law 2012, 49 (63 f.); *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 172. Dies würde sich ändern, wenn die Nutzer Tracking verhindern und zugleich Angebote (dann völlig kostenlos) nutzen könnten, *Warner/Sloan*, 15 Vanderbilt Journal of Entertainment and Technology Law 2012, 49 (78 ff.). Genau dies jedoch verhindern *tracking walls*.

[464] Siehe oben, Text bei § 5, Fn. 1075.

[465] Dazu genauer unten, § 6 C.II.6.

[466] Siehe oben, § 3 B.II.2.b).

[467] Vgl. *Kerber*, GRUR Int. 2016, 639 (644).

bb) Rechtssicherheit für Anbieter und Nutzer mit niedrigen Datenschutzpräferenzen

Die Einrichtung derartiger Optionen kommt jedoch nicht nur Nutzern mit signifikanten Datenschutzpräferenzen zugute. Vielmehr profitieren auch die Anbieter und Nutzer mit schwach ausgeprägten Datenschutzpräferenzen mittelbar, da das Kopplungsverbot des Art. 7 Abs. 4 DS-GVO tatbestandlich ausgeschaltet wird, weil die Vertragserfüllung dann nicht mehr von der Einwilligung in die Verarbeitung nicht vertragserforderlicher Daten *abhängig* ist.[468] Die datenschonende Option hebt die Kopplung zwischen Vertragserfüllung und Einwilligung gerade auf. Dies schafft Rechtssicherheit für Anbieter und für Nutzer mit schwach ausgeprägten Datenschutzpräferenzen hinsichtlich der datenintensiven Option,[469] die gerade bei der Auslegung des hochumstrittenen Kopplungsverbots andernfalls in weiter Ferne ist. Damit vermag das Recht auf eine datenschonende Option die beiden wichtigsten Pole heterogener Datenschutzpräferenzen rechtlich abzubilden.

cc) Aktive Wahl statt rationaler Ignoranz

Drittens lässt sich die für digitale Austauschprozesse bislang kennzeichnende rationale Ignoranz von Umständen der Datenverarbeitung durch die datenschonende Option reduzieren.[470] Denn die Anbieter sollten durch die regulatorische Vorgabe verpflichtet werden, eine saliente Wahlmöglichkeit in Form einer *active choice* zur Verfügung zu stellen.[471] Ähnlich wie die im Kontext des regulatorischen Rahmens für das Internet der Dinge diskutierten Pflichten, über die Verwendung von Daten als Gegenleistung explizit und salient zu informieren,[472] würde auch eine aktive Wahl das Bewusstsein für die Nutzung von Daten als Gegenleistung signifikant erhöhen. Bei erstem Aufruf des Dienstes oder der Applikation bzw. Installation des Gerätes[473] müsste sich der Nutzer daher aktiv zwischen der datenschonenden und der datenintensiven Option, sofern eine solche angeboten wird, entscheiden. Bislang bestand hier lediglich die Dichotomie von *tracking by default* oder *privacy by default*.[474] Gegenüber einer derartigen, einheitlichen, dispositiven Regelung jedoch er-

468 Siehe oben, § 4 B.I.3.a)dd)(3)(b)(bb).
469 Siehe auch *Hacker*, 7 International Data Privacy Law 2017, 266 (281).
470 Siehe auch *Hacker*, 7 International Data Privacy Law 2017, 266 (281).
471 Zu *active choice* allgemein *Sunstein*, 64 Duke Law Journal 2014, 1 (28 ff.); *Sunstein*, Choosing not to Choose, 2015, 113 ff.; *Hacker*, Verhaltensökonomik und Normativität, 2017, 488 ff.
472 *Wendehorst*, in: Schulze/Staudenmayer (Hrsg.), Digital Revolution. Challenges for Contract Law in Practice, 2016, 189 (207 f.). Diese Pflichten alleine schaffen aber noch keine vertraglichen Alternativen.
473 Just-in-time-Hinweise können wiederum als Opt-In ermöglicht werden, siehe oben, § 6 B.I.1.a)bb).
474 Siehe oben, § 4 C.III.

scheint eine verpflichtende Wahl unter den gegebenen Voraussetzungen überlegen: Jedenfalls im Grundsatz haben die Nutzer klare Präferenzen, die sich jedoch in unterschiedliche Gruppen aufspalten.[475] Ein einzelner *default* wird daher in seiner Lenkungswirkung jeweils mindestens einer Gruppe nicht gerecht.[476] Unter diesen Voraussetzungen ist daher in der verhaltensbasierten Regulierungstheorie die forcierte Selbstselektionierung im Rahmen der aktiven Wahl als sinnvolle Alternative zu dispositiven Regeln anerkannt,[477] deren Ausübung jedoch ressourcenschonend möglich sein muss.[478]

dd) Förderung von rationalen Entscheidungen und Reduzierung von Preisunschärfe durch *privacy scores*

Informiert wird diese Wahl jedoch viertens erst, wenn die Unterschiede zwischen den einzelnen Optionen durch auf einen Blick verständliche *privacy scores* kommuniziert werden.[479] Ähnlich wie der effektive Jahreszins bei einem Kredit aggregiert ein solcher Score datenschutzrechtliche Belastungen und Risiken durch die einzelnen Vertragsoptionen. Zwar ist die Berechnung des Scores mit deutlich mehr Unwägbarkeiten verbunden als beim mathematisch klar definierten effektiven Jahreszins.[480] Nichtsdestoweniger bestehen bereits eine Reihe von Anwendungen, die einen unidimensionalen *privacy score* einsatzfähig entwickelt haben: die Anwendungen Guard,[481] PrivacyFinder,[482] die Browser-Erweiterung von DuckDuckGo[483] sowie die von Forschern der Carnegie Mellon University lancierte App PrivacyGrade.[484] So wäre für Nutzer auf einen Blick erkennbar, wie invasiv die jeweilige Datensammlung und -ver-

[475] Siehe oben, § 3, Fn. 163.

[476] *Lin et al.*, 10th Symposium on Usable Privacy and Security (SOUPS) 2014, 199 (199, 207).

[477] *Carroll et al.*, 124 The Quarterly Journal of Economics 2009, 1639 (1641); *Sunstein*, 64 Duke Law Journal 2014, 1 (37 f.); *Hacker*, Verhaltensökonomik und Normativität, 2017, 489; konkret zu einer datenschonenden Alternative *Hacker/Petkova*, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1 (22).

[478] *Carroll et al.*, 124 The Quarterly Journal of Economics 2009, 1639 (1641); *Sunstein*, 64 Duke Law Journal 2014, 1 (39 f.); *Hacker*, Verhaltensökonomik und Normativität, 2017, 490; dazu sogleich noch unten, unter 3.b).

[479] Für die Einführung solcher Scores auch *Cranor*, 10 Journal on Telecommunications & High Technology Law 2012, 273 (291 ff.); *Reidenberg et al.*, 96 Washington University Law Review 2019, 1409 (1419 f.; 1430 ff.); für Pflichtinformationen allgemein, *Bar-Gill*, 11 Jerusalem Review of Legal Studies 2015, 75 (76 ff.); Vorschlag einer monetären Berechnung des „Datenpreises" bei *Hacker/Petkova*, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1 (22 f.), was jedoch gegenüber einem *privacy score* schwerer zu realisieren sein dürfte.

[480] Dazu sogleich unten, 2.d).

[481] Siehe oben, § 6, Fn. 139.

[482] *Cranor*, 10 Journal on Telecommunications & High Technology Law 2012, 273 (291 ff.).

[483] *Weinberg*, Protecting Your Personal Data Has Never Been This Easy, DuckDuckGo (23.1.2018), https://spreadprivacy.com/privacy-simplified/.

[484] http://privacygrade.org/.

arbeitung ist. Diese Informationen könnten sie dann gewinnbringend zu dem jeweiligen Nutzen und der Sensitivität des genutzten Produkts ins Verhältnis setzen. Damit ließen sich gleich mehrere Typen des in § 3 angesprochenen Marktversagens adressieren.

Einerseits wirkt ein verlässlicher *privacy score* Informationsüberlastung und verhaltensökonomischen Fehleinschätzungen entgegen, da auch langfristige oder für den Nutzer nicht offensichtliche Risiken für die Privatsphäre komprimiert eingepreist werden können. Andererseits präzisiert ein *privacy score* das notorisch unklare Preissignal bei datenbasierten Austauschprozessen.[485] Wie gesehen ist ein hinreichend determiniertes Preissignal Voraussetzung dafür, dass die dezentrale Wissensdiffusion im Markt zu einer effizienten Steuerung von Angebot und Nachfrage führt.[486]

Daher ist der *privacy score* vielleicht die wichtigste Neuerung des hier unterbreiteten Vorschlags: Durch ihn werden nicht nur die datenintensive und die datenschonende Option eines einzelnen Anbieters, sondern auch Angebote verschiedener Anbieter untereinander vergleichbar. Nur so lässt sich letztlich Preistransparenz herstellen und darüber ein effektiver Preiswettbewerb auch für datenbasierte Dienstleistungen ins Werk setzen.[487]

2. *Tatsächliche Voraussetzungen*

Die Umsetzung eines Rechts auf eine datenschonende Option, das mit einem *privacy score* gekoppelt ist, ist jedoch nur dann erstrebenswert, wenn die tatsächlichen Voraussetzungen dafür vorliegen: Erstens muss zumindest bei einem Teil der Nutzer eine hinreichende Zahlungsbereitschaft für die Wahl der datenschonenden Option zu erwarten sein (a)). Zweitens muss der *privacy score* nach verlässlichen Kriterien berechnet werden können (b)).

a) Hinreichende Zahlungsbereitschaft

Das Paradox der Privatheit[488] deutet darauf hin, dass trotz mannigfacher Bekundungen der Nutzer, an einem höheren Datenschutzniveau und einer stärkeren Kontrolle über ihre Daten interessiert zu sein, nicht einfach davon ausgegangen werden kann, dass Nutzer in realen Entscheidungssituationen bereit sein werden, statt mit ihren Daten mit einem moderaten Geldbetrag für ein Produkt zu zahlen. Bei genauerer Betrachtung erweist sich jedoch die Zahlungsbereitschaft für ein erhöhtes Datenschutzniveau als ebenso kontextabhängig wie die Datenschutzpräferenzen selbst. Dies impliziert, dass es für

---

485 *Ben-Shahar/Strahilevitz*, 45 Journal of Legal Studies 2016, S1 (S5).

486 Siehe oben, § 3 B.II.1.d).

487 Vgl. auch *Monopolkommission*, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015, Rn. 338 zu den positiven wettbewerblichen Auswirkungen des Rechts auf eine datenschonende Option ohne *privacy score*.

488 Dazu oben, § 3 B.II.1.

die Wirksamkeit des Rechts auf eine datenschonende Option auf die Schaffung eines unterstützenden Kontexts ankommen wird.

aa) Zahlungsbereitschaft und Salienz

Immer wieder wurde in empirischen Studien die Bereitschaft von Nutzern getestet, für ein erhöhtes Datenschutzniveau monetäre Zahlungen zu leisten (*willingness to pay*: WTP) oder ein bereits erworbenes Datenschutzniveau gegen Erhalt von monetären Zahlungen aufzugeben (*willingness to accept*: WTA). Dabei lässt sich unter anderem ein *endowment effect* nachweisen, bei dem Zahlungsbereitschaft (WTP) und Annahmebereitschaft (WTA) differieren.[489]

Einige bekannte Studien legen dabei eine geringe Bereitschaft zur Zahlung einer Datenschutzprämie (*privacy premium*) nahe.[490] Einer Vignette-Studie unter US-Bürgern zufolge würden diese für die Geheimhaltung verschiedener Ansammlungen von personenbezogenen Daten im Schnitt nur niedrige Beträge ausgegeben: einmalig 2,28 $ für die Browser-Historie; 4,05 $ für das digitale Adressbuch mit ihren Kontakten; 1,19 $ für Ortsdaten; und 3,58 $ für den Inhalt ihrer SMS.[491] Diese Ergebnisse ähneln einer weiteren Umfrage, wonach ein Viertel der Befragten eine Datenschutzprämie von 1,50 $ für den Verzicht auf die Erhebung von Ortsdaten und Audiomitschnitten bei einer Smartphone App zu zahlen bereit waren.[492] Noch pessimistischer stimmt auf den ersten Blick ein Feldexperiment: Darin entschlossen sich 39 von 42 Nutzern dafür, eine DVD von einem Unternehmen mit größerem Datenhunger (obligatorische Angabe des monatlichen Einkommens) zu erwerben, statt dasselbe Produkt für einen Euro mehr bei einem Wettbewerber zu erstehen, der die Privatsphäre vermeintlich stärker respektiert (obligatorische Angabe der Lieblingsfarbe).[493]

Dabei ist jedoch zu berücksichtigen, dass es sich jeweils nur um Durchschnittswerte bzw. Mehrheitsentscheidungen handelt. Eine höhere Zahlungsbereitschaft legten in der zuerst genannten Vignette-Studie mit US-Bürgern zum Beispiel solche mit einer größeren Erfahrung im Umgang mit Smartphones an den Tag;[494] bei Nutzern aus höheren Einkommensschichten verdoppelte bis verdreifachte sich die Zahlungsbereitschaft gar.[495] In der Feld-

[489] Siehe oben, § 3, Fn. 125.

[490] Siehe *Grossklags/Acquisti*, Proceedings of the Sixth Workshop on Economics of Information Security 2007, 1 (12 ff.) und die Nachweise in den folgenden Fußnoten; Überblick auch bei *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 254 ff.

[491] *Savage/Waldman*, The Value of Online Privacy: Evidence from Smartphone Applications, Technical Report, 2014, 20.

[492] *Egelman/Felt/D. Wagner*, in: Böhme (Hrsg.), The Economics of Information Security and Privacy, 2013, 211.

[493] *Beresford/Kübler/Preibusch*, 117 Economics Letters 2012, 25 (26).

[494] *Savage/Waldman*, The Value of Online Privacy: Evidence from Smartphone Applications, Technical Report, 2014, 25.

[495] *Savage/Waldman*, The Value of Online Privacy: Evidence from Smartphone Applications, Technical Report, 2014, 24.

studie mit der um einen Euro teureren DVD mag manchem Teilnehmer gar die Angabe der Lieblingsfarbe als stärker die Persönlichkeit betreffend erschienen sein als die Angabe eines monatlichen Einkommens, das durch den Anbieter im Übrigen nicht verifiziert werden konnte.[496] Jedenfalls stellte auch die teurere Variante keine besonders datenschonende Option dar, sodass der Aussagegehalt dieses Experiments für den hier in Rede stehenden Vorschlag gering ist.

Neuere Befragungen zeigen dann auch, dass die Nutzer seit einiger Zeit in der Tendenz eine steigende Zahlungsbereitschaft an den Tag legen. Dies mag mit der zunehmenden Bedeutung von Datenschutz im öffentlichen Diskurs zusammenhängen. Laut einer repräsentativen Umfrage unter deutschen Internetnutzern aus dem Jahr 2014 wären jedenfalls 35 % bereit, dafür zu bezahlen, dass ihre Daten nur genau so verwendet werden, wie sie es möchten;[497] unter denjenigen, die täglich online sind, sind es sogar 39 %.[498] Im Durchschnitt liegt die Zahlungsbereitschaft bei 41 € im Jahr.[499] Auch hier zeigen sich die bereits zuvor erwähnten Effekte der Einkommensverhältnisse: Bei einem Haushaltseinkommen von über 3500 € monatlich liegt die Summe bei 52 € im Jahr, bei jenen von bis zu 1000 € monatlich immerhin bei 27 €.[500] Die besondere Bedeutung des Datenschutzes für das Internet der Dinge ist den Nutzern ebenfalls bewusst. So zeigt eine Vignette-Studie aus dem Jahr 2019, dass die Teilnehmer bei einem IoT-Gerät für ein Smart Home, das in der Basisausstattung 49 $ kostet, im Durchschnitt eine Datenschutzprämie von 14 $ zahlen würden.[501]

Nicht auszuschließen ist bei Vignette-Studien naturgemäß, dass die Befragten bei einer realen Kaufentscheidung nur eine geringere Datenschutzprämie zahlen würden (*hypothetical bias*).[502] Laborexperimente bestätigen jedoch im Grundsatz, dass Datenschutzprämien in nicht unerheblicher Höhe in Kauf genommen werden, wenn die datenschutzrechtlichen Implikationen der jeweiligen Kaufentscheidung nur salient kommuniziert werden.[503] Hier kommt nun gerade der *privacy score* ins Spiel. Dieser beeinflusste in zwei Laborexperimenten das Kaufverhalten generell, besonders aber bei einem sensiblen Gut (Sexspielzeug), und führte zur Zahlung eines Mehrbetrags für erhöhten Datenschutz.[504] Ein weiteres Laborexperiment arbeitete ebenfalls mit einem *privacy*

---

[496] Dafür spricht auch, dass in demselben Experiment getestet wurde, wie die Wahl ausfällt, wenn beide Unternehmen die DVD zu exakt demselben Preis anbieten und sich daher nur in den abgefragten Daten unterscheiden. Hier teilten sich die Nutzer etwa hälftig zwischen den Unternehmen auf und beklagten in fast identischer Zahl den ungenügenden Datenschutz, siehe *Beresford/Kübler/Preibusch*, 117 Economics Letters 2012, 25 (26).

[497] *DIVSI*, Daten – Ware und Währung, 2014, 13.

[498] *DIVSI*, Daten – Ware und Währung, 2014, 14.

[499] *DIVSI*, Daten – Ware und Währung, 2014, 14.

[500] *DIVSI*, Daten – Ware und Währung, 2014, 14.

[501] *Barbosa et al.*, Proceedings on Privacy Enhancing Technologies 2019, 211 (220).

[502] *Murphy et al.*, 30 Environmental and Resource Economics 2005, 313.

[503] Siehe *Gideon et al.*, Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS) 2006, 133 (142) und die Nachweise in den folgenden Fußnoten.

[504] *Egelman et al.*, Proceedings of the SIGCHI Conference on Human Factors in Com-

score zwischen eins und vier, der zudem farblich kodiert wurde, und untersuchte dessen Einfluss auf das Kaufverhalten auf einem Onlinemarktplatz für IoT-Geräte. Dabei zahlten die Teilnehmer im Durchschnitt eine Datenschutzprämie von 6,18 $ auf einen Basispreis von 6,99 $, wenn das datenschutzfreundlichste Produkt als *default* vorgeschlagen wurde, und eine durchschnittliche Prämie von 3,74 $, wenn das am wenigsten datenschutzfreundliche Produkt den Regelfall darstellte.[505]

Diese Experimente fügen sich ein in die bereits angesprochene empirische Literatur zur Heterogenität von Datenschutzpräferenzen.[506] Danach sind diese im Wesentlichen U-förmig verteilt. In einer Vignette-Studie war gut 20 % der Teilnehmer die Geheimhaltung ihrer personenbezogenen Kaufhistorie mit einer Gutscheinkarte mehr als 11 $ wert, während gut 35 % diesen Wert auf weniger als 1 $ taxierten.[507] In einem Laborexperiment zahlte immerhin ein knappes Drittel einen Aufschlag von 0,50 € auf ein Kinoticket im Wert von 7 €, um die Angabe der jeweiligen Mobilfunknummer zu vermeiden.[508] Starke Varianz zeigen Datenschutzpräferenzen auch bei der Frage, ob es Anbietern erlaubt sein soll, personalisierte Werbung zu schalten.[509]

Dies zeigt insgesamt, dass die Bereitschaft zur Zahlung einer Datenschutzprämie stark zwischen Nutzern variiert, zwischen einem Fünftel und einem Drittel der Nutzer jedoch offenbar zur Zahlung von teilweise auch signifikanten Prämien bereit ist, wenn das unterschiedliche Datenschutzniveau transparent und deutlich dargestellt wird. Bei Verwendung eines *privacy score* steigt dieser Prozentsatz nach den genannten Studien sogar auf über 50 % an bzw. Nutzer sind bereit, im Durchschnitt auch erhebliche Preisaufschläge (in der Dimension von 5–10 €) für verbesserten Datenschutz hinzunehmen. Dies gilt insbesondere für das Internet der Dinge. Auch wenn diese Daten noch einer Überprüfung in Feldstudien harren, so lassen sie zumindest sehr plausibel erscheinen, dass ein signifikanter Teil der Nutzer eine monetäre, datenschonende Option wählen würde, sofern diese angemessen bepreist ist.[510]

puting Systems 2009, 319 (325): *privacy premium* von durchschnittlich 0,52 $ bei Sexspielzeug und 0,34 $ bei Batterie (Basispreis jeweils 15,50 $), wenn ein *privacy score* (Skala von 0–4) angezeigt wird; *Tsai et al.*, 22 Information Systems Research 2011, 254 (263 f.): *privacy premium* von ca. 0,60 $ für dieselben Produkte wie in der vorhergehenden Studie von einer Mehrheit der Teilnehmer bei Anzeige desselben *privacy score* gezahlt.

[505] *Gopavaram et al.*, IoTMarketplace: Informing Purchase Decisions with Risk Communication, Working Paper, 2019, ftp://svn.soic.indiana.edu/pub/techreports/TR742.pdf, 11.

[506] Siehe oben, § 3, Fn. 163.

[507] *Acquisti/John/Loewenstein*, What is Privacy Worth?, Working Paper, 2009, http://pages.stern.nyu.edu/~bakos/wise/papers/wise2009-6a1_paper.pdf, 25 f. Ein weiteres lokales Maximum existiert bei 2 $.

[508] *Jentzsch/Preibusch/Harasser*, Study on Monetising Privacy: An Economic Model for Pricing Personal Information, European Network and Information Security Agency, 2012, 36.

[509] *Lin et al.*, 10th Symposium on Usable Privacy and Security (SOUPS) 2014, 199 (204).

[510] Zur Preiskontrolle unten, § 6 C.II.5.b)bb).

bb) Datenschonende Option als Minderheitenschutz

Selbst wenn man bei realistischer Betrachtung davon ausgeht, dass die Anzahl derjenigen, die in reellen Konsumentscheidungen die datenschonende Option wählt, hinter den in den Vignette-Studien und Laborexperimenten suggerierten Zahlen zurückbleibt und letztlich eine kleine Minderheit darstellt,[511] erscheint die verpflichtende Einführung einer datenschonenden Option auch aus dem Gesichtspunkt des Minderheitenschutzes gerechtfertigt. Grundrechte und ihre Verwirklichung dienen typischerweise gerade auch dem Schutz von Minderheitsinteressen.[512] So wird das in Art. 8 Abs. 1 GG gewährleistete Recht auf politische Demonstrationen nicht dadurch in seiner Bedeutung geschmälert, dass sich lediglich ein geringer Teil der Grundrechtsberechtigten an politischen Demonstrationen beteiligt. In gleicher Weise ist die Verwirklichung des Datenschutzgrundrechts durch die Möglichkeit zur Durchsetzung hoher Datenschutzpräferenzen nicht deswegen von geringerem Belang, weil sie lediglich von einer Minderheit geteilt werden. Dass in multipolaren Grundrechtsverhältnissen wie den hier diskutierten immer die Grundrechte der anderen Akteure, insbesondere der Nutzer mit niedrigen Datenschutzpräferenzen und der Anbieter, in Rechnung gestellt und abgewogen werden müssen, versteht sich von selbst.[513] Nichtsdestoweniger ist zu bemerken, dass Datenschutz als Minderheitenschutz zugleich positive Effekte auch für jene Nutzer hat, welche die datenschonende Option nicht wählen: Wenn die Zahl der verarbeitbaren Datenpunkte reduziert wird, sinken die Präzision von adverser und ähnlichkeitsbasierter Interferenz und damit die negativen Externalitäten der Datenverarbeitung, die auch diese Nutzer betreffen können.[514]

b) Berechnung des *privacy score*

Eine weitere tatsächliche Voraussetzung für die Umsetzung des hier unterbreiteten Vorschlags ist, dass der *privacy score* nach verlässlichen Kriterien anbieterübergreifend und einheitlich berechnet werden kann. Dies ist nicht trivial.[515] Zwar haben einige Anbieter, wie gesehen, bereits einsatzfähige *privacy scores*

---

511 Vgl. *Calo*, 82 George Washington Law Review, 2014, 995 (1048); *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 37.

512 *Beaucamp/Meßerschmidt*, ZaöRV 2003, 779; *Kirchhof*, NVwZ 2014, 1537 (1540); *Dahl*, A Preface to Democratic Theory, Expanded Ed. 2006, 7 ff., 90 ff.; *Sen*, 45 Oxford Economic Papers 1993, 519 (522); deutlich auch *Hayek*, The Constitution of Liberty, 2011 [1960], 83: „It also follows that the importance of our being free to do a particular thing has nothing to do with the question of whether we or the majority are ever likely to make use of that particular possibility. […] It might even be said that the less likely the opportunity to make use of freedom to do a particular thing, the more precious it will be for society as a whole."

513 Dazu noch unten, § 6 C.II.6.

514 Dazu oben, § 3 II.1.c).

515 Kritisch insoweit daher *Reidenberg et al.*, 96 Washington University Law Review 2019, 1409 (1430 ff.).

entwickelt.[516] Deren korrekte Kalibrierung kann von außen jedoch nur schwer beurteilt werden. Gegenwärtig ist dies unter rechtlichen Gesichtspunkten von verminderter Relevanz, da ihr Einsatz ohnehin, sowohl auf Anbieterseite als auch auf Nutzerseite, freiwillig erfolgt. Wenn *privacy scores* jedoch für Anbieter rechtlich verpflichtend würden, müsste sichergestellt werden, dass Anbietern keine ungerechtfertigten Vor- oder Nachteile entstehen. Sie müssten, mit anderen Worten, die tatsächlichen Datenschutzrisiken möglichst korrekt und objektiv abbilden.[517] Dies ist letztlich eine Frage der empirisch-technischen Implementierung, welche den Rahmen dieser Arbeit übersteigt. Immerhin kann aber die Konstruktion des *privacy score* an dieser Stelle abstrakt beschrieben werden. Dafür sind zwei Schritte notwendig.[518]

Zunächst müssen die Selektionskriterien bestimmt werden, die in die Berechnung des Scores Eingang finden. Einen ersten Anhaltspunkt können die Kriterien für die von Mozilla entwickelten Datenschutz-Icons darstellen:[519] die Dauer der Aufbewahrung der Daten; der Grad, zu dem eine Wiederverwendung für andere als die ursprünglichen Zwecke erfolgt (*secondary use*);[520] der Grad, zu dem Daten mit Werbenetzwerken (*ad exchanges*) geteilt werden;[521] und der Grad, zu dem Daten nur über ein rechtsförmiges Verfahren an staatliche Institutionen (zum Beispiel Ermittlungsbehörden) weitergegeben werden. Verschiedene weitere Kriterien sollten hinzutreten, die zum Teil auch in die bereits existierenden *privacy scores* einfließen,[522] zum Beispiel: der Grad, zu dem die tatsächliche Datenverarbeitung mit den in der Datenschutzerklärung erwähnten Praktiken übereinstimmt;[523] der Grad der Lesbarkeit der Datenschutzerklärung;[524] die Verfügbarkeit von Verschlüsselung[525] und der Umfang der Aggregation der Daten mit anderen Datensätzen. All diese Kriterien sind bereits jetzt öffentlich verfügbar oder können durch Datenanalyse gewonnen

---

[516] Siehe oben, § 6, Fn. 479 ff.

[517] Gegen eine Subjektivierung der Scores, etwa durch Einbeziehung von Nutzererwartungen, auch *Reidenberg et al.*, 96 Washington University Law Review 2019, 1409 (1431).

[518] *Reidenberg et al.*, 96 Washington University Law Review 2019, 1409 (1430 ff.).

[519] Privacy Icons, Mozilla Wiki, https://wiki.mozilla.org/Privacy_Icons.

[520] Für die Möglichkeit einer automatisierten Analyse (*static code analysis*) der Zwecke der Datenverarbeitung, siehe *Lin et al.*, 10th Symposium on Usable Privacy and Security (SOUPS) 2014, 199 (201 f.).

[521] Siehe wiederum den Nachweis in der vorangehenden Fußnote.

[522] Die Browser-Erweiterung von DuckDuckGo etwa basiert auf einer automatisierten Analyse von „hidden tracker networks, encryption availability, and website privacy practices", in Zusammenarbeit mit Terms of Service; Didn't Read (siehe § 6, Fn. 120), *Weinberg*, Protecting Your Personal Data Has Never Been This Easy, DuckDuckGo (23.1.2018), https://spreadprivacy.com/privacy-simplified/.; PrivacyGrade nutzt ein Modell, das unter anderem die Differenz zwischen Nutzererwartungen und tatsächlichen Datenverarbeitungspraktiken berücksichtigt, siehe *Lin et al.*, Proceedings of the 2012 ACM Conference on Ubiquitous Computing 2012, 501 und http://privacygrade.org/.

[523] Siehe oben, Text bei § 6, Fn. 146 ff.

[524] Siehe oben, Text bei § 6, Fn. 199.

[525] Siehe oben, § 6 B.I.1.a).

werden. Ein Großteil der Informationen muss ohnehin nach Art. 13 DS-GVO veröffentlicht werden und kann daher durch die genannten Instrumente der automatisierten Analyse von Datenschutzerklärungen und Nutzungsbedingungen aufbereitet werden.[526] Differenzen wiederum zwischen den dort durch die Anbieter gemachten Angaben und der tatsächlichen Datenverarbeitung können ebenfalls durch automatisierte Analysewerkzeuge aufgeschlüsselt werden.[527] Somit bedarf es keiner weitergehenden Informationspflichten oder signifikanter technischer Neuentwicklungen für die Berechnung der einzelnen Werte der Kriterien eines *privacy score*.

In einem zweiten Schritt müssen dann Gewichtungsfaktoren für die einzelnen Kriterien erarbeitet werden.[528] Diese Faktoren objektiv zu gestalten, stellt eine besondere Herausforderung dar. Insgesamt sollten die Kriterien und die Gewichtungsfaktoren in einem transparenten Prozess unter Beteiligung der Öffentlichkeit sowie unter Einbeziehung von Vertretern von Anbietern und Nutzern (z. B. unter Einbeziehung von *crowdsourcing*[529]) festgelegt werden. Dies wird jedoch nicht unerhebliche Zeit, auch für empirische Tests, und Ressourcen in Anspruch nehmen. Dabei muss insbesondere, wie bei jeder Behebung von Marktversagen,[530] darauf geachtet werden, dass die erwarteten Kosten der Maßnahme den dadurch erwarteten Gewinn nicht übersteigen. Dies kann letztlich nur auf der Basis von Pilotprojekten abgeschätzt werden. Es wäre jedoch einen Versuch wert. Solange allerdings standardisierte *privacy scores* noch nicht verfügbar sind, sollten stattdessen die verschiedenen Vertrags- oder Nutzungsoptionen jeweils auf einen One-Pager der Datenschutzerklärung verweisen müssen,[531] um dergestalt eine möglichst weitgehende Vergleichbarkeit der Angebote zu gewährleisten.

3. Implementierung der Wahlmöglichkeit

Die tatsächlichen Voraussetzungen für eine datenschonende Pflichtalternative liegen also im Wesentlichen bereits vor. Eine rechtliche Implementierung der Wahlmöglichkeit kann daher jederzeit erfolgen. Sie muss insbesondere spezifizieren, durch welche Parameter die datenschonende Option definiert werden (a)) und wie die Wahl zwischen einer datenschonenden und einer nicht datenschonenden Alternative ausgeübt werden kann (b)).

---

[526] Siehe oben, § 6 B.II.1.

[527] Siehe oben, Text bei § 6, Fn. 146 ff., sowie die Nachweise § 6, in Fn. 520 und 158; zur automatisierten Analyse der Lesbarkeit von Datenschutzerklärungen, siehe den Text bei § 6, Fn. 199 ff.

[528] *Reidenberg et al.*, 96 Washington University Law Review 2019, 1409 (1432 f.).

[529] *Wilson et al.*, Proceedings of the 25th International Conference on World Wide Web 2016, 133; *Wilson et al.*, 13 (1) ACM Transactions on the Web (TWEB) 2018, Article 1.

[530] Siehe, statt vieler, *Veljanovski*, in: Baldwin/Cave/Lodge (Hrsg.), The Oxford Handbook of Regulation, 2010, 18 (22).

[531] Zum One-Pager oben, § 6 C.I.1.a)aa)(2).

a) Wahlmöglichkeiten

Grundsätzlich erscheint es dabei sinnvoll, Anbieter lediglich zum Angebot *einer* datenschonenden Option zu verpflichten. Zwar wäre es denkbar, ein ganzes Menü an Optionen, von stark über mittel datenschonende bis hin zu stärker und sehr stark invasiven Alternativen, vorzuschreiben.[532] Dies würde jedoch nicht nur in kaum mehr zu rechtfertigender Weise in die Vertragsfreiheit der Anbieter eingreifen, sondern auch den Nutzern die Wahl tendenziell erschweren.[533] Eine empirische Studie zeigt, dass die Interaktion mit Wahlmöglichkeiten hinsichtlich Datenschutzoptionen dort am größten ist (55 %), wo lediglich zwei Optionen (Aktivierung oder Deaktivierung weitergehender Datenerhebung) angeboten werden.[534] Auch aus anderen Kontexten ist bekannt, dass zu viele Optionen zu Überlastung und letztlich möglicherweise schlechterer Entscheidungsqualität führen.[535]

aa) Vertraglich erforderliche vs. nicht erforderliche Daten

Die Crux ist daher zu bestimmen, welche Formen der Datenverarbeitung für die datenschonende Option zugelassen sein sollen. Dabei erscheint es sinnvoll, zunächst einmal zwischen vertragserforderlichen und nicht vertragserforderlichen personenbezogenen Daten zu differenzieren.[536] Anders als bei Art. 7 Abs. 4 DS-GVO und Art. 6 Abs. 1. lit. b DS-GVO sollte dabei ein enger Begriff der vertragserforderlichen Daten *explizit* festgeschrieben werden. Dies impliziert insbesondere, dass nur solche Daten im Rahmen der datenschonenden Option verarbeitet werden dürfen, deren Verarbeitung für die Erfüllung der (wirksam vereinbarten) Pflichten des Anbieters, und nicht des Nutzers, technisch notwendig sind.[537] Aus Gründen der Rechtssicherheit sollte dennoch am subjektiven Erforderlichkeitsmaßstab festgehalten werden.[538] Auch Anbieter-

---

[532] Vgl. *Becker*, JZ 2017, 171 (178).

[533] *Novotny/Spiekermann*, Personal Information Markets AND Privacy: A New Model to Solve the Controversy, in: Hildebrandt et al. (Hrsg.), Digital Enlightenment Yearbook 2013, 2013, 102 (108).

[534] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (9).

[535] *Iyengar/Lepper*, 79 Journal of Personality and Social Psychology, 2000, 995; *Solomon et al.*, Consumer Behaviour: A European Perspective, 2013, 333; siehe auch nochmals *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (2).

[536] *Novotny/Spiekermann*, Personal Information Markets AND Privacy: A New Model to Solve the Controversy, in: Hildebrandt et al. (Hrsg.), Digital Enlightenment Yearbook 2013, 2013, 102 (107).

[537] Vgl. *Becker*, JZ 2017, 171 (176 f.).

[538] Objektiver Maßstab hingegen bei *Novotny/Spiekermann*, Personal Information Markets AND Privacy: A New Model to Solve the Controversy, in: Hildebrandt et al. (Hrsg.), Digital Enlightenment Yearbook 2013, 2013, 102 (107): („minimum information […] necessary and sufficient to perform the principal service"); ebenfalls bei *Becker*, JZ 2017, 171 (176 f.): funktional für Basisversion und möglichst viele zeitgemäße Funktionen notwendig;

pflichten zur Personalisierung des Produkts, also zu einer von der Standardversion abweichenden Angebotserbringung, können jedoch – unabhängig von ihrer zivilrechtlichen Wirksamkeit[539] – eine Datenverarbeitung nicht legitimieren, da sonst durch geschickte Wahl des Personalisierungsgrads durch den Anbieter die datenschonende in eine datenintensive Option konvertiert werden könnte.[540]

Dies bedeutet in der praktischen Umsetzung, dass zum Beispiel Ortsdaten (*location data*) bei Verwendung einer Navigationsapplikation, nicht aber bei Nutzung eines sozialen Netzwerks standardmäßig erhoben werden dürfen. Hinsichtlich der datenintensiven Option scheitert eine Einwilligung in die Verarbeitung von Ortsdaten dahingegen auch bei einem sozialen Netzwerk mangels Abhängigkeit nicht mehr an Art. 7 Abs. 4 DS-GVO.

bb) Wahl der Cookies

Besonders relevant ist die Differenzierung zwischen einer datenschonenden und einer nicht datenschonenden Alternative bei der Wahl der Cookies. Wie bereits gesehen, ist eine aktive Auswahl verschiedener Typen von Cookies im Rahmen einer Einwilligung bereits jetzt bei manchen, wenngleich nur wenigen, Webseiten und Applikationen möglich.[541] Dies zeigt, dass eine selektive Aktivierung bestimmter Typen von Cookies technisch ohne Weiteres möglich ist.[542]

(1) Typen von Cookies

Mit Blick auf ihre Funktion unterscheidet man grundsätzlich fünf verschiedene Typen von Cookies (oder anderen Geräte-Identifiern).[543] Personalisierungs-/Designcookies regeln etwa die Schriftart und -größe.[544] Analysecookies erfassen das Nutzerverhalten auf der Webseite, unter anderem, um dem Seitenbetreiber eine Verbesserung des Inhalts zu ermöglichen.[545] Social Media-Cookies implementieren Plug-Ins, zum Beispiel von Facebook oder YouTube,

unklar bleibt hierbei jedoch jeweils, wie die Basisversion und die zeitgemäßen Funktionen bzw. der *principal service* bestimmt werden sollen, siehe bereits oben, § 4 B.I.3.a)dd)(3)(a)(bb)b.

[539] Siehe oben, § 5 C.II.1.e)cc)(b)(cc).

[540] Vgl. *Becker*, JZ 2017, 171 (174, 176).

[541] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (4); siehe auch oben, Text bei § 4, Fn. 886.

[542] Siehe auch *Degeling et al.*, 26th Annual Network and Distributed System Security Symposium (NDSS '19), 1 (11).

[543] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (7).

[544] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (7).

[545] *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (7).

und senden Informationen an diese Drittanbieter.[546] Marketingcookies wiederum sammeln Informationen zu Zwecken personalisierter Werbung.[547] Essenzielle (oder auch notwendige) Cookies schließlich sind technisch zur Erbringung der jeweiligen Leistung erforderlich.[548] Dies sind insbesondere Cookies, welche die Einwilligungsentscheidung des Nutzers speichern oder einen elektronischen Warenkorb befüllen.[549] Letzteres Beispiel zeigt jedoch bereits, dass die Definition eines essenziellen Cookies nicht immer technisch präzise möglich ist: Ob ein Warenkorb, der auch über eine Nutzungssession hinaus Warenbestände dauerhaft speichern kann, technisch funktional erforderlich ist oder lediglich ein personalisierendes Komfort-Instrument darstellt, kann nicht immer zweifelsfrei entschieden werden.[550]

(2) Datenschonende Cookies

Das Problem für eine datenschonende Option liegt daher darin, diejenigen Typen von Cookies (und anderen Geräte-Identifiern) rechtssicher zu bestimmen, die für die Funktion einer Applikation oder Webseite technisch erforderlich sind.[551] Hier müssen letztlich bestimmte technische Standards für unterschiedliche Verarbeitungssituationen eingeführt werden,[552] die sich an die Diskussion zu Art. 5 Abs. 3 S. 2 ePrivacy-Richtlinie anlehnen können.[553] Grundsätzlich sollten in einer datenschonenden Option lediglich essenzielle Cookies erlaubt sein sowie Personalisierungscookies in dem Maße, in dem Personalisierungsoptionen tatsächlich vom Nutzer aktiv ausgewählt werden (zum Beispiel die Schriftgröße in einer Zeitungs-App verändert wird). Analyse-, Social Media- und Marketingcookies dürfen hingegen in einer datenschonenden Option grundsätzlich nicht gesetzt werden.

In der datenintensiven Version hingegen müssen die Anbieter zwar auch das geltende Datenschutzrecht respektieren; eine Einwilligung in die genannten Kategorien von Cookies muss daher auch dort aktiv abgegeben werden.[554] Jedoch können die Anbieter die Wahl der datenintensiven Option von der Akzeptanz aller Formen von Cookies abhängig machen, da Art. 7 Abs. 4 DSGVO infolge des Angebots der datenschonenden Option auch insoweit nicht gilt. Derartige *tracking walls* sind auch technisch einfach durch die Wahl einer

---

546 *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (7); siehe bereits oben, § 2 A.

547 *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (7).

548 *Utz et al.*, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1 (7).

549 Vgl. *Mellet/Beauvisage*, Consumption Markets & Culture 2019, 1 (7).

550 Vgl. *Engeler/Felber*, ZD 2017, 251 (255); *Engeler*, ZD 2018, 55 (61).

551 *Engeler/Felber*, ZD 2017, 251 (255); *Engeler*, ZD 2018, 55 (61).

552 *Kring/Marosi*, K&R 2016, 773 (776); siehe auch oben, Text bei § 4, Fn. 1038.

553 Dazu oben, Text bei § 4, Fn. 802.

554 Siehe oben, § 4 B.I.4.b)aa)(2).

entsprechenden Cookie Library zu implementieren, sodass das werbungsbasierte Geschäftsmodell letztlich nicht durch das datenschonende Angebot unterlaufen wird.[555]

b) Ausübung der Wahl (*agreement technologies*)

Die Ausübung der Wahl zwischen einer datenschonenden und einer datenintensiven Option darf jedoch nicht zur unverhältnismäßigen Belastung für die Nutzer werden.[556] Daher sollte die Wahl auch mit aktiv gewählten Browser- oder Smartphone-Einstellungen oder über einen Datenschutzassistenten möglich sein: Maschinelles Lernen stellt hier in zunehmendem Maße *agreement technologies*[557] zur Verfügung, die eigene, hier nicht im Einzelnen zu vertiefende Regulierungsfragen aufwerfen,[558] technisch gesehen jedoch (in unterschiedlichem Grade) autonom Vertragsangebote selektieren und Zustimmung signalisieren können.[559]

Wird also beispielsweise ein *do track*-Signal gesendet, muss dies als wirksame Zustimmung zu den Bedingungen der datenintensiven Option gewertet werden.[560] Über ein spezifisches Signal (z. B. *choose monetary options*) sollte ferner, bei stark autonomen Assistenten (*agreement technologies*) über eine Analogie zum Stellvertretungsrecht,[561] auch die Wahl der datenschonenden Option und der Abschluss eines entsprechenden Vertrags möglich sein. Dabei könnte der Nutzer bestimmte Obergrenzen für die Nutzung von Apps/Web-

[555] *Degeling et al.*, 26th Annual Network and Distributed System Security Symposium (NDSS '19), 1 (11).

[556] Vgl. *Willis*, 29 Berkeley Technology Law Journal 2014, 61 (84).

[557] Überblick über Begriff und Stand der Technik bei *Santos et al.*, Artificial Intelligence and Law 2019, https://doi.org/10.1007/s10506-019-09259-8, 1 (2 ff.); *Billhardt et al.*, 8 Applied Sciences 2018, Article 816, 1 (2 ff. mit Überblick über reale Anwendungen in 6 ff.); grundlegend *Luck/McBurney*, IEEE SMC Conference on Distributed Human-Machine Systems 2008, 1 (3 ff.); siehe ferner *Ossowski/Sierra/Botti*, in: Ossowski (Hrsg.), Agreement technologies, 2013, 3 (3 ff.), die weiteren Beiträge in Ossowski (Hrsg.). Agreement technologies, 2013, sowie die Nachweise in den folgenden Fußnoten.

[558] *Sartor*, in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, 263 (276 ff.); *Brownsword*, in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, 165 (193 ff.); *Grundmann/Hacker*, 13 European Review of Contract Law 2017, 255 (283 f.); *Gal/Elkin-Koren*, 30 Harvard Journal of Law and Technology 2016, 309 (339 ff.).

[559] Siehe nur *Surden*, Computable Contracts, 46 UC Davis Law Review 2012, 629 (694 f.); *Grundmann/Hacker*, 13 European Review of Contract Law 2017, 255 (280, 283); *Sartor*, in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, 263 (266 ff.); *Brownsword*, in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, 165 (189 ff.); zu *machine-to-machine communication*, siehe auch den Überblick bei *Weyrich/Schmidt/Ebert*, 31(4) IEEE Software 2014, 19; *Balevi/Al Rabee/Gitlin*, IEEE International Conference on Communications (ICC) 2018, 1.

[560] Siehe oben, § 6 C.I.3.c)aa)(1).

[561] So auch *Surden*, 46 UC Davis Law Review 2012, 629 (694); *Sartor*, in: Grundmann (Hrsg.), European Contract Law in the Digital Age, 2018, 263 (272 ff.); *Grundmann/Hacker*, 13 European Review of Contract Law 2017, 255 (283); siehe auch bereits oben, § 6 C.I.3.c)aa)(1)(b)(bb).

sites oder einen Bestätigungsvorbehalt („Wollen Sie wirklich einen Vertrag mit x über die Nutzung von y zum Preis von z abschließen?") festlegen. Die Einzelheiten hängen von der genauen Ausgestaltung eines Rechts auf eine datenschonende Option ab, die hier nicht im Detail geleistet werden kann. Festzuhalten bleibt jedenfalls, dass die weitgehend automatisierte Ausübung der Wahl *de lege lata* nach hier vertretener Auffassung durchaus möglich ist.[562] Dabei geht zwar der mit einer aktiven Wahl verbundene Lerneffekt verloren; dies ist jedoch zur Reduzierung der Belästigung der Nutzer mit wiederholten Anfragen aus hiesiger Sicht hinzunehmen.

4. Sektorspezifizität

Die Einführung einer datenschonenden Option ist, wie der vorangegangene Abschnitt gezeigt hat, technisch ohne Weiteres möglich und wird von einigen Anbietern bereits jetzt praktiziert. Genau dies deutet auf die Notwendigkeit hin, eine rechtliche Verpflichtung zur Einführung einer derartigen Alternative nur sektorspezifisch zu etablieren. Sofern hinreichende Alternativen am Markt bestehen, die den Zugang zu Geräten, Diensten oder Applikationen in datenschonender Weise ermöglichen, besteht keine Notwendigkeit für eine regulatorische Intervention in das Marktgeschehen.[563]

Ein Beispiel für marktgängige und effektiv nutzbare datenschonende Angebote ist der Markt für E-Mail-Webservice-Provider. Hier bieten Gmail (Google), Yahoo Mail (Yahoo) und Hotmail (Microsoft) rein datenfinanzierte Produkte an. Daneben existieren jedoch Wettbewerber wie etwa Posteo[564] oder Tutanota,[565] bei denen starke Zurückhaltung bei der Datenverarbeitung durch monetäre Zahlungen erkauft werden kann. Posteo verwendet keine Tracking- oder Analysecookies, bindet keine Social Plug-Ins ein, verschlüsselt Daten und bietet keine Werbung.[566] Damit erfüllt es (bei Unterstellung der Korrektheit der Datenschutzerklärung) die Grundvoraussetzungen einer datenschonenden Option. Gleiches gilt für Tutanota.[567] Mit einer Gebühr von einem Euro pro Monat[568] ist auch der Preis jeweils zumutbar.

Eine umfassende Analyse aller Sektoren der digitalen Wirtschaft kann hier nicht geleistet werden. Jedoch sollen kurz drei zentrale Beispiele untersucht werden, die sich unmittelbar aus den drei Leitfällen ergeben[569] und bei denen die rechtliche Verankerung einer datenschonenden Option sehr naheliegt: so-

[562] Siehe oben, § 6 C.I.3.c)aa).

[563] *Monopolkommission*, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015, Rn. 338.

[564] https://posteo.de.

[565] https://tutanota.com/de/.

[566] Posteo, Datenschutzerklärung, https://posteo.de/site/datenschutzerklaerung.

[567] Tutanota, Datenschutz, https://tutanota.com/de/privacy.

[568] Posteo, Konditionen, https://posteo.de/site/leistungen; https://tutanota.com/de/pricing.

[569] Siehe dazu oben, § 3 D.I.

ziale Netzwerke; Suchmaschinen; und IoT-Geräte. Ihnen ist gemeinsam, dass in diesen Bereichen gegenwärtig datenschonende Optionen am Markt nicht in hinreichender Weise angeboten werden und aufgrund hoher Entwicklungskosten und anderer Marktzutrittsbarrieren mit einem Markteintritt von datenschonenden Anbietern auch nicht in naher Zukunft gerechnet werden kann.

a) Soziale Netzwerke

Führende soziale Netzwerke[570] weisen bislang keine einfach zu handhabende datenschonende Option auf. Zwar ist es etwa bei Facebook möglich, durch manuelle Einstellung aus verschiedenen Formen der Datenverarbeitung hinauszuoptieren.[571] Dies umfasst jedoch erstens keineswegs alle Formen von Analyse-, Social Media- und Marketingcookies oder der Datenerhebung und Weiterleitung an Dritte,[572] sodass die Bedingungen einer datenschonenden Option ohnehin nicht erfüllt sind. Ferner zeigen die bereits mehrfach thematisierten *default*-Effekte, dass selbst bei einer einfachen und salienten Möglichkeit der Abwahl dieser Cookies die überwältigende Mehrzahl der Nutzer einfach die Voreinstellungen bestehen lässt.[573] Dies wird noch verstärkt durch den Umstand, dass in Ermangelung von *single click privacy*[574] die Voreinstellungen auf mehreren, zum Teil schwer auffindbaren Seiten geändert werden müssten.[575] Die bislang implementierten Opt-Out-Möglichkeiten stellen daher in mehrfacher Hinsicht keine taugliche datenschonende Option dar.

Am relevanten Markt[576] existieren zwar eine Reihe von Wettbewerbern zu Facebook, die hohe Datenschutzpräferenzen besser respektieren,[577] etwa So-

[570] Zu Begriff und Varianten des sozialen Netzwerks Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 170, 175; *Golland*, Datenverarbeitung in sozialen Netzwerken, 2019, 10 f.; *Kampert*, Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, 2016, 7 ff.

[571] *Forbrukerrådet*, Deceived by Design, Bericht, 2018, 31.

[572] *Forbrukerrådet*, Deceived by Design, Bericht, 2018, 33 f.; Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 654. Insbesondere umfasst die Kontrollmöglichkeit nicht die Verwendung durch Facebook selbst erhobener Daten oder die Erhebung von Daten durch Dritte zu anderen Zwecken als für Werbung (Stand: November 2019, siehe https://www.facebook.com/ads/preferences/?entry_product=ad_settings_screen).

[573] Siehe oben, § 4, Fn. 876 f.

[574] Siehe oben, § 6, Fn. 314.

[575] *Forbrukerrådet*, Deceived by Design, Bericht, 2018, 33 f.

[576] Zur Marktabgrenzung bei sozialen Netzwerken siehe Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 166 ff.; *Filistrucchi*, in: *OECD* (Hrsg.), Rethinking Antitrust Tools for Multi-Sided Platforms, 2018, 37–54; *Wismer/Rasek*, in: *OECD* (Hrsg.), Rethinking Antitrust Tools for Multi-Sided Platforms, 2018, 55; *Monopolkommission*, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015, Rn. 294 ff.

[577] *Brown*, Fed Up with Facebook? Here are 6 Alternatives, maketecheasier (18.5.2019), https://www.maketecheasier.com/facebook-alternatives-social-networks/.

ciall,[578] Minds[579] oder MeWe.[580] Anders als bei einem datenschonenden E-Mail-Anbieter bieten sie jedoch keine äquivalenten Alternativen zu Facebook.[581] Denn soziale Netzwerke leben von Netzwerkeffekten:[582] Je mehr Nutzer ein Netzwerk hat, desto größer der Nutzen nicht nur für Werbetreibende (positiver indirekter Netzwerkeffekt[583]), sondern auch für die Nutzer selbst (positiver direkter Netzwerkeffekt[584]). Insofern bieten Alternativen mit gegenüber Facebook vernachlässigbaren Nutzerzahlen nach hier vertretener Auffassung gerade keine ausreichende datenschonende Marktoption für Nutzer. Dies ist jedoch letztlich eine Wertungsfrage, die naturgemäß auch anders entschieden werden kann.

Jedenfalls sorgen die Netzwerkeffekte zusammen mit den nicht unerheblichen Entwicklungskosten auch für signifikante Marktzutrittsbarrieren,[585] sodass die Entwicklung von datenschonenden Alternativen mit ähnlicher Reichweite wie Facebook äußerst unwahrscheinlich erscheint. Die einzige Möglichkeit, Nutzern mit stark ausgeprägten Datenschutzpräferenzen Zugang zu funktional hochwertigen sozialen Netzwerken zu ermöglichen, besteht daher darin, die Netzwerke auf rechtlichem Wege zu verpflichten, eine datenschonende Option einzurichten.

b) Suchmaschinen

Ganz ähnlich stellt sich die Situation auf dem Markt für Suchmaschinen dar. Die mit Abstand führende Suchmaschine, Google, bietet ebenso wie die großen Konkurrenten Yahoo und Bing keine einfach zu handhabende datenscho-

[578] https://sociall.io/.

[579] https://www.minds.com/.

[580] https://mewe.com/.

[581] Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 413: mehr als 90 % Marktanteil von Facebook auf dem relevanten Markt; ebd., Rn. 417: „Lediglich Facebook.com bietet sämtliche Funktionalitäten zur Abbildung eines virtuellen sozialen Raumes an"; *Hacker/Petkova*, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1 (21); *Raue*, JZ 2018, 961 (965 f.); *Martinelli*, in: Reins (Hrsg.), Regulating New Technologies in Uncertain Times, 2019, 133 (136).

[582] Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 218, 221; *Künzler*, Direct Consumer Influence – The Missing Strategy to Integrate Data Privacy Preferences into the Market, Working Paper, 2019, https://ssrn.com/abstract=3395928, 12 f.

[583] Bundeskartellamt, Beschluss vom 6.2.2019, B6–22/16, Rn. 220; *Katz/Shapiro*, 75 American Economic Review 1985, 424; *Shy*, 38 Review of Industrial Organization 2011, 119 (120); *Haucap/Heimeshoff*, 11 International Economics and Economic Policy 2014, 49 (51, 58 f.).

[584] *Katz/Shapiro*, 75 American Economic Review 1985, 424; *Belleflamme/Peitz*, Industrial Organization, 2010, 549; *Shy*, 38 Review of Industrial Organization 2011, 119 (120); *Engert*, AcP 213 (2013), 321 (325); *Haucap/Heimeshoff*, 11 International Economics and Economic Policy 2014, 49 (51); *Monopolkommission*, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015, Rn. 300.

[585] *Lianos/Motchenkova*, 9 Journal of Competition Law & Economics 2013, 419 (428); *Monopolkommission*, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015, Rn. 302; *Rubinstein/Gal*, 59 Arizona Law Review 2017, 339 (349 ff.).

nende Option.[586] Der kleine Wettbewerber DuckDuckGo respektiert zwar umfänglich die Privatsphäre,[587] bietet jedoch eine gegenüber den dateninvasiven Konkurrenten deutlich reduzierte Suchleistungsperformance.[588] Denn auch hier wirken sich Netzwerk- und Skaleneffekte aus,[589] die durch kleinere Wettbewerber nur sehr schwer überwunden werden können. Jedenfalls bis zu einem gewissen Punkt gilt: Je größer das Korpus an historischen Suchanfragen und Clicks (*query logs*), auf das die Maschine zugreifen kann, desto akkurater die Treffer.[590] Wiederum können Nutzer mit stark ausgeprägten Datenschutzpräferenzen daher keinen Zugang zu besonders leistungsfähigen Angeboten, hier Suchmaschinen, erhalten.

c) IoT-Geräte, besonders autonome Fahrzeuge

Ein weiterer Sektor, in dem die rechtliche Verankerung einer datenschonenden Option sinnvoll erscheint, ist jener der IoT-Geräte.[591] Auch hier lässt sich die Weiterleitung von Daten zu nicht funktionalen Zwecken typischerweise bislang nicht einfach begrenzen.[592] Dies ist insbesondere deshalb misslich, weil es sich häufig um besonders aufschlussreiche oder sensible Daten handelt, die in der Privat- oder gar Intimsphäre der betroffenen Personen erhoben werden. Gerade bei komplexen Produkten, wie etwa autonomen und vernetzten Fahrzeugen, sind zudem so hohe Entwicklungskosten zu konstatieren,[593] dass ein Markteinstieg von datenschonenden Wettbewerbern nicht abzusehen ist.

Einige Initiativen zeigen zwar, dass das Bewusstsein für Datenschutz und Nutzerkontrolle in der Industrie steigt.[594] Nichtsdestoweniger sollte bereits zum jetzigen Zeitpunkt ein Recht auf eine datenschonende Option imple-

---

[586] Siehe für Google *Forbrukerrådet*, Deceived by Design, Bericht, 2018, 35 f.; die Dashboards von Yahoo und Bing funktionieren ähnlich.

[587] https://duckduckgo.com/privacy.

[588] *Argenton/Prüfer*, 8 Journal of Competition Law and Economics 2012, 73; *Haucap/Heimeshoff*, 11 International Economics and Economic Policy 2014, 49 (56).

[589] *Haucap/Heimeshoff*, 11 International Economics and Economic Policy 2014, 49 (51, 54 f.); *Monopolkommission*, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015, Rn. 200 ff.

[590] *Argenton/Prüfer*, 8 Journal of Competition Law and Economics 2012, 73 (76); *Lianos/Motchenkova*, 9 Journal of Competition Law & Economics 2013, 419 (445); *Etro*, Search Advertising, Vox CEPR Policy Portal (11.6.2011), https://voxeu.org/article/search-advertising; Behauptung eines niedrigen Punktes, an dem zusätzliche Daten keinen positiven Effekt haben, allerdings ohne Begründung, bei *Manne/Wright*, 34 Harvard Journal of Law & Public Policy 2011, 171 (212); zu möglicher Substitution durch frei zugängliche Daten, die allerdings zu spezifischen Suchinhalten unwahrscheinlich erscheint, *Monopolkommission*, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015, Rn. 203.

[591] Siehe bereits *Hacker*, 7 International Data Privacy Law 2017, 266 (281); *Becker*, JZ 2017, 171 (175 ff.).

[592] Siehe oben, Text bei § 6, Fn. 321.

[593] Siehe etwa *Becker*, Die 100-Milliarden-Euro-Frage. Digitale Angebote im Auto, SZ (13.3.2019), https://www.sueddeutsche.de/auto/auto-vernetzung-digital-1.4358303.

[594] Siehe oben, § 6, Fn. 322.

mentiert werden, nicht nur um Datenschutzpräferenzen zur Durchsetzung zu verhelfen, sondern auch um die Menge an unerwünscht erhobenen, sensiblen IoT-Daten und damit auch diesbezügliche negative Externalitäten[595] zu minimieren.[596] Sollten sich im Zuge der zunehmenden Markteinführung von IoT-Geräten in einzelnen Bereichen datenschonende Alternativen am Markt etablieren, deren Bestand auch ohne Pflicht zum Angebot einer solchen Alternative erwartet werden kann, so kann die rechtliche Verpflichtung bereichsspezifisch wieder aufgehoben werden. In Anbetracht der zunehmenden Vernetzung der privaten und öffentlichen Lebenswelt kann jedoch zum gegenwärtigen Zeitpunkt nach hier vertretener Ansicht nur ein rechtlicher Zwang zur Etablierung einer datenschonenden Option die Grundlage für die souveräne und autonome Durchsetzung heterogener Datenschutzpräferenzen im Internet der Dinge sein, etwa vermittels der bereits diskutierten Datenschutzassistenten.

5. Einwände

Den bereits diskutierten Argumenten für ein Recht auf eine datenschonende Option steht eine Reihe von möglichen Einwänden gegenüber, die im Folgenden erörtert werden, jedoch im Ergebnis nicht durchgreifen können.

a) Wirkungslosigkeit

Ein erster Einwand betrifft die Wirkmächtigkeit eines Rechts auf eine datenschonende Option selbst für diejenigen Personen, die es ausüben. So ließe sich argumentieren, dass das Recht für die wirksame Minimierung von datenschutzrechtlichen Risiken durch einen Nutzer flächendeckend, also für praktisch alle infrage kommenden Geräte, Dienste und Applikationen, ausgeübt werden müsste. Denn schon kleine Mengen an Daten können womöglich tief blicken lassen und werden häufig applikationsübergreifend zusammengeführt. Insofern könnte man meinen, es sei wirkungslos, lediglich bei großen Anbietern (zum Beispiel nur bei Facebook und Google) eine datenschonende Option zu wählen. Umgekehrt ist es jedoch unrealistisch anzunehmen, dass selbst Nutzer mit stark ausgeprägten Datenschutzpräferenzen bei *allen* Angeboten die datenschonende und damit monetär kostenpflichtige Alternative wählen. Hinzu kommt, dass, so möchte man meinen, die Einführung einer datenschonenden Option für all jene Nutzer wirkungslos ist, für die bereits Profile vorliegen, also die ganz überwiegende Anzahl derer, die sich gegenwärtig in der digitalen Wirtschaft bewegen. Diesem Einwand der Wirkungslosigkeit ist jedoch seinerseits eine Reihe von Erwägungen entgegenzuhalten.

---

595 Siehe oben, § 3 B.II.1.c).

596 Im Ergebnis so auch *Becker*, JZ 2017, 171 (175 ff.); *Hacker*, 7 International Data Privacy Law 2017, 266 (281).

aa) Wirksamkeit für Altnutzer

Erstens ist zwar zuzugeben, dass ein Recht auf eine datenschonende Option besonders neuen Nutzern zugutekommt, über die noch keine Profile vorliegen. Jedoch ist bekannt, dass Profildaten schnell veralten.[597] Inferenzen werden daher mit zunehmendem Zeitablauf immer unzuverlässiger. Bei Einstieg in eine datenschonende Option zu einem bestimmten Zeitpunkt nehmen die datenschutzrechtlichen Risiken für den Nutzer daher in der Folge grundsätzlich ab.[598] Zudem können sich auch Altnutzer neue digitale Identitäten zulegen, etwa mit Anti-Tracking-Tools. Schließlich spricht der reduzierte Nutzen einer datenschonenden Option in einer Übergangszeit nicht prinzipiell gegen ihre Einführung, wenn sich auf lange Sicht ihre Wirksamkeit erhöht, da dann der Anteil der neuen Nutzer (bezogen auf den Stichtag der Einführung) ständig steigt.

bb) Wirksamkeit trotz Datenerhebung an anderer Stelle

Zweitens werden datenbasierte Analysetechniken zwar immer wirkmächtiger. Auch lassen sich Individuen anhand von sehr wenigen Daten de-anonymisieren;[599] damit ist jedoch noch nichts über ihre weiteren Eigenschaften und Präferenzen gesagt. Zu deren Vorhersage benötigen auch die leistungsstärksten Modelle der Gegenwart, wie eingangs erwähnt,[600] in aller Regel immer noch eine erhebliche Anzahl an Daten.[601] Kleine Mengen an Daten verraten daher in dieser Hinsicht nicht allzu viel, zu groß ist die Varianz. Dies zeigt ein Blick auf die Studie, bei der mithilfe des Nutzungsverhaltens auf Facebook Persönlichkeitszüge abgeleitet wurden.[602] Das algorithmische Modell erreichte dabei eine Genauigkeit, die über der eines langjährigen Partners der betroffenen Per-

[597] *Mayer-Schönberger/Cukier*, Big Data: A revolution that will transform how we live, work, and think, 2013, Kapitel 6; *Bundesverband der digitalen Wirtschaft*, Data Economy, 2018, 19.

[598] Dies gilt unter der Voraussetzung, dass keine neuartigen Analysemöglichkeiten im Laufe der Zeit hinzukommen, die eine bessere Auswertung der Daten erlauben. Eine solche Entwicklung ist zwar technisch möglich, der Einsatz derartiger Instrumente wird aber in aller Regel datenschutzrechtswidrig sein, wenn keine Einwilligung des Nutzers vorliegt und er durch Ausübung des Rechts auf datenschonende Option im Sinne von Art. 21 DS-GVO widersprochen hat; siehe auch oben, Text bei § 4, Fn. 153.

[599] Siehe *Rocher/Hendrickx/de Montjoye*, 10 Nature Communications 2019, Article 3069; *Narayanan/Shmatikov*, Proceedings of the 2008 IEEE Symposium on Security and Privacy 2008, 111; *Sweeney*, Uniqueness of Simple Demographics in the U.S. Population, Laboratory for International Data Privacy, Working Paper LIDAP-WP4, 2000, 2f.; *Shu et al.*, 18 ACM SIGKDD Explorations Newsletter 2017, 5; und oben, § 4 A.II.2.a)aa)(2)(a)(aa).

[600] Siehe oben, § 2 B.III.

[601] Siehe *C. Sun et al.*, Proceedings of the IEEE International Conference on Computer Vision 2017, 843 (844); *Goodfellow/Bengio/Courville*, Deep Learning, 2016, 18ff.

[602] *Youyou/Kosinski/Stillwell*, 112 Proceedings of the National Academy of Sciences 2015, 1036.

son lag.[603] Dafür musste das Modell jedoch Kenntnis von über 250 Likes spezifischer Seiten (Autos, Musik etc.) auf Facebook haben. Schon bei Kenntnis von immerhin 200 Likes sank die Vorhersagegenauigkeit erheblich ab.[604] Für die beste (und absolut gesehen immer noch eher moderate: Pearsons r = 0,66) Vorhersagegenauigkeit mussten gar 500 Likes verfügbar sein.[605] Da Webseitenbesuche nicht mit aktiven Likes gleichgesetzt werden können (man kann sich auch über Dinge informieren, zu denen man kritisch steht), dürfte die Zahl der notwendigen Observationen außerhalb eines einzelnen Netzwerks noch deutlich höher liegen.

cc) Strategische Nutzung bei sensiblen Daten

Betroffene Personen können daher insbesondere bei solchen Geräten, Diensten oder Applikationen auf datenschonende Optionen umsteigen, bei denen sensible Daten in größerer Menge anfallen. Auch diese können zwar teilweise aus anderen Daten abgeleitet werden, aber eben nicht mit der gleichen Konfidenz wie bei einer direkten Messung.[606] Im Übrigen darf nicht verkannt werden, dass die Aggregation und anschließende Analyse von Daten, die bei der Wahl von datenintensiven Optionen gewonnen werden, durch das Datenschutzrecht stark begrenzt wird. Soweit diesbezügliche Risiken noch weiter reduziert werden sollen, kann dies durch flankierende regulatorische Maßnahmen, etwa die bereits angesprochene schwarze Liste für Art. 6 Abs. 1 lit. f DS-GVO,[607] umgesetzt werden. Dies zeigt einmal mehr, dass auch die datenschonende Option keine Pauschallösung bietet, sondern Teil eines Maßnahmenpakets sein muss, das unterschiedliche Risiken adressiert. Auch bei Verabschiedung lediglich eines Rechts auf eine datenschonende Option kann diesem jedoch eine signifikante Wirksamkeit nicht abgesprochen werden.

b) Zwei-Klassen-Datengesellschaft

Ein zweiter Einwand geht dahin, dass die Einführung eines Rechts auf eine datenschonende, aber monetär zu bezahlende Option zu einer Zwei-Klassen-Datengesellschaft führt, bei der sich nur noch die Wohlhabenden Datenschutz leisten können.[608] Dieses Argument greift jedoch gegenüber dem hier gemach-

---

[603] *Youyou/Kosinski/Stillwell*, 112 Proceedings of the National Academy of Sciences 2015, 1036 (1038).

[604] *Youyou/Kosinski/Stillwell*, 112 Proceedings of the National Academy of Sciences 2015, 1036 (1038); siehe auch *Kosinski/Stillwell/Graepel*, 110 Proceedings of the National Academy of Sciences 2013, 5802 (5804).

[605] *Youyou/Kosinski/Stillwell*, 112 Proceedings of the National Academy of Sciences 2015, 1036 (1037).

[606] Siehe oben, § 4 B.I.3.b)dd)(2).

[607] Siehe oben, § 4 C.I.4.

[608] *Härting*, CR 2016, 646 (648 f.); *Krohm/Müller-Peltzer*, ZD 2017, 551 (553) für den Fall eines hohen Entgelts für die datenschonende Option; siehe auch *Schulz*, in: Gola, DS-GVO,

ten Vorschlag in mehrfacher Hinsicht nicht durch. Zuzugeben ist allerdings, dass bei vielen Angeboten zwei unterschiedliche Datenschutzniveaus implementiert werden – dies ist ja auch gerade Ziel des Vorschlags, da dadurch Wahlfreiheit geschaffen wird. Ferner muss in der Tat berücksichtigt werden, dass die Zahlungsbereitschaft für eine Datenschutzprämie bei Besserverdienenden grundsätzlich stärker ausgeprägt ist.[609] Dennoch führen die distributiven Konsequenzen des Vorschlags nicht zu einem Zustand, der als Zwei-Klassen-Datengesellschaft bezeichnet werden könnte.

aa) Pareto-Verbesserung

Dies liegt erstens daran, dass der Begriff „Zwei-Klassen-Datengesellschaft" impliziert, dass in der datenintensiven Option nur „Datenschutz zweiter Klasse" geboten würde. Dies übersieht jedoch, dass für diese Alternative das Datenschutzrecht genau wie vor Einführung des Rechts auf eine datenschonende Option bestehen und durchgesetzt würde. Es ergäbe sich mithin keine Veränderung der Rechtslage für all jene, die nicht die datenschonende Option auswählen. Das Recht auf diese Option stellt sich daher als Pareto-Verbesserung dar:[610] Für Nutzer mit stark ausgeprägten Datenschutzpräferenzen bietet es einen vorzugswürdigen Zustand, für alle anderen ändert sich in der Sache nichts, sie werden mithin nicht schlechter gestellt.

Ein faktischer Unterschied besteht lediglich darin, dass in der Folge des Angebots einer datenschonenden Option Art. 7 Abs. 4 DS-GVO regelmäßig leerläuft und daher in der datenintensiven Version auch Einwilligungen wirksam sind, wenn diese z. B. mit *tracking walls* verknüpft werden.[611] Dies ist jedoch Konsequenz des geltenden Rechts und bereits jetzt, auch ohne eine Einführung des Rechts auf eine datenschonende Option, die Folge von deren freiwilliger Einführung durch einen Anbieter.[612] Insofern wird es den Anbietern nicht ermöglicht, das Datenschutzniveau gegenüber den *de lege lata* zur Verfügung stehenden Optionen abzusenken.

bb) Preiskontrolle

Der zutreffende Kern des Einwands der Zwei-Klassen-Datengesellschaft liegt vielmehr darin, dass eine datenschonende Option nur dann zur Etablierung von Wahlfreiheit sinnvoll ist, wenn sichergestellt wird, dass ihre monetäre Bepreisung nicht zu ihrer faktischen wirtschaftlichen Unverfügbarkeit für einen

2. Aufl. 2018, Art. 7 DS-GVO Rn. 30; *Calo*, 82 George Washington Law Review, 2014, 995 (1048) (Gefahr der Verschärfung des *digital divide*).

609 Dazu oben, § 6 C.II.2.a)aa).

610 Siehe zum Begriff der Pareto-Verbesserung etwa *Varian*, Intermediate Micro-Economics, 8. Aufl., 2010, 15; *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, 5. Aufl. 2012, 13.

611 Siehe oben, § 4 B.I.3.a)dd)(3)(b)(bb).

612 Siehe nochmals § 4 B.I.3.a)dd)(3)(b)(bb).

Großteil der Nutzer führt.[613] Böte etwa Facebook eine datenschonende Option für 50 € im Monat an, so wäre angesichts der durchschnittlichen Budgetrestriktionen von Nutzern in der Sache nicht viel gewonnen. Angesichts negativer Reputationseffekte ist dies zwar unwahrscheinlich, zur Lenkung von Nutzern in die dateninvasive Option jedoch auch nicht vollständig ausgeschlossen.[614] Die genannten Netzwerkeffekte könnten dann einen wirksamen Preiswettbewerb, der zu einer Senkung der Preise für die datenschonende Option führen würde, verhindern.[615]

Daher muss, wie der Verfasser an anderer Stelle bereits ausgeführt hat,[616] die datenschonende Option mit einem Regime der (behutsamen) Preiskontrolle verbunden werden.[617] Dies lässt sich implementieren durch eine Inversion des Kontrollmechanismus, der im Kartellrecht zur Durchsetzung des Verbots der gezielten Kampfpreisunterbietung (*predatory pricing*, Art. 102 S. 1 AEUV) bemüht wird: Während übliche Angebote nicht unter den Grenzkosten abgegeben werden dürfen,[618] sollte die datenschonende Option nicht signifikant über den Grenzkosten bepreist werden dürfen (*inverse predatory pricing approach*).[619] Sind die Grenzkosten nicht bekannt, können die – typischerweise leichter zu berechnenden[620] – durchschnittlichen variablen Kosten als Näherung verwendet werden.[621] Wenn auch diese nicht bestimmt werden können, muss auf ein anderes Kriterium umgestellt werden: den marginalen Wert der

---

613 *Krohm/Müller-Peltzer*, ZD 2017, 551 (553); *Irion/Luchetta*, Online Personal Data Processing and EU Data Protection Reform, CEPS Task Force Report, 2013, 38.

614 *Hoofnagle/Whittington*, 61 UCLA Law Review 2014, 606 (662).

615 Zu den Netzwerkeffekten bereits oben, § 6 C.II.4.a) und b); siehe ferner *Hacker/Petkova*, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1 (25).

616 *Hacker/Petkova*, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1 (25 f.).

617 Ähnlich auch *Golland*, MMR 2018, 130 (134 f.); *Novotny/Spiekermann*, Personal Information Markets AND Privacy: A New Model to Solve the Controversy, in: Hildebrandt et al. (Hrsg.), Digital Enlightenment Yearbook 2013, 2013, 102 (108); *Irion/Luchetta*, Online Personal Data Processing and EU Data Protection Reform, CEPS Task Force Report, 2013, 38; *Becker*, JZ 2017, 171 (178 f.).

618 *Areeda/Turner*, 88 Harvard Law Review 1975, 697 (712 ff.); *Baumol*, 39 The Journal of Law and Economics 1996, 49 (49); vgl. auch EuGH, Urt. v. 3.7.1991 – Rs. 62/86 (*AKZO*) – Rn. 72 (kein Verkauf unter durchschnittlichen Gesamtkosten bei Vorliegen eines Verdrängungsplans); EuG, Urt. v. 6.10.1994 – T-83/91 (Tetra Pak II) – Rn. 149; EuGH, Urt. v. 14.11.1996 – Rs. C-333/94 P (*Tetra Pak II*) – Rn. 42; *Fuchs*, in: Immenga/Mestmäcker, Wettbewerbsrecht, 6. Aufl. 2019, Art. 102 AEUV Rn. 235.

619 *Hacker/Petkova*, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1 (26): Grenze bei 150 % der Grenzkosten.

620 *Areeda/Turner*, 88 Harvard Law Review 1975, 697 (716); *Giocoli*, 18 The European Journal of the History of Economic Thought 2011, 777 (795 f.).

621 EuGH, Urt. v. 3.7.1991 – Rs. 62/86 (*AKZO*) – Rn. 71 f.; EuG, Urt. v. 6.10.1994 – T-83/91 (Tetra Pak II) – Rn. 148; EuGH, Urt. v. 14.11.1996 – Rs. C-333/94 P (*Tetra Pak II*) – Rn. 42; grundlegend die theoretische Vorarbeit von *Areeda/Turner*, 88 Harvard Law Review 1975, 697 (716–718); siehe auch *Fuchs*, in: Immenga/Mestmäcker, Wettbewerbsrecht, 6. Aufl. 2019, Art. 102 AEUV Rn. 234 ff.; *Baumol*, 39 The Journal of Law and Economics 1996, 49.

Verarbeitung personenbezogener Daten.[622] Die Preisobergrenze für eine datenschonende Option muss sich dann am durchschnittlichen Wert der personenbezogenen Daten für den Anbieter orientieren, abzüglich des Gewinns aus nicht personalisierter Werbung,[623] vermehrt jedoch um, vom Anbieter jeweils zu belegende, Mehrkosten für die Erbringung der datenschonenden gegenüber der dateninvasiven Option.

Empirische Untersuchungen legen nahe, dass der marginale Wert der personenbezogenen Daten bei Facebook zwischen einem und vier Euro pro Monat beträgt.[624] In dieser Dimension müsste daher der obere Grenzwert eines monetären Angebots liegen. Angesichts der durchschnittlichen, in einer Befragung ermittelten Zahlungsbereitschaft deutscher Nutzer für datenschonende Angebote in Höhe von 41 € pro Jahr[625] dürfte selbst eine an der Obergrenze orientierte Bepreisung für Nutzer mit stark ausgeprägten Datenschutzpräferenzen, deren Zahlungsbereitschaft höher liegen dürfte, eine realistische Option darstellen. Schon aus Reputationsgründen ist jedoch ein monetärer Preis unterhalb der Obergrenze wahrscheinlich.[626]

Wegen der Schwierigkeit der Berechnung der Grenzkosten bzw. des marginalen Werts personenbezogener Daten[627] wird auch diese Preiskontrolle im Wesentlichen als eine Form der Exzesskontrolle stattfinden müssen.[628] Der vielleicht wichtigste Anreiz für Anbieter, moderate Preise für die datenschonende Option zu verlangen, dürfte darin liegen, dass bei überhöhtem Preis keine zumutbare Alternative im Sinne des Kopplungsverbots des Art. 7 Abs. 4 DS-GVO angenommen werden kann und daher die Einwilligung hinsichtlich der dateninvasiven Option unwirksam zu werden droht.[629] Dies kann die Datenschutzrechtswidrigkeit der Verarbeitung in der dateninvasiven Variante zur Folge haben und damit nicht nur Schadensersatzansprüche (Art. 82 DS-GVO), sondern auch empfindliche Geldbußen und Sanktionen (Art. 83 f. DS-GVO) auslösen. Letztlich kann durch die aus dem Kartellrecht in abgewandelter Form übernommene Preiskontrolle die tatsächliche Wählbarkeit der datenschonenden Option für eine möglichst große Anzahl von Nutzern gewährleistet werden.

---

[622] *Hacker/Petkova*, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1 (26); *Golland*, MMR 2018, 130 (134 f.).

[623] *Golland*, MMR 2018, 130 (134 f.).

[624] *Hacker/Petkova*, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1 (23 f.); *Aziz/Telang*, What is a Cookie Worth?, Working Paper, 2016, https://ssrn.com/abstract=2757325, 30.

[625] *DIVSI*, Daten – Ware und Währung, 2014, 14.

[626] *Becker*, JZ 2017, 171 (179).

[627] *Krohm/Müller-Peltzer*, ZD 2017, 551 (553 f.); *Golland*, MMR 2018, 130 (135); ausführlich *Hacker*, in: Lohsse/Schulze/Staudenmayer (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, 2020, (im Erscheinen).

[628] Zu einer Datenexzesskontrolle nach Maßgabe von § 138 Abs. 1 BGB, siehe oben § 5 C.II.2.

[629] Siehe oben, § 4 B.I.3.a)dd)(3)(b)(bb).

cc) Kein Recht auf völlig kostenlose Leistung

Diejenigen, bei denen die Differenzen zwischen Datenschutzpräferenzen und Marktangebot nicht behoben werden, sind damit lediglich solche Nutzer, die stark ausgeprägte Datenschutzpräferenzen, aber nicht die finanzielle Ausstattung haben, um sich die monetäre Variante leisten zu können. Blickt man auf bislang angebotene datenschonende Optionen, so dürfte dies jedoch nur eine verschwindende Minderheit betreffen. Posteo und Tutanota etwa bieten einen datenschonenden E-Mail-Dienst für einen Euro pro Monat an.[630] Die Washington Post verzichtet gegen einen Aufpreis von ca. 2 € pro Monat auf *third-party tracking*.[631] Es handelt sich mithin um Beträge, die im Rahmen der Budgetrestriktionen der allermeisten Nutzer mit hohen Datenschutzpräferenzen liegen dürften.

Zwar ist nicht auszuschließen, dass einzelne Individuen mit hohen Datenschutzpräferenzen nicht in der Lage oder willens sind, die verlangten monetären Beträge aufzubringen, auch wenn sie absolut gesehen gering sind. Jedoch ist dies in einer marktwirtschaftlich strukturierten Konsumgesellschaft keine Besonderheit. Wer nicht bereit ist, entweder monetär oder datenbasiert für eine Leistung zu zahlen, kann sie nicht in Anspruch nehmen. Es gibt kein Recht auf eine völlig kostenlose Leistung – auch und gerade nicht in der digitalen Wirtschaft.

c) Mangelnde Stabilität von Präferenzen

Ein dritter Einwand gegen eine datenschonende Option könnte lauten, dass damit Datenschutzpräferenzen zur Durchsetzung verholfen werden soll, diese Präferenzen jedoch instabil und stark kontextabhängig sind. Dies ist, wie bereits ausgeführt, als empirische Feststellung zutreffend.[632] Die Konsequenz kann jedoch nicht sein, dass die Durchsetzung von Datenschutzpräferenzen überhaupt kein legitimes rechtliches Ziel sein könnte. Vielmehr muss es ausreichen, dass der Nutzer eine initiale Entscheidung (für eine dateninvasive oder eine datenschonende Option) korrigieren kann. So kann die Einwilligung jederzeit nach Art. 7 Abs. 3 DS-GVO widerrufen und ein monetärer Vertrag im Rahmen des gesetzlich oder vertraglich Zulässigen gekündigt werden. Dergestalt können Nutzer zwischen den Optionen wechseln und gewandelte Präferenzen zur Geltung bringen. Datenschutzassistenten können wiederum bei der Modellierung von Präferenzen helfen[633] und womöglich einen Hinweis geben, sobald die initiale Entscheidung nicht mehr den ermittelten aktuellen Präferenzen entspricht.

---

[630] Posteo, Konditionen, https://posteo.de/site/leistungen; https://tutanota.com/de/pricing.

[631] https://www.washingtonpost.com/gdpr-consent/; das datenschonende Abo des Standard kostet 6 € monatlich, siehe https://abo.derstandard.at/pur-faq/.

[632] Siehe oben, § 6 C.I.3.b)bb)(2)(b).

[633] Siehe oben, § 6 C.I.3.a)bb) und § 6 C.I.3.b)bb)(2)(b).

d) Mangelnde Rationalität

Zuletzt ist kritisch zu konstatieren, dass eine datenschonende Option allein, auch wenn sie mit einem *privacy score* gekoppelt wird, keine rationale Wahl durch die Nutzer verbürgen kann, da weiterhin verhaltensökonomische Effekte eine verzerrte Bewertung der verschiedenen Optionen bewirken können.[634] Insbesondere der Vergleich zwischen einem monetären und einem rein datenbasierten Preis ist in der Tat anspruchsvoll.[635]

Auch hier muss man jedoch wiederum klarstellen, dass die datenschonende Option kein Allheilmittel gegen jegliche Formen von Marktversagen im Bereich der digitalen Wirtschaft darstellen kann.[636] Ganz allgemein wird man rationale Entscheidungen über datenschutzrechtliche oder andere Fragestellungen nie garantieren können. Wie gesehen, könnte eine datenschonende Option nach entsprechenden empirischen Tests mit *debiasing*-Maßnahmen verbunden werden, um verhaltensökonomischen Effekten entgegenzuwirken.[637] Wichtiger noch erscheint jedoch, dass eine individuelle Entscheidung, nach hier vertretener Auffassung, auch dann autonom erfolgen kann, wenn sie Rationalitätsdefizite aufweist.[638] Insofern ändert beschränkte Rationalität nichts an der Tatsache, dass das Recht auf eine datenschonende Option einen echten Fortschritt für die autonome Durchsetzung von Datenschutzpräferenzen bieten würde.

6. Grundrechtskonformität

Zu guter Letzt müsste das Recht auf eine datenschonende Option mit höherrangigem Recht, insbesondere den Grundrechten, vereinbar sein. Sinnvoll ist die Verankerung des diskutierten Rechts auf unionaler Ebene, zum Beispiel im Rahmen des Erlasses der ePrivacy-Verordnung. Art. 16 Abs. 2 AEUV kann dafür als Kompetenzgrundlage herangezogen werden. Daher bilden die Unionsgrundrechte den Prüfungsmaßstab.[639] Das Recht auf eine datenschonende Option muss sich daher als schonender Ausgleich zwischen den verschiedenen unionalen Grundrechtspositionen der betroffenen Akteure bewähren.

a) Betroffene unionale Grundrechtspositionen

In die Abwägung ist nicht nur das Datenschutzgrundrecht (Art. 8 Abs. 1 GRCh) und, je nach Form des Angebots, das Recht auf Informationsfreiheit (Art. 11 Abs. 1 GRCh) der Nutzer mit stark ausgeprägten Datenschutzpräfe-

634 Siehe oben, § 3 B.II.1.b).
635 *Hermstrüwer*, 8 JIPITEC 2017, 9 Rn. 49 f.
636 Vgl. *Calo*, 82 George Washington Law Review, 2014, 995 (1048).
637 Siehe oben, § 6 C.I.2.b).
638 Siehe den Text bei § 6, Fn. 23 f.
639 Art. 51 Abs. 1 S. 1 GRCh; BVerfG NJW 1987, 577 (582) – Solange II; BVErfG NJW 2000, 3124 (3125) – Bananenmarktordnung; BVErfG NVwZ 2007, 937 (938).

renzen einzustellen, sondern auch die Vertragsfreiheit, und allgemeiner die unternehmerische Freiheit der Anbieter (Art. 16 GRCh[640]), die zur Akzeptanz einer bestimmten Zahlungsmodalität gezwungen werden.[641] Das Datenschutzgrundrecht der Nutzer mit lediglich mittel bis niedrig ausgeprägten Datenschutzpräferenzen ist nach dem oben Gesagten nicht negativ berührt, da das Datenschutzniveau in der datenintensiven Option nicht abgesenkt wird. Vielmehr werden Rechtspositionen dieser Nutzer in zweierlei Hinsicht gestärkt. Erstens stützt die Einführung einer datenschonenden Option indirekt ihre Vertragsfreiheit, da der von diesen Nutzern gewünschte Einsatz von Daten als Gegenleistung im Rahmen der datenintensiven Option dadurch rechtssicher ermöglicht wird (durch die Ausschaltung von Art. 7 Abs. 4 DS-GVO).[642] Zweitens stärkt die datenschonende Option grundsätzlich auch das Schutzniveau ihres Datenschutzgrundrechts, da negative Externalitäten der Datenverarbeitung, die auch Erkenntnisse über Nutzer der datenintensiven Option umfassen können, durch die Reduzierung der insgesamt erhobenen Daten vermindert werden.[643]

b) Rechtfertigung

Ein Eingriff ist daher lediglich in die Vertragsfreiheit, und damit verbunden in die unternehmerische Freiheit, der Anbieter zu konstatieren. Die Rechtfertigung eines Eingriffs in ein Unionsgrundrecht setzt nach Art. 52 Abs. 1 S. 2 GRCh die Geeignetheit der Förderung eines legitimen Zwecks, die Erforderlichkeit der Maßnahme sowie eine Angemessenheit im Sinne einer Bewältigung der Kollision von Grundrechtspositionen voraus.[644] Ferner darf der Wesensgehalt nicht angetastet werden,[645] was hier jedoch außer Zweifel steht.

Zum grundgesetzlichen Recht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht klargestellt, dass „dem Einzelnen ein informationeller Selbstschutz auch tatsächlich möglich und zumutbar sein [muss]. Ist das nicht der Fall, besteht eine staatliche Verantwortung, die Voraussetzungen selbstbestimmter Kommunikationsteilhabe zu gewährleisten."[646] Daraus

---

640 EuGH, Urt. v. 18.7.2013 – Rs. C-426/11 (*Alemo-Herron*) – Rn. 32.

641 Vgl. auch *Wagner/Eidenmüller*, 86 University of Chicago Law Review 2019, 581 (606).

642 Siehe oben, § 6 C.II.1.c)bb).

643 Vgl. oben, § 3 B.II.1.c).

644 EuGH, Urt. v. 13.4.2000 – Rs. C-292/97 (*Karlssohn*) – Rn. 45; Urt. v. 13.7.1989 – Rs. 5/88 (*Wachauf*) – Rn. 18; *Terhechte*, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 52 GRCh Rn. 8 ff.; *Streinz/W. Michl*, in: Streinz, EUV/AEUV, 3. Aufl. 2018, GRCh, Art. 52 Rn. 16 ff.; *Schwerdtfeger*, in: Meyer/Hölscheidt, Charta der Grundrechte der Europäischen Union, 5. Aufl. 2019, Art. 52 Rn. 38; zum Verhältnismäßigkeitsgrundsatz im Unionsrecht auch allgemein *Trstenjak/Beysen*, EuR 2012, 265.

645 Art. 52 Abs. 1 S. 2 GRCh; EuGH, Urt. v. 13.4.2000 – Rs. C-292/97 (*Karlssohn*) – Rn. 45; Urt. v. 13.7.1989 – Rs. 5/88 (*Wachauf*) – Rn. 18; *Terhechte*, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 52 GRCh Rn. 7.

646 BVerfG MMR 2007, 93 (93).

folge eine Schutzpflicht,[647] „die rechtlichen Voraussetzungen eines wirkungsvollen informationellen Selbstschutzes bereitzustellen".[648] Diese Erwägungen lassen sich auch auf die hier in Rede stehende datenschonende Teilhabe an datenbasierten Austauschprozessen übertragen, wenngleich Prüfungsmaßstab die Unionsgrundrechte, und nicht jene des GG, sind.

Das Recht auf eine datenschonende Option ist grundsätzlich geeignet, einen legitimen Zweck – die Verwirklichung von Autonomie und die Durchsetzung des Datenschutzgrundrechts der Nutzer[649] – zu fördern. Denkbar und empfehlenswert ist allerdings, zunächst Pilotprojekte in regulatorischen Experimentierräumen zu starten, um so die konkreten Auswirkungen und die Effektivität im Feld zu testen. Durch die Beschränkung auf Sektoren, in denen keine zumutbaren datenschonenden Alternativen am Markt bestehen, geht das Recht auch nicht über das zur Erfüllung des genannten Zwecks Erforderliche hinaus. Mildere, aber ebenso effektive Mittel sind nach hier vertretener Auffassung gegenwärtig auch nicht ersichtlich. Wollte man lediglich das Einwilligungsregime verbessern, so würden damit, wie gezeigt, nicht mit hinreichender Sicherheit neue, datenschonende Alternativen geschaffen. Gleiches gilt für die Einführung eines *privacy score* ohne datenschonende Option. Umgekehrt bewirkt jedoch die Verpflichtung auf das Angebot einer datenschonenden Option ohne *privacy score* keine Reduktion der Unschärfe des Datenpreises. Eine breite, auch gesellschaftliche Debatte über mögliche mildere Mittel steht jedoch erst am Anfang und soll hier keineswegs abgeschnitten werden. Zentral dürfte für die Erforderlichkeit jedenfalls sein, an der Sektorspezifizität festzuhalten.

Im Kern läuft die grundrechtliche Bewertung des Rechts auf eine datenschonende Option auf die Abwägung zwischen dem Datenschutzgrundrecht der Nutzer mit stark ausgeprägten Datenschutzpräferenzen, leicht verstärkt durch die genannten Positionen der übrigen Nutzer, mit der Vertragsfreiheit der Anbieter hinaus. Dabei muss nach dem EuGH ein angemessenes Gleichgewicht zwischen allen anwendbaren Grundrechten hergestellt werden.[650] Entscheidend für die Abwägung dürfte sein, inwiefern man es als zumutbar erachtet, dass Nutzer mit stark ausgeprägten Datenschutzpräferenzen, statt einen datenschonenden Zugang zu verschiedenen Angeboten zu erhalten, auf eine Inanspruchnahme dieser Dienste verzichten. Denn Konsumverzicht ist in den betroffenen Sektoren regelmäßig in Ermangelung eines Rechts auf eine datenschonende Option die einzige realistische Möglichkeit zur Durchsetzung hoher Datenschutzpräferenzen.

---

[647] Siehe dazu auch *Mörsdorf*, JZ 2019, 1066 (1068) m. w. N.

[648] BVerfG MMR 2007, 93 (93).

[649] Zu kollidierenden Grundrechten als Schranke von Chartagrundrechten *Streinz/W. Michl*, in: Streinz, EUV/AEUV, 3. Aufl. 2018, GRCh, Art. 52 Rn. 17.

[650] EuGH, Urt. v. 7.3.2014 – Rs. C-314/12 (*UPC Telekabel*) – Rn. 63; ebenso Urt. v. 31.1.2013 – Rs. C-12/11 (*McDonagh*) – Rn. 62; Urt. v. 22.1.2013 – Rs. C-283/11 (*Sky Österreich*) – Rn. 58, 60; Urt. v. 6.9.2012 – Rs. C-544/10 (*Deutsches Weintor*) – Rn. 47; Urt. v. 29.1.2008 – Rs. C-275/06 (*Promusicae*) – Rn. 65 f.

Auch hier wird die Bewertung letztlich von der Relevanz der infrage stehenden Geräte, Dienste oder Applikationen, mithin dem betroffenen Bereich der digitalen Wirtschaft, abhängen. Hinsichtlich der oben untersuchten Sektoren (soziale Netzwerke; Suchmaschinen; IoT-Geräte) ist nach hier vertretener Auffassung ein Konsumverzicht jedoch keine zumutbare Alternative.[651] Denn damit werden datenschutzorientierte Nutzer in einer zunehmend vernetzten Welt von einem breiten, besonders innovativen Marktsegment ausgeschlossen. In dem Maße, in dem Datenerhebung und -verarbeitung im Internet der Dinge unentrinnbar wird (z. B. in einer Smart City),[652] ist Verzicht gar schlechterdings kaum mehr möglich. Das Recht auf eine datenschonende Option ist daher essenziell für die wirksame Ausübung von Autonomie in vernetzten Umgebungen.[653] Ein präferenzkonformer Datenschutz, und damit eine effektive Durchsetzung des Datenschutzgrundrechts, wäre ohne datenschonende Option für Individuen mit stark ausgeprägten Datenschutzpräferenzen praktisch kaum möglich.

Demgegenüber erscheint der Eingriff in die Vertragsfreiheit der Anbieter weniger gewichtig. Wie dargestellt ist die Umsetzung eines Rechts auf eine datenschonende Option technisch ohne Weiteres möglich und wird bereits jetzt von einigen Anbietern praktiziert. Die Anbieter werden letztlich nur dazu gezwungen, eine Zahlungsmodalität zu eröffnen, die ohnehin das gesetzliche Zahlungsmittel darstellt.[654] Die größte Belastung dürfte daher darin liegen, dass unterschiedliche Formen der Datenerhebung und weiteren Verarbeitung für die unterschiedlichen Optionen aufgebaut werden müssen.[655] Auch dies erscheint jedoch als vergleichsweise geringe Bürde,[656] da bereits nach geltendem Datenschutzrecht Datenschutz durch Technikgestaltung und Voreinstellungen gewährleistet sein muss (Art. 25 DS-GVO) und viele Anbieter, wenn auch auf gewundenen Pfaden, Möglichkeiten zum Opt-Out anbieten.[657] Die unterschiedliche Verarbeitung von Daten je nach Umfang der vom Nutzer erteilten Einwilligung muss daher nach hier vertretener Auffassung bereits jetzt zu großen Teilen praktiziert werden. Insgesamt überwiegen daher die grundrechtlich geschützten Interessen der Nutzer jene der Anbieter und streiten für die Grundrechtskonformität des Rechts auf eine datenschonende Option.

Wie bereits erwähnt sollte schließlich ein *privacy score* nur dann verpflichtend eingeführt werden, wenn er standardisiert und hinreichend valide ist.

---

651 Ebenso im Ergebnis *Becker*, JZ 2017, 171 (174).

652 Siehe oben, § 3 B.II.2.b).

653 Siehe bereits oben, § 6 A.; kritisch aber OLG Düsseldorf NZKart 2019, 495 (499 f.).

654 Art. 10 f. der Verordnung (EG) Nr. 974/98 des Rates vom 3. Mai 1998 über die Einführung des Euro, ABl. 1998 L 139/1.

655 Siehe oben, § 6, Fn. 463.

656 Vgl. auch *Wagner/Eidenmüller*, 86 University of Chicago Law Review 2019, 581 (606); *Hacker*, 7 International Data Privacy Law 2017, 266 (282).

657 Siehe oben, § 6 C.II.4.a) und b); *Forbrukerrådet*, Deceived by Design, Bericht, 2018, 31 ff.

Unter diesen Voraussetzungen stellt auch er keine unangemessene Belastung dar. Denn gerade durch die Einbeziehung eines *privacy score* wird der in der digitalen Wirtschaft in vielfacher Hinsicht gefährdete Wettbewerbsmechanismus signifikant gestärkt.[658] Die Verfügbarmachung eines hinreichend bestimmten Preissignals erscheint daher grundsätzlich, und anders als das Recht auf eine datenschonende Option nicht nur sektorspezifisch, als ein gerechtfertigter Eingriff in die Vertragsfreiheit der Anbieter.

7. Zusammenfassung zum Recht auf eine datenschonende Option

Das hier konzipierte Recht auf eine datenschonende Option beinhaltet drei zentrale Weichenstellungen. Erstens müssen Anbieter danach eine datenschonende Vertrags- oder Nutzungsoption zur Verfügung stellen, bei der lediglich technisch erforderliche Daten verarbeitet werden und kein datenbasiertes, sondern allenfalls ein monetäres Entgelt verlangt wird. Zweitens muss dies verbunden werden mit einem *privacy score*, der die Unterschiede hinsichtlich der Datenschutzrisiken der verschiedenen Optionen auf einen Blick sichtbar und vergleichbar macht. Drittens sollte ein Recht auf eine datenschonende Option jedoch nur sektorspezifisch eingeführt werden, sofern nämlich in einem bestimmten Bereich keine adäquaten datenschonenden Alternativen am Markt verfügbar sind. Dies liegt etwa bei sozialen Netzwerken, Suchmaschinen und dem Internet der Dinge nahe.

Für ein solches Recht sprechen im Wesentlichen vier Argumente. Erstens kann nur so die Durchsetzung stark ausgeprägter Datenschutzpräferenzen in den betroffenen Marktsegmenten erfolgen und Souveränität der Nutzer über ihre Daten partiell wiederhergestellt werden. Zweitens wird durch ein derartiges Recht auch Rechtssicherheit für Anbieter und Nutzer geschaffen, da eine Einwilligung im Rahmen der datenintensiven Option nicht mehr am Kopplungsverbot des Art. 7 Abs. 4 DS-GVO scheitern kann. Damit vermag das Recht auf eine datenschonende Option die beiden wichtigsten Pole heterogener Datenschutzpräferenzen rechtlich abzubilden. Drittens fördert eine aktive Wahl eine bewusste Entscheidung über datenschutzrechtliche Belange und wirkt rationaler Ignoranz entgegen. Zugleich muss es jedoch auch möglich sein, die Wahl automatisiert und antizipiert auszuüben, etwa durch Datenschutzassistenten, um eine Entscheidungsüberlastung zu verhindern. Viertens kann durch die Kopplung mit einem *privacy score* das bislang in datenbasierten Austauschprozessen unklare Preissignal präzisiert werden. Zugleich muss eine wirksame Preiskontrolle dafür sorgen, dass die datenschonende Option eine realistische Wahlmöglichkeit bleibt.

Insgesamt wirkt das Recht auf eine datenschonende Option damit mehreren der im dritten Kapitel identifizierten Typen von Marktversagen entgegen.

---

[658] Siehe oben, § 6 C.II.1.c)dd) und § 3 B.II.1.d).

Dadurch nicht adressierten Typen von Marktversagen muss mit anderen Maßnahmen begegnet werden. Durch die sektorspezifische Begrenzung und den gegenüber dem bereits jetzt datenschutzrechtlich Erforderlichen vergleichsweise milden Eingriff in die Vertragsfreiheit der Anbieter stellt sich das Recht auf eine datenschonende Option letztlich auch als angemessener Ausgleich zwischen den beteiligten Grundrechtspositionen dar.

D. Ergebnisse von § 6

1. (Privat-)Autonomie, Informiertheit und Datenschutzpräferenzen sind zwar nicht untrennbar, aber doch eng miteinander verwoben in vernetzten Umgebungen. Autonomes Handeln setzt dreierlei voraus: (i) die Ausbildung von Handlungspräferenzen; (ii) die hinreichend von externer Beeinflussung unabhängige Formierung dieser Präferenzen, insbesondere die Möglichkeit zu kritischer Reflexion der Beeinflussung; und (iii) schließlich die Möglichkeit der Durchsetzung der Präferenzen. Auch aus autonomietheoretischer Sicht gehört daher die Möglichkeit der Realisierung heterogener Datenschutzpräferenzen zu einer autonomieförderlichen Umgebung. Datenschutzrecht muss daher immer auch Datenermöglichungsrecht sein.

2. Ein erster Weg der Durchsetzung spezifischer Datenschutzpräferenzen kann sich auf technische Applikationen zur Minimierung von Datenschutzrisiken stützen. Auf Nutzerseite sind dies insbesondere *privacy-enhancing technologies* wie Verschlüsselungstechniken, Identity-Management-Systeme und Anti-Tracking-Tools. Sie müssen von Anbietern grundsätzlich toleriert werden. Bislang jedoch werden sie nur selten genutzt; ferner können sie auf technischem Wege überwunden werden. Daneben stehen zunehmend in der Informatik entwickelte Anwendungen maschinellen Lernens, die Datenschutzerklärungen, Nutzungsbedingungen oder Verarbeitungspraktiken automatisiert auf ihre Rechtmäßigkeit untersuchen können. Das größte Potenzial bieten diese Instrumente für Aufsichtsbehörden und mit Klagebefugnis ausgestattete Verbände. Problematische Angebote können so rapide und skalierbar ausfindig gemacht werden. Code etabliert sich damit als weitere Kontrollinstanz neben Nutzern und hergebrachten Rechtsdurchsetzungsinstitutionen.

3. Trotz erheblichen Potenzials haben diese Instrumente jedoch zwei Nachteile. Erstens provozieren sie einen technischen Rüstungswettbewerb mit Anbietern, welche die Analyse- und Blockierfunktionen der Applikationen zu umgehen suchen. Dies produziert nicht unerhebliche soziale Kosten. Zweitens können sie zwar die Informationslage von Nutzern verbessern, jedoch nicht aus sich heraus neue vertragliche Optionen zur Durchsetzung bestimmter Datenschutzpräferenzen schaffen.

4. Neben technische Lösungen muss daher ein rechtlicher Rahmen der Entscheidungsunterstützung treten. Dieser sollte sich einerseits auf die Verbesserung der Einwilligung und der Kommunikation von Datenschutzpräferenzen, andererseits auf die Verfügbarmachung datenschutzfreundlicher Angebote am Markt konzentrieren. Hinsichtlich des ersten Ziels lassen sich transparenzbasierte, verhaltensbasierte und technologiebasierte Ansätze unterscheiden. Während transparenzbasierte Ansätze bislang empirisch nur zu einer marginalen Verbesserung der Informationslage der Nutzer führen konnten und verhaltensbasierte Ansätze im Rahmen von Art. 25 DS-GVO bereits Anwendung finden, dürfte die Zukunft den technologiebasierten Maßnahmen gehören. Dazu zählen insbesondere selbstlernende Datenschutzassistenten, welche die Präferenzen der Nutzer prädiktiv modellieren, automatisiert oder gar autonom kommunizieren und datenverarbeitende Geräte, Dienste oder Applikationen, soweit möglich, präferenzkonform konfigurieren können.

5. Damit diese technologiebasierten Ansätze jedoch ihre volle Wirksamkeit entfalten können, müssen zwei rechtliche Anpassungen vorgenommen werden. Erstens muss die automatisierte und autonome Kommunikation von Datenschutzpräferenzen rechtswirksam und rechtssicher möglich sein. Nach hier vertretener, aber umstrittener Auffassung ist dies nach der DS-GVO und der deutschen Rechtsgeschäftslehre bereits der Fall. Vorzugswürdig wäre nichtsdestoweniger eine europäische Lösung im Rahmen der ePrivacy-Verordnung. Zweitens kann eine Kommunikation von Datenschutzpräferenzen nur dann gelingen, wenn zwischen Datenschutzassistenten einerseits und datenverarbeitenden Geräten, Diensten oder Applikationen andererseits ein sicherer Kommunikationskanal aufgebaut werden kann. Dieser muss durch eine verpflichtende Datenschutz-Schnittstelle gewährleistet werden.

6. Diese Formen der Verbesserung der Informiertheit der Nutzer und der Kommunikation ihrer Präferenzen müssen schließlich begleitet werden von einem Recht auf eine datenschonende Option. Dieses sollte sektorspezifisch dort etabliert werden, wo datenschonende Angebote am Markt nicht adäquat verfügbar sind. Anbieter und Nutzer mit schwach ausgeprägten Datenschutzpräferenzen profitieren davon ebenfalls, da mit Ausräumung des Kopplungsverbots datenintensive Optionen rechtssicher nutzbar sind. Das Dilemma individueller Kontrolle im Datenschutzrecht wird so gelöst. Zudem sollte das diskutierte Recht mit einem *privacy score* gekoppelt werden, um Vergleichbarkeit zwischen den verschiedenen Angeboten herzustellen. Nur durch die Verbindung von echter Wahlmöglichkeit mit automatisiert oder autonom intervenierenden Datenschutzassistenten kann sich in einer zunehmend vernetzten Umgebung eine residuale Form der Datensouveränität entfalten.

Teil 4

Schluss

§7 Lösungsansätze für die drei rechtlichen Herausforderungen, *de lege lata* und *de lege ferenda*

Im Folgenden werden noch einmal, gleichsam als thematisch fokussierte Zusammenfassung, die verschiedenen im Rahmen der Untersuchung gefundenen Lösungsansätze den drei eingangs der Arbeit benannten rechtlichen Herausforderungen systematisch zugeordnet. Dabei zeigt sich einmal mehr, dass für die Bewältigung der regulatorischen Spannungslagen, welche die nahezu ubiquitäre Datenverarbeitung in digital mediierten Austauschprozessen mit sich bringt, kein einfaches Allheilmittel zur Verfügung steht. Vielmehr bedarf es einer Kombination unterschiedlicher regulatorischer Strategien, um die verschiedentlichen Risiken der hier untersuchten neuen Technologien einzudämmen, aber auch ihr Potenzial für die privatautonome Gestaltung von Marktprozessen nutzbar zu machen.

A. Erste rechtliche Herausforderung: Multirelationalität von Daten

Die erste, im dritten Kapitel dieser Arbeit aus der zunehmenden Vernetzung digital basierter Austauschprozesse abgeleitete rechtliche Herausforderung besteht in der Multirelationalität der verarbeiteten personenbezogenen Daten.[1] Ihnen wohnt ein Drittbezug inne, der etwa beim Einsatz von Daten als Gegenleistung durch die vielfältigen Möglichkeiten der Monetarisierung von Daten unter Einbeziehung von Drittakteuren augenfällig wird. In der digital synchronisierten Welt präsentiert sich die Weiterleitung von personenbezogenen Daten an Dritte, die Datenerhebung durch Dritte sowie bei Dritten als übergreifender Problemkomplex, dem auch die drei Leitfälle dieser Arbeit gewidmet waren.[2] Lösungen zur Bewältigung dieses inhärenten Drittbezugs wurden auf zwei Ebenen erarbeitet, einer regulatorischen und einer ermöglichenden.

[1] §3 A.
[2] §3 D.I.

I. Regulatorische Dimension

Einerseits zeigte sich dabei, dass die Drittnutzung von Daten in allen Fallgestaltungen (Weiterleitung an Dritte, Datenerhebung durch Dritte und bei Dritten) nur unter strengen Voraussetzungen möglich sein kann, wenn das Ziel der individuellen Kontrolle betroffener Personen über die Verarbeitung ihrer Daten nicht vollends aufgegeben werden soll. Dies impliziert insbesondere, dass das Kopplungsverbot in Art. 7 Abs. 4 DS-GVO uneingeschränkt auch auf die Nutzung von Daten als Gegenleistung anwendbar ist[3] und mit Blick auf die Drittbezugsfälle streng ausgelegt werden muss.[4] Einwilligungserklärungen können insoweit nur wirksam sein, wenn die Verarbeitung der erfassten Daten zumindest einem von zwei Kriterien genügt: Entweder muss die Verarbeitung nach einem subjektiven Erforderlichkeitsmaßstab, unter Ausblendung etwaiger Nutzerpflichten zur Datenüberlassung oder zur Duldung der Verarbeitung,[5] mithin zur Erfüllung von wirksam vereinbarten Pflichten des datenschutzrechtlich Verantwortlichen notwendig sein;[6] oder es müssen, wenn Ersteres wie häufig bei drittbezogener Verarbeitung nicht der Fall ist, funktional äquivalente Alternativen zum Angebot des jeweiligen Anbieters am Markt vorhanden sein, die ohne eine Einwilligung in die betreffenden Vorgänge auskommen.[7] Dieses zweite Kriterium wird regelmäßig bei Märkten, die von erheblichen Netzwerkeffekten geprägt sind, ebenfalls nicht erfüllt werden können, da es insoweit an der funktionalen Äquivalenz fehlt.[8] Der Weg zu einer wirksamen Einwilligung führt dann *de lege lata* lediglich über das freiwillige Angebot einer datenschonenden Option durch den jeweiligen Anbieter, neben der von der Einwilligung erfassten datenintensiven: Dadurch wird die Kopplung von Diensterbringung und Einwilligung rechtswirksam aufgehoben.[9] Da dies ohne Weiteres technisch möglich ist, stellt die vorgelegte Interpretation das Modell datenfinanzierter Dienste auch nicht grundsätzlich infrage. Letztlich sollte eine zeitgemäße Auslegung des unionalen Datenschutzrechts daher darum bemüht sein, Fälle des funktional erforderlichen Drittbezugs von jenen abzugrenzen, die über diese Funktionalität hinausgehen, und für letztere Kategorie Anreize setzen, damit Anbieter tragfähige Alternativen für die Betroffenen zur Verfügung zu stellen.

Will der Anbieter diesen Weg des Angebots einer datenschonenden Alternative nicht freiwillig gehen, sondern sich statt auf die Einwilligung auf die Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f DS-GVO stützen, so sind auch

[3] § 4 B.I.3.a)dd)(5)(a)(aa).
[4] § 4 B.I.3.a)dd)(3).
[5] § 4 B.I.3.a)dd)(5)(a)(aa)a.
[6] § 4 B.I.3.a)dd)(3)(a)(aa)g.
[7] § 4 B.I.3.a)dd)(3)(b)(bb) und § 4 B.I.3.a)dd)(3)(c), besonders bei § 4, Fn. 574; für Cookies speziell § 4 B.I.4.b)aa)(2).
[8] § 4 B.I.3.a)dd)(5)(a)(aa)g und § 6 C.II.4.a).
[9] § 4 B.I.3.a)dd)(6).

hier strenge Anforderungen zu stellen.[10] Die erheblichen, mit dem Drittbezug einhergehenden datenschutzrechtlichen Risiken werden zwar nicht in allen Fällen, aber doch regelmäßig zu einem Überwiegen der Interessen der betroffenen Person führen.[11] Am ehesten ist eine Erlaubnis nach der Interessenabwägungsklausel bei der Erfassung personenbezogener Daten von Unbeteiligten durch IoT-Geräte und -Applikationen möglich, da hier regelmäßig keine alternativen Formen der datenschutzrechtlich wirksamen Legitimierung für die Anbieter zur Verfügung stehen.[12]

Diese Lesart der Interessenabwägungsklausel macht den Rückgriff auf die Rechtsgrundlage des Art. 6 Abs. 1 lit. b DS-GVO für Anbieter besonders attraktiv, kann hier doch durch die strategische Etablierung von Vertragspflichten eine Erlaubniswirkung erreicht werden. Jedoch gilt in diesem Rahmen derselbe subjektive Erforderlichkeitsmaßstab mit Ausblendung der Nutzerpflichten wie im Rahmen des Kopplungsverbots,[13] sodass weitergehende Datenverarbeitungsprozesse nur durch die Einführung von Pflichten des Verantwortlichen legitimiert werden könnten. Genau für diesen Fall besteht in der DS-GVO allerdings eine signifikante Schutzlücke, da im Grundsatz jegliche Vertragspflichten des Verantwortlichen Erlaubniswirkung entfalten. Diese Lücke kann und muss nach hier vertretener Auffassung durch das allgemeine Privatrecht geschlossen werden.[14] So unterliegen einseitig statuierte Vertragspflichten des Verantwortlichen einer Kontrolle durch das AGB-Recht und § 138 BGB,[15] die grundsätzlich auch Hauptleistungspflichten erfasst – infolge der im fünften Kapitel herausgearbeiteten Fälle von Marktversagen auch im Bereich der §§ 307 ff. BGB.[16] Mit dem hier erarbeiteten modifizierten *Aziz*-Test können für diese Kontrolle marktkonforme Maßstäbe, die sich an hypothetischen Verhandlungsergebnissen orientieren, benannt werden.[17] Die AGB-rechtliche Unangemessenheit indiziert dann regelmäßig auch den Verstoß gegen den datenschutzrechtlichen Grundsatz von Treu und Glauben.[18] So können die regulatorischen Dimensionen von allgemeinem Privatrecht und Datenschutzrecht ineinandergreifen, um ein sich wechselseitig ergänzendes Instrumentarium zur Erfassung konsensualer Datenverarbeitung entstehen zu lassen.[19]

---

[10] § 4 C.I.2.
[11] § 4 C.I.3.
[12] § 4 C.I.3.c).
[13] § 4 B.II.2.b)bb).
[14] Siehe Text bei § 4, Fn. 546 und 938.
[15] § 5 C.II.
[16] § 5 C.II.1.e)aa).
[17] § 5 C.II.1.e)aa)(3).
[18] § 5 C.II.1.g)cc).
[19] Zu den methodischen Grundlagen dieser wechselseitigen Ergänzung siehe § 5 A.

II. Ermöglichende Dimension

Auch hinsichtlich des Drittbezugs von Daten erschöpft sich das Datenprivatrecht jedoch nicht in einer regulatorischen Perspektive. Vielmehr wurde auch insoweit der Versuch unternommen, soweit als möglich diese Fallgruppen einer privatautonomen Regelung zwischen den jeweils beteiligten Parteien zugänglich zu machen.[20] Die Einbeziehung der jeweils Dritten kann dabei durch mehrseitige Verträge,[21] Stellvertretung,[22] Verträge zugunsten Dritter,[23] Bedingungen zugunsten Dritter,[24] oder auch durch Rechtsfiguren wie den Vertrag mit Schutzwirkung zugunsten Dritter erfolgen.[25] Da Verträge insoweit jedoch vielfach als Einwillungssubstitute fungieren, dürfen deren Voraussetzungen nicht durch die vorschnelle Annahme konkludenter Vertragsschlüsse unterlaufen werden. In Übertragung des Kriteriums der Unmissverständlichkeit der Einwilligung müssen daher auch vertragliche Gestaltungsvarianten grundsätzlich eine explizite Zustimmung der betroffenen Person vorsehen.[26] Für die Anbahnung, den Abschluss und die Implementierung derartiger vertraglicher Arrangements sollten und können nach hier vertretener Auffassung verstärkt auch autonome Assistenzsysteme genutzt werden, welche die zunehmend komplexen und hochfrequenten Verarbeitungsangebote in vernetzten, „smarten" Umgebungen zu navigieren helfen.[27]

B. Zweite rechtliche Herausforderung: Ambivalenz von Nutzen und Risiken

Die zweite regulatorische Herausforderung liegt in der Ambivalenz der geschilderten Datenverarbeitungsprozesse hinsichtlich Kosten und Nutzen.[28] Einerseits haben gerade adaptive, mit Methoden maschinellen Lernens operierende Formen der Datenverarbeitung ein erhebliches individuelles und auch soziales Potenzial,[29] andererseits lösen sie signifikante ökonomische und soziale Risiken aus.[30] Während die Feststellung dieser Ambivalenz nachgerade den Charakter eines Gemeinplatzes hat,[31] ist die Erarbeitung von Lösungen,

[20] § 5 B.III.
[21] § 5 B.III.2.a)aa).
[22] § 5 B.III.2.a)bb).
[23] § 5 B.III.2.a)cc); § 5 B.III.2.b)bb).
[24] § 5 B.III.2.a)dd).
[25] § 5 B.III.2.b)cc).
[26] § 5 B.III.2.b)aa)(1)(b)(cc).
[27] § 6 C.I.3.
[28] § 3 B.
[29] § 3 B.I.
[30] § 3 B.II.
[31] Siehe nur Picard, *Affective Computing*, 1997, 136.

die den unterschiedlichen Risiken und Möglichkeiten gerecht werden, ungleich diffiziler.

Einen flexiblen und übergreifenden Ansatzpunkt bietet die Interessenabwägungsklausel nach Art. 6 Abs. 1 lit. f DS-GVO, in deren Rahmen nach hier vertretener Auffassung nicht nur verarbeiterbezogene, drittbezogene und daraus folgende kollektive Vorteile der Verarbeitung, sondern – entgegen dem missverständlichen Wortlaut – auch dasselbe Spektrum an Risiken Berücksichtigung finden muss.[32] So können Verarbeitungsprozesse etwa erlaubt werden, wenn ein besonderes soziales Interesse an der Verarbeitung besteht; umgekehrt kann die Legitimierung abgelehnt werden, wenn sich besondere, auch kollektive Risiken manifestieren.[33] Insgesamt müssen hier jedoch dringend effektive Formen der rechtssicheren Operationalisierung dieser offen gestalteten Abwägungsklausel gefunden werden.[34]

I. Marktversagen

Spezifischere Formen von Regulierung beziehen sich auf die vier im dritten Kapitel identifizierten Formen von Marktversagen.[35] Hier wird das Bedürfnis einer Kombination unterschiedlicher Regulierungsinstrumente besonders augenfällig.

Einer Informationsasymmetrie zwischen Anbieter und Nutzer – sei sie rationaler Ignoranz oder Informationsüberlastung geschuldet[36] – können vor allem transparenzbasierte Ansätze entgegenwirken.[37] Aufgezeigt wurden insoweit Formen der automatisierten Analyse von Datenschutzerklärungen und von Vertragsbedingungen durch nutzerseitige Datenschutzassistenten,[38] Möglichkeiten der verbesserten Kommunikation von Pflichtinformationen[39] sowie die Einführung eines verpflichtenden *privacy score*, welcher die Höhe der erwartbaren datenschutzrechtlichen Risiken auf einen Blick, wenngleich notwendig approximativ, erfassbar macht.[40]

Verhaltensökonomischen Effekten wiederum, welche die rationale Entscheidung über Alternativen datenbasierter Austauschprozesse erschweren,[41] kann mit verhaltensbasierten Ansätzen entgegengetreten werden.[42] Allerdings ist hier insoweit Zurückhaltung angebracht, als deren Präzision (etwa im Fall

[32] § 4 C.I.2.a)bb).
[33] Siehe Text bei § 4, Fn. 999.
[34] § 4 C.I.4.
[35] § 3 B.II.1.
[36] § 3 B.II.1.a).
[37] § 6 C.I.1.
[38] § 6 B.II.1.
[39] § 6 C.I.1.a)aa).
[40] § 6 C.II.1.b)bb). und § 6 C.II.2.b).
[41] § 3 B.II.1.b).
[42] § 6 C.I.2.

von *debiasing*) jeweils empirisch vorab überprüft werden sollte.[43] Ein möglichst objektiver *privacy score* könnte jedoch auch in diesem Kontext zu einer Verbesserung beitragen, wenn in diesen die jeweiligen Risiken unverzerrt integriert werden. *Privacy by default*, häufig im Kontext verhaltensbasierter Ansätze genannt, legitimiert sich nach hier vertretener Auffassung hingegen vorrangig durch die Reduzierung negativer Externalitäten,[44] womit der dritte Typ von Marktversagen angesprochen ist.

Diese negativen Externalitäten der Datenverarbeitung sind gerade in der jüngeren ökonomischen Literatur stärker in den Vordergrund gerückt.[45] Der in der DS-GVO mittlerweile in einer spezifischen Spielart verortete Datenschutz durch Voreinstellungen senkt grundsätzlich die Menge der insgesamt vorhandenen Daten und kann daher negative Externalitäten, die zumeist durch die Analyse großer Datenmengen entstehen, tendenziell reduzieren.[46] Ferner müssen, wie bereits erwähnt, auch im Rahmen von Art. 6 Abs. 1 lit. f DS-GVO potenzielle negative Externalitäten in die Abwägung einbezogen werden.[47]

Die letzte und empirisch noch am wenigsten in der ökonomischen Literatur erfasste Form des Marktversagens geht von der Unschärfe des Datenpreissignals aus, das insofern seine dezentrale Steuerungsfunktion nur ungenügend erfüllen kann.[48] Dies impliziert einerseits, dass regulatorische Instrumente des Datenschutzrechts (Art. 6 Abs. 1 lit. f DS-GVO[49]) und des Zivilrechts (AGB-Kontrolle,[50] § 138 BGB[51]) stärker als bislang auch zu einer, wenngleich immer noch zurückgenommenen, Kontrolle des Äquivalenzverhältnisses der vertraglichen Hauptleistungspflicht berufen sind. Andererseits legt diese Unschärfe ebenfalls dringlich die Erarbeitung und Einführung eines *privacy score* nahe, damit der marktförmige Koordinationsmechanismus seine Steuerungswirkung auch unter den Rahmenbedingungen der digitalen Wirtschaft wieder voll entfalten kann.[52]

II. Soziale Risiken

Neben den genannten Formen von Marktversagen generiert die Konvergenz von Tracking-Technologien und künstlicher Intelligenz mit dem Internet der Dinge auch vier signifikante soziale Risiken, zu deren Reduzierung die genannten Vorschläge jedoch ebenfalls beitragen können.

---

[43] § 6 C.I.2.b).
[44] § 6 C.I.2.b) und § 4 C.III.2.
[45] § 3 B.II.1.c).
[46] § 4 C.III.2.
[47] § 4 C.I.2.a)bb).
[48] § 3 B.II.1.d).
[49] § 4 C.I.
[50] § 5 C.II.1.
[51] § 5 C.II.2.
[52] § 6 C.II.1.b)bb). und § 6 C.II.2.b).

Erstens lässt die Dauerschleife aus Tracking-Technologien, maschineller Datenanalyse und Adaptation von IoT-Geräten, die ihrerseits wiederum Daten erheben, bei signifikanten Teilen der Betroffenen ein Gefühl der Überwachung entstehen, welches *chilling*-Effekte verursacht.[53] Dies kann wiederum durch eine enge Limitierung der Weiterleitung von Daten an Dritte sowie der Erhebung durch Dritte und bei Dritten adressiert werden: Auch die Gefahr von *chilling*-Effekten spricht dafür, all jene Fälle, sofern keine äquivalenten Alternativangebote am Markt bestehen, auf das funktional notwendige Minimum zu begrenzen.[54]

Zweitens gewinnt die Datenerhebung und -analyse durch die wachsende Durchdringung des Lebensalltags zunehmend den Charakter der Unentziehbarkeit.[55] Analoge Entlastungsräume schrumpfen. Dies kann letztlich nur eine technologisch fundierte Navigation der verschiedenen Einwilligungsszenarien durch Datenschutzassistenten[56] verbunden mit einem, sogleich im Rahmen der dritten rechtlichen Herausforderung dargestellten, expliziten Recht auf eine datenschonende Option[57] abmildern.

Drittens kann auch das bislang häufig mangelnde Bewusstsein dafür, dass überhaupt eine spezifische Nachverfolgung und individualisierte Analyse vorgenommen wird,[58] durch transparenzbasierte Ansätze gestärkt werden. Dies ist insbesondere wichtig für IoT-Geräte, die zunehmend ein *Internet of Everything* aufbauen, ohne dass man ihnen ihre datenerhebenden Funktionen unmittelbar ansehen würde.[59]

Das vierte, hier nur am Rande thematisierte soziale Risiko, jenes der Diskriminierung,[60] wird schließlich partiell durch Art. 9 DS-GVO adressiert,[61] lässt sich jedoch durch einen simplen Verzicht auf die Erhebung und Analyse unmittelbar sensitiver Merkmale wegen deren Korrelation mit diversen anderen Merkmalen nicht befriedigend lösen. Hier kann die Implementierung von diskriminierungsreduzierenden Verfahren bereits auf der Code-Ebene (sogenannte *algorithmic fairness*) Abhilfe schaffen, wie der Verfasser andernorts dargelegt hat.[62] Dies zeigt nicht zuletzt, dass die sachgerechte Erfassung der in dieser Untersuchung verhandelten Risiken letztlich die Entwicklung eines Datenprivat-

---

[53] § 3 B.II.2.a).
[54] § 4 D. Punkt 11 und Text bei § 4, Fn. 1010.
[55] § 3 B.II.2.b).
[56] § 6 C.I.3.
[57] § 6 C.II.
[58] § 3 B.II.2.c).
[59] § 4 B.I.3.a)cc)(3)(c).
[60] § 3 B.II.2.d).
[61] § 4 B.I.3.b)dd).
[62] *Hacker*, 55 Common Market Law Review 2018, 1143 (1175 ff.); *Zehlike/Hacker/Wiedemann*, 34 Data Mining and Knowledge Discovery 2020, 163; siehe auch *Gesellschaft für Informatik*, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen, 2018, 39 ff., 91 ff.; *Wachter/Mittelstadt/Russell*, Why Fairness Cannot Be Automated: Bridg-

rechts erforderlich macht, welches über die Verbindung von Datenschutzrecht und bürgerlichem Recht hinausgeht.

C. Dritte rechtliche Herausforderung: Heterogenität von Datenschutzpräferenzen

Die dritte rechtliche Herausforderung – die Bewältigung heterogener Datenschutzpräferenzen[63] – liegt unmittelbar an der Schnittstelle von ermöglichendem und regulatorischem Privatrecht.[64]

I. Das Dilemma individueller Kontrolle

Eine zentrale Aufgabe rechtlicher Technikgestaltung dürfte künftig darin liegen, die tatsächlichen Möglichkeiten der Wahrnehmung von Privatautonomie, inklusive der effektiven Durchsetzung heterogener Datenschutzpräferenzen, unter den Bedingungen vernetzten Austauschs zu erhalten bzw. wiederherzustellen. Dies bedingt jedoch, jedenfalls in Teilen der digitalen Wirtschaft, regulatorische Eingriffe in die Marktstruktur. Denn das bisherige Regime zur privatautonomen Gestaltung datenbasierter Austauschprozesse leidet an einer doppelten Dysfunktionalität, dem Dilemma individueller Kontrolle im Datenschutzrecht.[65] Einerseits ist es rationalen Parteien mit niedrigen Datenschutzpräferenzen verwehrt, ihre Daten, angesichts des Kopplungsverbots in Art. 7 Abs. 4 DS-GVO und des unklaren Erforderlichkeitsmaßstab nach Art. 6 Abs. 1 lit. b DS-GVO, rechtssicher zur Erweiterung ihrer Budgetrestriktionen einzusetzen. Hinsichtlich der übrigen Nutzer hingegen versagt das individuelle Kontrollregime typischerweise wegen rationaler Ignoranz, verhaltensökonomischen Effekten und negativen Externalitäten. Es mangelt insoweit bereits an den empirisch-ökonomischen Voraussetzungen für die effektive Wahrnehmung von Privatautonomie. Heterogenität der Datenschutzpräferenzen wird normativ daher nur unzureichend bewältigt.

II. Ein Lösungsvorschlag in drei Schritten

Insgesamt erscheinen hier aus einer Vogelperspektive drei Schritte als notwendig. Erstens muss die datenschutzrechtliche Einwilligung in die allgemei-

---

ing the Gap Between EU Non-Discrimination Law and AI, Working Paper, 2020, https://ssrn.com/abstract=3547922.

[63] §3 C.

[64] Zu diesen Perspektiven auf Privatrecht, siehe §1 C.

[65] Siehe zusammenfassend §4 D. Punkte 4.–7. sowie §4 B.I.3.a)dd), §4 B.I.5. und §4 B.II.4.

ne Rechtsgeschäftslehre eingeordnet werden, die seit jeher das Spannungsverhältnis von Privatautonomie und konkurrierenden Interessenlagen aufzulösen bemüht ist.[66] Dabei zeigt sich jedoch, dass sich einige Grundkonzepte zivilrechtlicher Willenserklärungen nur eingeschränkt oder modifiziert auf die Einwilligung übertragen lassen.[67]

Zweitens muss die Kommunikation von Datenschutzpräferenzen, etwa durch automatisierte oder zunehmend autonome Datenschutzassistenten, effektiv und rechtlich wirksam möglich sein. Die informierte Einwilligung muss der technologischen Einwilligung weichen. Dafür zeichnen technologiebasierte Ansätze verantwortlich,[68] die über transparenz- und verhaltensbasierte Ansätze hinausgehen. Ihnen dürfte, angesichts der signifikanten Limitationen der beiden zuletzt genannten Ansätze,[69] die Zukunft gehören. Diese technologiebasierten Ansätze, welche sich aktiv der Techniken maschinellen Lernens für Präferenzmodellierung und -kommunikation bedienen, können ihr Potenzial jedoch nur entfalten, wenn nicht nur die Tatbestände der Einwilligung und des Stellvertretungsrechts *de lege lata* in einer die technologisch unterstützte Autonomie förderlichen Weise ausgelegt werden,[70] sondern *de lege ferenda* auch die Einrichtung von entsprechenden Kommunikationsschnittstellen auf Seiten der datenerhebenden Geräte und Applikationen vorgeschrieben wird.[71]

Drittens muss die Möglichkeit der Durchsetzung heterogener Datenschutzpräferenzen – unter den gegenwärtigen Umständen vor allem: stark ausgeprägter Datenschutzpräferenzen – durch sektorspezifische Marktregulierung gewährleistet werden.[72] Dafür sollte ein Recht auf eine datenschonende Option anerkannt werden, das immer dann greift, wenn derartige Angebote am Markt nicht in hinreichendem Maße bereitgehalten werden.[73] Dies ist nicht zuletzt Ausprägung des Gebots des verfassungsrechtlichen Minderheitenschutzes.[74] Erste Ansatzpunkte zu diesem Recht können sich bei entsprechender Auslegung bereits *de lege lata* aus dem Zusammenspiel von Art. 7 Abs. 4 DS-GVO und Art. 6 Abs. 1 lit. f DS-GVO ergeben.[75] Es sollte jedoch aus Gründen der Rechtsklarheit und zur Regelung von Einzelfragen ausdrücklich auf Unionsebene verankert werden.[76] Dieses Recht muss insbesondere, sofern es die Bedingungen dezentraler Koordination digitaler Märkte verbessern soll,[77] mit der

[66] § 5 B.II.
[67] § 5 B.II.2.
[68] § 6 C.I.3.
[69] § 6 C.I.1.b) und § 6 C.I.2.b).
[70] § 6 C.I.3.c)aa).
[71] § 6 C.I.3.c)bb).
[72] § 6 C.II.
[73] § 6 C.II.4.
[74] § 6 C.II.2.a)bb). und § 6 C.II.4.
[75] § 6 C.II.1.a).
[76] § 6 C.II.1.a).
[77] § 6 C.II.1.c)dd).

bereits erwähnten Pflichtangabe eines *privacy score* verbunden werden, der den Unterschied zwischen der datenintensiven und der datenschonenden Option auf einen Blick erfassbar macht.[78] Um letztere auch *de facto* als attraktive Angebotsvariante zu etablieren, sollte zudem eine Rahmenkontrolle des monetären Preises der datenschonenden Alternative unter Adaptation kartellrechtlicher Maßstäbe erfolgen (*inverse predatory pricing approach*).[79] So lässt sich einerseits die Wettbewerbsstruktur digitaler Märkte verbessern und andererseits zumindest eine Residualform von Privatautonomie erhalten: als technologisch moderierte Wahlfreiheit zwischen unterschiedlichen Datenverarbeitungsintensitäten in vernetzten Austauschprozessen.

[78] § 6 C.II.1.b)aa). und § 6 C.II.2.b).
[79] § 6 C.II.5.b)(2).

§ 8 Wesentliche Ergebnisse der Arbeit in zehn Thesen

1. Der Aufstieg technisch vernetzter Umgebungen, die Tracking-Technologien, Formen der künstlichen Intelligenz und das Internet der Dinge kurzschließen, überschreitet auch die Grenzen tradierter Rechtsgebiete. Dies macht den Aufbau und die systematische Durchdringung eines Datenprivatrechts erforderlich, welches das unionale Datenschutzrecht mit dem mitgliedstaatlichen Privatrecht verbindet.

2. Im Sinne einer doppelten Zuspitzung müssen dabei spezifische, aus der Konvergenz der genannten Basistechnologien gegen ein *Internet of Everything* resultierende regulatorische Risiken adressiert, zugleich jedoch auch die Funktionsbedingungen für die privatautonome Gestaltung von Rechtsverhältnissen soweit als möglich erhalten bzw. wiederhergestellt werden. Im Zuge dessen muss das Daten*schutz*recht zugleich als effektives, aber grundrechtssensibles Daten*ermöglichungs*recht verstanden werden.

3. Für die Integration des unionalen Datenschutzrechts in das Privatrecht muss methodisch zwar zwischen dem Anwendungsvorrang des Unionsrechts und einer Sachintegration von Normgruppen ebenengleicher (nationaler oder unionaler) Provenienz streng unterschieden werden. In beiden Fällen ist jedoch das aus der Rechtsprechung des EuGH entwickelte Kriterium der Risikospezifizität von entscheidender Bedeutung. Wenn nationale Rechtsnormen eigenständige Risiken adressieren, können sie die Regelungsprärogative des Unionsrechts grundsätzlich überwinden. Zugleich können anhand dieses Kriteriums unterschiedliche, unionsrechtlich determinierte Regelungsmaterien in ein sachgerechtes Verhältnis zueinander gebracht werden.

4. Hinsichtlich der drei hier behandelten Leitfälle, die sich jeweils durch einen Drittbezug der Datenverarbeitung auszeichnen, lässt sich übergreifend feststellen, dass auf Grundlage der bisher vorherrschenden Geschäftsmodelle die Datenweiterleitung zu Zwecken personalisierter Werbung oder zu nicht funktional erforderlicher Verarbeitung im Internet der Dinge (Leitfall 1), *third-party tracking* (Leitfall 2) sowie Datenerhebung bei Dritten in stark vernetzten Umgebungen (Leitfall 3) kaum in datenschutzrechtskonformer Weise durchgeführt werden kann. Damit sind datenbasierten Geschäftsmodellen, aber auch der Entwicklung des Internets der Dinge enge datenschutzrechtliche Grenzen gesetzt. Diese können jedoch vielfach bereits durch die freiwillige Eröffnung

einer datenschonenden Option durch die jeweiligen Anbieter überwunden werden, weil dann das datenschutzrechtliche Kopplungsverbot nicht mehr greift. Das Geschäftsmodell der Nutzung von Daten als Gegenleistung ist daher nicht grundsätzlich gefährdet, muss aber rechtskonform modifiziert werden.

5. Die datenschutzrechtliche Einwilligungserklärung kann und muss im Rahmen eines Datenprivatrechts in die Rechtsgeschäftslehre des BGB integriert werden. Sie stellt nach hier vertretener Auffassung eine geschäftsähnliche Handlung dar. Der Rückgriff auf Vorschriften des allgemeinen Teils des BGB kann jedoch nur beschränkt und punktuell erfolgen, um die Harmonisierungswirkung des unionalen Datenschutzrechts nicht über Gebühr zu gefährden. Insgesamt zeigen sich dabei erhebliche Unterschiede zwischen der Dogmatik der Einwilligung und jener der zivilrechtlichen Willenserklärung.

6. Auch für privatautonome Gestaltungen zwischen Anbieter und Nutzer gelten die allgemeinen Grenzen der Privatautonomie. Zwar schlägt die Datenschutzrechtswidrigkeit einer vertraglich vereinbarten Datenverarbeitung nicht gemäß § 134 BGB auf die Wirksamkeit des Vertrags durch, wenn dieser mit der betroffenen Person selbst abgeschlossen wurde. § 134 BGB greift jedoch ein, wenn die betroffene Person nicht am Vertrag beteiligt ist (z. B. beim Datenhandel). Ferner kann die AGB-Kontrolle von Einwilligungserklärungen und datenschutzrelevanten Vertragsklauseln nach Maßgabe eines hypothetischen Verhandlungsmechanismus operationalisiert werden (*Aziz*-Test), der auch dann greift, wenn eine Datenüberlassung als Hauptleistung vereinbart wurde. Als verlängerter Arm der AGB-Kontrolle implementiert § 138 Abs. 1 BGB schließlich eine „datenbasierte *laesio enormis*".

7. Im deliktischen Bereich stellt Art. 82 Abs. 1 DS-GVO grundsätzlich eine *lex specialis* zu nationalen Anspruchsgrundlagen dar. Daneben ist etwa § 823 BGB in Verbindung mit dem allgemeinen Persönlichkeitsrecht nur anwendbar, soweit Risiken betroffen sind, die im Rahmen der DS-GVO keine Relevanz entfalten, was im Zeitalter ubiquitärer Datenverarbeitung selten sein dürfte. Dieser Anspruch dürfte nach hier vertretener Auffassung daher gegenüber Art. 82 DS-GVO erheblich an Bedeutung verlieren.

8. Insgesamt kommt es zu vielfältigen Wechselwirkungen zwischen Datenschutzrecht und bürgerlichem Recht. So wirkt die DS-GVO auf den allgemeinen Teil des BGB (Übertragung des Unmissverständlichkeitsgebots), bei Widerruf der Einwilligung auf das Schuldrecht (Kündigungsrecht und Schadensersatz), auf das Haftungsrecht (Datenverarbeitung als Sonderrechtsbeziehung nach § 278 BGB; Art. 82 DS-GVO als *lex specialis*) sowie ganz entscheidend auf die Frage der Wirksamkeit privatautonomer Gestaltungen nach § 134 BGB (partielles Durchschlagen der Datenschutzrechtswidrigkeit) und nach § 307 Abs. 1 und 2 BGB (Datenschutzrecht als ein Beurteilungsmaßstab) ein. Umgekehrt indizieren insbesondere die Unwirksamkeit nach § 307 Abs. 1 S. 1

BGB sowie nach § 138 BGB regelmäßig die Verletzung des datenschutzrechtlichen Grundsatzes von Treu und Glauben durch Verarbeitungsvorgänge, die auf den unwirksamen Klauseln basieren. Dieser Grundsatz wiederum verdrängt in manchen, wenngleich nicht allen, datenbasierten Austauschprozessen § 242 BGB.

9. In übergreifender Perspektive offenbaren die datenschutz- und zivilrechtlichen Ermöglichungsstrukturen jedoch erhebliche Defizite im rechtlichen wie auch im tatsächlichen Bereich. Insbesondere die privatautonome Gestaltung durch Einwilligung und Vertrag versagt gegenwärtig weitgehend aufgrund einer doppelten Dysfunktionalität, dem Dilemma individueller Kontrolle im Datenschutzrecht: Jene, die rational über ihre Daten verfügen könnten und diese gerne als Budgeterweiterung einsetzen wollen, sind an dahingehender, rechtssicherer Kontrahierung in erheblicher Weise durch das datenschutzrechtliche Kopplungsverbot gehindert; hinsichtlich der übrigen Nutzer fehlt es regelmäßig an den empirisch-ökonomischen Voraussetzungen für die wirksame Inanspruchnahme (quasi)rechtsgeschäftlicher Gestaltungsmacht. Allen hehren Beschwörungen der Privatautonomie und Aufrufen zu digitaler Selbstverantwortung zum Trotz zeichnen empirische Studien ein eindeutiges Bild: Die große Mehrheit der Nutzer beschäftigt sich in konkreten Entscheidungssituationen nicht hinreichend mit Datenschutzfragen, um diesbezüglich eine bewusste und hinreichend informierte Entscheidung zu treffen.

10. Um das Dilemma individueller Kontrolle zu lösen, muss die effektive Wahrnehmung materieller Privatautonomie daher in vernetzten Umgebungen, zumal unter den Gegebenheiten nahezu ubiquitärer Datenverarbeitung im heraufziehenden *Internet of Everything*, doppelt unterstützt werden: technisch durch zunehmend autonome Datenschutzassistenten und regulatorisch durch ein Recht auf eine datenschonende Option. Automatisierte Datenerhebung und -analyse muss mit automatisierter Kommunikation und Durchsetzung von heterogenen Datenschutzpräferenzen beantwortet, die informierte durch die technologische Einwilligung abgelöst werden. Nur so kann die privatautonome Gestaltung von Austauschprozessen in hochvernetzten Umgebungen wenigstens in einer maschinell mediierten Residualform verwirklicht werden.

Literaturverzeichnis

Abdelwahab, *Sherif*, *et al.*, Enabling smart cloud services through remote sensing: An internet of everything enabler, 1 IEEE Internet of Things Journal 2014, 276–288.

Abeck, *Sebastian*, *et al.*, A Context Map as the Basis for a Microservice Architecture for the Connected Car Domain, INFORMATIK 2019, 125–138.

Abrams, *Marty/Crompton*, *Malcolm*, Multi-layered privacy notices: A better way, 2(1) Privacy Law Bulletin 2005, 1–6.

Acar, *Güneş*, *et al.*, The Web Never Forgets: Persistent Tracking Mechanisms in the Wild, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security 2014, 674–689.

–, Facebook Tracking Through Social Plug-ins, Technical report prepared for the Belgian Privacy Commission, Leuven 2015.

Accenture Strategy, Satisfy the Craving for Insurance Personalization, Paris u. a. 2017.

Ackerman, *Mark S./Cranor*, *Lorrie Faith*, Privacy critics: UI components to safeguard users' privacy, CHI Extended Abstracts 1999, 258–259.

Ackermann, *Thomas*, Der Schutz des negativen Interesses, Tübingen 2007.

Acquisti, *Alessandro*, Privacy in electronic commerce and the economics of immediate gratification, Proceedings of the 5th ACM Conference on Electronic Commerce 2004, 21–29.

–, Nudging privacy: The behavioral economics of personal information, 7(6) IEEE Security & Privacy 2009, 82–85.

Acquisti, *Alessandro/Brandimarte*, *Laura/Loewenstein*, *George*, Privacy and human behavior in the age of information, 347 Science 2015, 509–514.

Acquisti, *Alessandro/John*, *Leslie/Loewenstein*, *George*, What is Privacy Worth?, Working Paper, 2009, http://pages.stern.nyu.edu/~bakos/wise/papers/wise2009-6a1_paper.pdf.

–, What is Privacy Worth?, 42 The Journal of Legal Studies 2013, 249–274.

Acquisti, *Alessandro/Taylor*, *Curtis/Wagman*, *Liad*, The Economics of Privacy, 54 Journal of Economic Literature 2016, 442–492.

Acquisti, *Alessandro*, *et al.*, Nudges for privacy and security: Understanding and assisting users' choices online, 50(3) ACM Computing Surveys (CSUR) 2017, Article 44, 1–44.

Adams, *Michael*, Ökonomische Analyse des Gesetzes zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen (AGBGesetz), in: Neumann, Manfred (Hrsg.), Ansprüche, Eigentums- und Verfügungsrechte, Berlin 1983, 655–680.

Adjerid, *Idris/Acquisti*, *Alessandro/Brandimarte*, *Laura/Loewenstein*, *George*, Sleights of Privacy: Framing, Disclosures, and the Limits of Transparency, Proceedings of the Ninth Symposium on Usable Privacy and Security 2013, 1–17.

Adjerid, *Idris/Peer*, *Eyal/Acquisti*, *Alessandro*, Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making, 42 MIS Quarterly 2018, 465–488.

Adjerid, *Idris/Samat*, *Sonam/Acquisti*, *Alessandro*, A Query-Theory Perspective of Privacy Decision Making, 45 The Journal of Legal Studies 2016, S97-S121.

Adomeit, *Klaus/Mohr*, *Jochen*, Verantwortung von Unternehmen für diskriminierende Stellenanzeigen durch Dritte, NJW 2007, 2522–2524.

AGCM, WhatsApp Fined for 3 Million Euro for Having Forced Its Users to Share Their Personal Data with Facebook, Pressemitteilung (12.7.2017), http://www.agcm.it/en/newsroom/press-releases/2380-whatsapp-fined-for-3-millioneuro-for-having-forced-its-users-to-share-their-personal-data-with-facebook.html.

Agrawal, *Rakesh/Srikant*, *Ramakrishnan*, Privacy-preserving data mining, 29 ACM Sigmod Record 2000, 439–450.

Aher, *Bhushan*, A Look at IoT Architecture, DZone (18.8.2018), https://dzone.com/articles/iot-architecture-2.

Aiello, *William*, *et al.*, Just fast keying: Key agreement in a hostile internet, 7(2) ACM Transactions on Information and System Security 2004, 1–30.

Airbnb, Cookie-Richtlinie, https://www.airbnb.de/terms/cookie_policy (zuletzt abgerufen am 9.5.2019).

AK Technik der Datenschutzbeauftragten des Bundes und der Länder, Arbeitspapier „Datenschutzfreundliche Technologien", Bonn 1997, http://www.datenschutz-bayern.de/technik/grundsatz/apdsft.htm.

Akerlof, *George A.*, The Market for „Lemons": Quality Uncertainty and the Market Mechanism, 84 The Quarterly Journal of Economics 1970, 488–500.

Alam, *Firoj/Ricardi*, *Giuseppe*, Fusion of Acoustic, Linguistic and Psycholinguistic Features for Speaker Personality Traits Recognition, Proceedings of the 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 955–959.

Albers, *Marion*, Informationelle Selbstbestimmung, Baden-Baden 2005.

Albrecht, *Jan Philipp*, Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung, CR 2016, 88–98.

Alemanno, *Alberto/Sibony*, *Anne-Lise* (Hrsg.), Nudge and the Law: A European Perspective, Oxford/Portland, OR 2015.

Alemanno, *Alberto/Sibony*, *Anne-Lise*, Introduction, in: Alemanno, Alberto/Sibony, Anne-Lise (Hrsg.), Nudge and the Law: A European Perspective, Oxford/Portland, OR 2015, 1–25.

Alexander, *Christian*, Vertragsrecht und Lauterkeitsrecht unter dem Einfluss der Richtlinie 2005/29/EG über unlautere Geschäftspraktiken, WRP 2012, 515–523.

Alexandrova, *Maria*, The Impact of Edge Computing on IoT: The Main Benefits and Real-Life Use Cases, DZone (6.2.2019), https://dzone.com/articles/the-impact-of-edge-computing-on-iot-the-main-benef.

Allais, *Maurice*, Le Comportement de l'Homme Rationnel devant le Risque: Critique des Postulats et Axiomes de l'Ecole Americaine, 21 Econometrica 1953, 503–546.

Aloisi, *Antonio/Gramano*, *Elena*, Artificial Intelligence Is Watching You at Work. Digital Surveillance, Employee Monitoring and Regulatory Issues in the EU Context, Special Issue of Comparative Labor Law & Policy Journal 2020, https://ssrn.com/abstract=3399548.

Alonso, *Eduardo/Mondragón*, *Esther*, Agency, Learning and Animal-Based Reinforcement Learning, in: Nickles, Matthias (Hrsg.), Agents and Computational Autonomy, Berlin 2005, 1–6.

Alpers, *Sascha*, *et al.*, PRIVACY-AVARE: An approach to manage and distribute privacy settings, 3rd IEEE International Conference on Computer and Communications (ICCC) 2017, 1460–1468.
Altman, *Morris* (Hrsg.), Handbook of Contemporary Behavioral Economics: Foundations and Developments, Armonk/London 2006.
Amazon Europe, Cookies, https://www.amazon.de/gp/help/customer/display.html/?nodeId=201890250 (zuletzt abgerufen am 9.5.2019).
Anweiler, *Jochen*, Die Auslegungsmethoden des Gerichtshofs der Europäischen Gemeinschaften, Frankfurt am Main u. a. 1997.
Arbeitsgruppe „Digitaler Neustart" der Konferenz der Justizministerinnen und Justizminister der Länder, Bericht vom 15. Mai 2017, o. O. 2017.
Areeda, *Phillip/Turner*, *Donald F.*, Predatory Pricing and Related Practices under Section 2 of the Sherman Act, 88 Harvard Law Review 1975, 697–733.
Argenton, *Cédric/Prüfer*, *Jens*, Search engine competition with network externalities, 8 Journal of Competition Law and Economics 2012, 73–105.
Aridor, *Guy*, *et al.*, The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR, NBER Working Paper No. w26900, 2020, https://www.nber.org/papers/w26900.
Arneson, *Richard*, Autonomy and Preference Formation, in: Coleman, Jules/Buchanan, Allen (Hrsg.), In Harm's Way: Essays in Honor of Joel Feinberg, Cambridge, UK, 1991, 42–73.
Arning, *Marian/Moos*, *Flemming*, Big Data bei verhaltensbezogener Online-Werbung – Programmatic Buying und Real Time Advertising, ZD 2014, 242–248.
Arning, *Marian/Moos*, *Flemming/Schefzig*, *Jens*, Vergiss(,) Europa!, CR 2014, 447–456.
Arnold, *René*, *et al.*, Any Sirious Concerns Yet? – An Empirical Analysis of Voice Assistants' Impact on Consumer Behavior and Assessment of Emerging Policy Challenges, Working Paper, 2019, https://ssrn.com/abstract=3426809.
Arrieta-Ibarra, *Imanol*, *et al.*, Should We Treat Data as Labor? Moving beyond „Free", 108 AEA Papers and Proceedings 2018, 38–42.
Article 29 Data Protection Working Party, Opinion 10/2004 on More Harmonised Information Provisions, WP 100, Brüssel 2004.
–, Opinion 04/2012 on Cookie Consent Exemption, WP 194, Brüssel 2012.
–, Opinion 02/2013 on apps on smart devices, WP 202, Brüssel 2013.
–, Opinion 03/2013 on purpose limitation, WP 203, Brüssel 2013.
–, Working Document 02/2013 providing guidance on obtaining consent for cookies, WP 208, Brüssel 2013.
–, Statement on the role of a risk-based approach in data protection legal frameworks, WP 218, Brüssel 2014.
–, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting, WP 224, Brüssel 2014.
–, Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC), WP 240, Brüssel 2016.
–, Guidelines on the right to data portability, WP 242 rev. 01, Brüssel 2017.
–, Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), WP 247, Brüssel 2017.
–, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, Brüssel 2017.

Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, Brüssel 2007.
–, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", WP 169, Brüssel 2010.
–, Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting, WP 171, Brüssel 2010.
–, Stellungnahme 15/2011 zur Definition von Einwilligung, WP 187, Brüssel 2011.
–, Stellungnahme 16/2011 zur Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung, WP 188, Brüssel 2011.
–, Stellungnahme 05/2012 zum Cloud Computing, WP 196, Brüssel 2012.
–, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, Brüssel 2014.
–, Stellungnahme 06/2014 zum Begriff des berechtigten Interesses des für die Verarbeitung Verantwortlichen gemäß Artikel 7 der Richtlinie 95/46/EG, WP 217, Brüssel 2014.
–, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, WP 223, Brüssel 2014.
–, Leitlinien zu automatisierten Entscheidungen im Einzelfall einschließlich Profiling für die Zwecke der Verordnung 2016/679, WP 251 rev. 1, Brüssel 2018.
–, Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679, WP 259 rev.01, Brüssel 2018.
–, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev. 1, Brüssel 2018.
Ashley, *Kevin D.*, Artificial Intelligence and Legal Analytics. New Tools for Law Practice in The Digital Age, Cambridge, UK 2017.
Ashton, *Kevin*, That ‚Internet of Things' Thing, RFID Journal (22.6.2009), https://www.rfidjournal.com/articles/view?4986.
Assmann, *Heinz-Dieter*, Das Verhältnis von Aufsichtsrecht und Zivilrecht im Kapitalmarktrecht, in: Festschrift Schneider, Köln 2011, 37–55.
Auer, *Marietta*, Materialisierung, Flexibilisierung, Richterfreiheit. Generalklauseln im Spiegel der Antinomien des Privatrechtsdenkens, Tübingen 2005.
–, Neues zu Umfang und Grenzen der richtlinienkonformen Auslegung, NJW 2007, 1106–1109.
–, Zum Erkenntnisziel der Rechtstheorie. Philosophische Grundlagen multidisziplinärer Rechtswissenschaft, Baden-Baden 2018.
–, Digitale Leistungen, ZfPW 2019, 130–147.
Auer-Reindsorff, *Astrid*, Noch mehr Informationspflichten, aber keine transparenten Icons in Sicht, MMR 2019, 209–210.
Ausloos, *Jef*, The Right to Erasure in EU Data Protection Law, Oxford 2020.
Austin, *Lisa M.*, *et al.*, Towards Dynamic Transparency: The AppTrans (Transparency for Android Applications) Project, Working Paper, 2018, https://ssrn.com/abstract=3203601.
Australian Communications and Media Authority, Optimal conditions for effective self- and co-regulatory arrangements, Occasional Paper, Canberra u. a. 2015.
Autorité de la Concurrence/Bundeskartellamt, Competition Law and Data, Joint Report (10.5.2016).
Ayenson, *Mika D.*, *et al.*, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning, Working Paper, 2011, https://ssrn.com/abstract=1898390.
Ayres, *Ian/Gertner*, *Robert*, Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules, 99 Yale Law Journal 1989, 87–130.

Ayres, *Ian/Schwartz*, *Alan*, The No-Reading Problem in Consumer Contract Law, 66 Stanford Law Review 2014, 545–609.

Aziz, *Arslan/Telang*, *Rahul*, What is a Cookie Worth?, Working Paper, 2016, https://ssrn.com/abstract=2757325.

Bach, *Ivo*, Neue Richtlinien zum Verbrauchsgüterkauf und zu Verbraucherverträgen über digitale Inhalte, NJW 2019, 1705–1711.

Bachmann, *Gregor*, Private Ordnung, Tübingen 2006.

Baetge, *Dietmar*, Allgemeininteressen in der Inhaltskontrolle: Der Einfluss öffentlicher Interessen auf die Wirksamkeit Allgemeiner Geschäftsbedingungen, AcP 202 (2002), 972–993.

Bakos, *Yannis/Marotta-Wurgler*, *Florencia/Trossen*, *David R.*, Does Anyone Read the Fine Print?, 43 The Journal of Legal Studies 2014, 1–35.

Balebako, *Rebecca*, *et al.*, The impact of timing on the salience of smartphone app privacy notices, Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices 2015, 63–74.

Balevi, *Eren/Al Rabee*, *Faeik T./Gitlin*, *Richard D.*, ALOHA-NOMA for massive machine-to-machine IoT communication, IEEE International Conference on Communications (ICC) 2018, 1–5.

Balseiro, *Santiago R*, *et al.*, Yield optimization of display advertising with ad exchange, 60 Management Science 2014, 2886–2907.

Balzer, *Peter/Lang*, *Volker*, Anmerkung zu BGH, Urt. v. 3. 6. 2014, BKR 2014, 377–381.

Bamberger, *Kenneth A.*, *et al.*, Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps, 35 Berkeley Technology Law Journal 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3464667.

Banerjee, *Syagnik/Hemphill*, *Thomas/Longstreet*, *Phil*, Is IOT a Threat to Consumer Consent?, Working Paper, 2017, https://ssrn.com/abstract=3038872.

Barbosa, *Natã M.*, *et al.* „What if?" Predicting Individual Users' Smart Home Privacy Preferences and Their Changes, Proceedings on Privacy Enhancing Technologies 2019, 211–231.

Bar-Gill, *Oren*, Seduction by Contract, Oxford 2012.

–, Defending (Smart) Disclosure: Comment on More than You Wanted to Know, 11 Jerusalem Review of Legal Studies 2015, 75–82.

Barkhausen, *Walter*, Anmerkung zu BGH, Urteil vom 9. 7. 1953, NJW 1953, 1666.

Barnes, *Susan B.*, A privacy paradox: Social networking in the United States, 11(9) First Monday, 2006, http://firstmonday.org/issues/issue11_9/barnes/index.html.

Barocas, *Solon/Levy*, *Karen*, Privacy Dependencies, Washington Law Review (im Erscheinen), https://ssrn.com/abstract=3447384.

Barocas, *Solon/Nissenbaum*, *Helen*, Big data's end run around procedural privacy protections, 57(11) Communications of the ACM 2014, 31–33.

Barocas, *Solon/Selbst*, *Andrew D.*, Big Data's Disparate Impact, 104 California Law Review 2016, 671–732.

Bartholomeyczik, *Horst*, Äquivalenzprinzip, Waffengleichheit und Gegengewichtsprinzip in der modernen Rechtsentwicklung, AcP 166 (1966), 30–75.

Bartle, *Ian/Vass*, *Peter*, Self-Regulation and the Regulatory State: A survey of policy and practice, Centre for the Study of Regulated Industries, University of Bath School of Management, Research Report 17, Bath 2005.

Bartsch, *Michael*, Die „Vertraulichkeit und Integrität informationstechnischer Systeme" als sonstiges Recht nach § 823 Abs. 1 BGB, CR 2008, 613–617.

Basedow, *Jürgen*, EuGH: Über Lücken in privatrechtlichen EU-Verordnungen, ZEuP 2014, 402–409.

Baumann, *Annika*, *et al.*, Maximize What Matters: Predicting Customer Churn with Decision-Centric Ensemble Selection, Twenty-Third European Conference on Information Systems (ECIS) 2015, Article 15, 1–17.

Baumann, *Annika*, *et al.*, The Price of Privacy, 61 Business & Information Systems Engineering 2019, 413–431.

Baumgartner, *Ulrich/Gausling*, *Tina*, Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen, ZD 2017, 308–313.

Baumol, *William J.*, Predation and the logic of the average variable cost test, 39 The Journal of Law and Economics 1996, 49–72.

Beater, *Axel*, Generalklauseln und Fallgruppen, AcP 194 (1994), 82–92.

–, Deliktischer Äußerungsschutz als Rechts- und Erkenntnisquelle des Medienrechts, JZ 2004, 889–893.

Beaucamp, *Guy/Meßerschmidt*, *Klaus*, Minderheitenschutz in den baltischen Staaten und in der Bundesrepublik Deutschland – ein Rechtsvergleich im Überblick, ZaöRV 2003, 779–799.

Becher, *Shmuel I./Benoliel*, *Uri*, Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR, in: Mathis, Klaus/Tor, Avishalom (Hrsg.), Consumer Law & Economics, Cham 2020, (im Erscheinen).

Becker, *Carina*, Das Recht auf Vergessenwerden, 2019.

Becker, *Christoph*, Die Lehre von der laesio enormis in der Sicht der heutigen Wucherproblematik, Köln u. a. 1993.

Becker, *Joachim*, Die 100-Milliarden-Euro-Frage. Digitale Angebote im Auto, SZ (13.3.2019), https://www.sueddeutsche.de/auto/auto-vernetzung-digital-1.4358303.

Becker, *Maximilian*, Ein Recht auf datenerhebungsfreie Produkte, JZ 2017, 171–181.

Becker, *Michael*, Der unfaire Vertrag, Tübingen 2003.

BeckOK BGB, hrsg. v. Bamberger, Georg, et al., 53. Ed., München 2020 (zit.: *Bearbeiter*, in: BeckOK BGB).

BeckOK DatenschutzR, hrsg. v. Brink, Stefan/Wolff, Heinrich Amadeus, 31. Ed., München 2020 (zit.: *Bearbeiter*, in: BeckOK DatenschutzR).

Beimowski, *Joachim*, Zur ökonomischen Analyse Allgemeiner Geschäftsbedingungen, München 1989.

Bekey, *George A.*, Current trends in robotics: technology and ethics, in: Lin, Patrick, et al. (Hrsg.), Robot Ethics, Cambridge, MA 2012, 17–34.

Beljin, *Saša*, Die Zusammenhänge zwischen dem Vorrang, den Instituten der innerstaatlichen Beachtlichkeit und der Durchführung des Gemeinschaftsrechts, EuR 2002, 351–376.

Belleflamme, *Paul/Peitz*, *Martin*, Industrial Organization. Markets and Strategies, Cambridge, UK 2010.

Bender, *Rolf*, Probleme des Konsumentenkredits, NJW 1980, 1129–1136.

Bengio, *Yoshua*, *et al.*, Greedy layer-wise training of deep networks, Advances in Neural Information Processing Systems, 2006, 153–160.

Bengoetxea, *Joxerramon*, The legal reasoning of the European Court of Justice. Towards a European Jurisprudence, Oxford 1993.

Benndorf, *Volker/Kübler*, *Dorothea/Normann*, *Hans-Theo*, Privacy Concerns, Voluntary Disclosure of Information, and Unraveling: An Experiment, 75 European Economic Review 2015, 43–59.

Bennear, *Lori*, Evaluating Management-Based Regulation: A Valuable Tool in the Regulatory Toolbox?, in: Coglianese, Cary/Nash, Jennifer (Hrsg.), Leveraging the Private Sector: Management-Based Strategies for Improving Environmental Performance, Washington, DC 2006, 51–86.

Ben-Shahar, *Omri*, Data Pollution, 11 Journal of Legal Analysis, 2019, 104–159.

Ben-Shahar, *Omri/Chilton*, *Adam*, Simplification of Privacy Disclosures: An Experimental Test, 45 Journal of Legal Studies 2016, S41-S67.

Ben-Shahar, *Omri/Schneider*, *Carl E.*, More Than You Wanted to Know, Princeton 2014.

Ben-Shahar, *Omri/Strahilevitz*, *Lior Jacob*, Contracting over Privacy: Introduction, 45 Journal of Legal Studies 2016, S1-S11.

Benson M., Clinical implications of omics and systems medicine: focus on predictive and individualized treatment, 279 Journal of Internal Medicine 2016, 229–240.

Berberich, *Matthias/Steiner*, *Malgorzata*, Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers, 2 European Data Protection Law Review 2016, 422–426.

Beresford, *Alastair R./Kübler*, *Dorothea/Preibusch*, *Sören*, Unwillingness to pay for privacy: A field experiment, 117 Economics Letters 2012, 25–27.

Bergt, *Matthias*, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag, ZD 2015, 365–371.

–, Verhaltensregeln als Mittel zur Beseitigung der Rechtsunsicherheit in der Datenschutz-Grundverordnung, CR 2016, 670–678.

–, Gemeinsame Datenschutz-Verantwortlichkeit für Drittinhalte – Facebook-Fanpages, ITRB 2018, 151–153.

Berk, *Richard*, *et al.*, Fairness in criminal justice risk assessments: The state of the art, Sociological Methods & Research 2018, Article 0049124118782533, 1–42.

Berofsky, *Bernard*, Liberation from Self. A Theory of Personal Autonomy, Cambridge, UK 1995.

Bertea, *Stefano*, Looking for Coherence within the European Community, 11 European Law Journal 2005, 154–172.

Beshears, *John*, *et al.*, How Does Simplified Disclosure Affect Individuals' Mutual Fund Choice?, in: Wise, David A. (Hrsg.), Explorations in the Economics of Aging, Chicago 2011, 75–96.

Bettman, *James R./Payne*, *John W./Staelin*, *Richard*, Cognitive Considerations in Designing Effective Labels for Presenting Risk Information, 5 Journal of Public Policy & Marketing 1986, 1–28.

Betz, *Christoph*, Automatisierte Sprachanalyse zum Profiling von Stellenbewerbern, ZD 2019, 148–152.

Beyvers, *Eva/Herbrich*, *Tilman*, Das Niederlassungsprinzip im Datenschutzrecht – am Beispiel von Facebook – Der neue Ansatz des EuGH und die Rechtsfolgen, ZD 2014, 558–562.

Bieder, *Marcus*, Der Schutz vor täuschungsgeeigneten Formularverträgen, AcP 216 (2016), 911–951.

Bier, *Christoph/Kühne*, *Kay/Beyerer*, *Jürgen*, PrivacyInsight: the next generation privacy dashboard, Proceedings of the 4th Annual Privacy Forum 2016, 135–152.

Bierekoven, *Christiane*, Anmerkung zu Breyer, NJW 2017, 2420–2421.

Bieresborn, *Dirk/Giesberts-Kaminski*, *Bernadette*, Auswirkungen der EU-Datenschutz-Grundverordnung und der Anpassungsgesetze auf die Sozialgerichtsbarkeit (Teil I), SGb 2018, 449–455.

Bijker, *Wiebe E./Law*, *John*, General Introduction, in: Bijker, Wiebe E./Law, John (Hrsg.), Shaping Technology/Building Society. Studies in Sociotechnical Change, Cambridge, MA/London 1992, 1–14.

Billhardt, *Holger*, *et al.*, Agreement technologies for coordination in smart cities, 8 Applied Sciences 2018, Article 816, 1–38.

Billing, *Tom*, Die Bedeutung von § 307 III 1 BGB im System der AGB-rechtlichen Inhaltskontrolle, München 2006.

Binns, *Reuben*, Data protection impact assessments: A meta-regulatory approach, 7 International Data Privacy Law 2017, 22–35.

Bischhoff, *Paul*, Comparing the privacy policy of internet giants side-by-side, comparitech (20.3.2017), https://www.comparitech.com/blog/vpn-privacy/we-compared-the-privacy-policies-of-internet-giants-side-by-side/.

Bleckmann, *Albert*, Probleme der Auslegung europäischer Richtlinien, ZGR 1992, 364–375.

Blume, *Peter*, The Inherent Contradictions in Data Protection Law, 2 International Data Privacy Law 2012, 26–34.

Bock, *Kirsten*, Data Protection Certification: Decorative or Effective Instrument? Audit and Seals as a Way to Enforce Privacy, in: Wright, David/De Hert, Paul (Hrsg.), Enforcing Privacy. Regulatory, Legal and Technological Approaches, Schweiz 2016, 335–356.

Boerman, *Sophie C./Kruikemeier*, *Sanne/Zuiderveen Borgesius*, *Frederik J.*, Online behavioral advertising: A literature review and research agenda, 46 Journal of Advertising 2017, 363–376.

Böhm, *Franz*, Privatrechtsgesellschaft und Marktwirtschaft, ORDO 17 (1966), 75–151.

Böhning, *Björn*, Datenschutz – Die Debatte muss geführt werden, ZD 2013, 421–422.

Bolognini, *Luca/Balboni*, *Paolo*, IoT and Cloud Computing: Specific Security and Data Protection Issues, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 71–79.

Bolognini, *Luca/Ziegler*, *Sébastian*, Evolution of Data Protection Norms and Their Impact on the Internet of Things, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 93–105.

Börding, *Andreas et al.*, Neue Herausforderungen der Digitalisierung für das deutsche Zivilrecht, CR 2017, 134–140.

Borges, *Georg*, Rechtliche Rahmenbedingungen für autonome Systeme, NJW 2018, 977–982.

Borking, *John*, Der Identity-Protector, DuD 1996, 654–658.

Börner, *Andreas*, Die „Heilung" von AGB durch die Berücksichtigung vertragsabschlußbegleitender Umstände nach § 24 a Nr. 3 AGBG, JZ 1995, 595–601.

Botta, *Alessio*, *et al.*, Integration of cloud computing and internet of things: a survey, 56 Future Generation Computer Systems 2016, 684–700.

Botta, *Marco/Wiedemann*, *Klaus*, The interaction of EU competition, consumer, and data protection law in the digital economy: the regulatory dilemma in the Facebook odyssey, 64 The Antitrust Bulletin 2019, 428–446.

Bradford, *Anu*, The Brussels Effect, 107 Northwestern University Law Review 2012, 1–67.

Bradshaw, *Jeffrey M.*, *et al.*, The seven deadly myths of „autonomous systems", 28 IEEE Intelligent Systems 2013, 54–61.

Brambring, *Günter*, Teil- oder Gesamtnichtigkeit beim Ehevertrag, NJW 2007, 865–870.

Brand, *Frank*, Ökonomische Fragestellungen mit vielen Einflussgrößen als Netzwerke, Working Papers of the Institute of Management Berlin at the Berlin School of Economics (FHW Berlin), No. 29, 2006.

Brandimarte, *Laura/Acquisti*, *Alessandro/Loewenstein*, *George*, Misplaced confidences: Privacy and the control paradox, 4 Social Psychological and Personality Science, 2013, 340–347.

Brandner, *Hans Erich*, Maßstab und Schranken der Inhaltskontrolle bei Verbraucherverträgen, MDR 1997, 312–315.

Braun, *Daniel*, *et al.*, Customer-centered LegalTech: automated analysis of standard form, Internationales Rechtsinformatik Symposium (IRIS) 2018, 627–634.

–, Consumer Protection in the Digital Era: The Potential of Customer-Centered LegalTech, INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft 2019, 407–420.

Braunstein, *Alex/Granka*, *Laura/Staddon*, *Jessica*, Indirect content privacy surveys: measuring privacy without asking about it, Proceedings of the Seventh Symposium on Usable Privacy and Security 2011, Article 15, 1–14.

Bräutigam, *Peter*, Das Nutzungsverhältnis bei sozialen Netzwerken – Zivilrechtlicher Austausch von IT-Leistung gegen personenbezogene Daten, MMR 2012, 635–641.

Bräutigam, *Peter/Klindt*, *Thomas*, Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, 1137–1142.

Breiner, *Spencer/Sriram*, *Ram D./Subrahmanian*, *Eswaran*, Compositional Models for the Internet of Everything, AAAI Spring Symposium Series 2018, 107–110.

Brink, *Stefan/Eckhardt*, *Jens*, Wann ist ein Datum ein personenbezogenes Datum? – Anwendungsbereich des Datenschutzrechts, ZD 2015, 205–212.

Brisch, Klaus M./Laue, Philip, Anmerkung, CR 2008, 724–726.

Britz, *Gabriele*, Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, 1–11.

Brkan, *Maja*, The Unstoppable Expansion of EU Fundamental Right to Data Protection. Little Shop of Horrors?, 23 Maastricht Journal of European and Comparative Law 2016, 812–841.

Brömmelmeyer, *Christoph*, Belohnungen für gesundheitsbewusstes Verhalten in der Lebens- und Berufsunfähigkeitsversicherung? Rechtliche Rahmenbedingungen für Vitalitäts-Tarife, r + s 2017, 225–232.

Brookman, *Justin/Hans*, *G.S.*, Why Collection Matters: Surveillance as a De Facto Harm, Center for Democracy and Technology, 2013, https://fpf.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

Brown, *Andrew*, Fed Up with Facebook? Here are 6 Alternatives, maketecheasier (18.5. 2019), https://www.maketecheasier.com/facebook-alternatives-social-networks/.

Brown, *Noam/Sandholm*, *Tuomas*, Superhuman AI for heads-up no-limit poker: Libratus beats top professionals, 359 Science 2018, 418–424.

–, Superhuman AI for multiplayer poker, 365 Science 2019, 885–890.

Brownsword, *Roger*, Technological management and the Rule of Law, 8 Law, Innovation and Technology 2016, 100–140.

–, in: Grundmann, Stefan (Hrsg.), European Contract Law in the Digital Age, Cambridge, UK 2018, 165–204.

Bruneteau, *Frederic*, *et al.*, Usage-Based Insurance. Global Study, Brüssel u. a. 2016.

Bruns, *Hendrik*, *et al.*, Can nudges be transparent and yet effective?, 65 Journal of Economic Psychology 2018, 41–59.

Büchi, *Moritz/Fosch Villaronga*, *Eduard/Lutz*, *Christoph/Tamò-Larrieux*, *Aurelia/Velidi*, *Shruthi/Viljoen*, *Salome*, Chilling Effects of Profiling Activities: Mapping the Issues, Working Paper, 2019, https://ssrn.com/abstract=3379275.

Buchner, *Benedikt*, Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006.

–, Die Einwilligung im Datenschutzrecht, DuD 2010, 39–43.

–, Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 155–161.

–, Die Einwilligung in Werbung, WRP 2018, 1283–1289.

–, Datenschutz und Kartellrecht, WRP 2019, 1243–1248.

–, Grundsätze des Datenschutzrechts, in: Tinnefeld, Marie-Therese, et al. (Hrsg.), Einführung in das Datenschutzrecht, 7. Aufl., Berlin 2020, 220–332.

Buck-Heeb, *Petra*, Aufklärung über Innenprovisionen, unvermeidbarer Rechtsirrtum und die Überlagerung durch Aufsichtsrecht, WM 2014, 1601–1605.

Buck-Heeb, *Petra/Poelzig*, *Dörte*, Die Verhaltenspflichten (§§ 63 ff. WpHG n. F.) nach dem 2. FiMaNoG – Inhalt und Durchsetzung, BKR 2017, 485–495.

Budzikiewicz, *Christine*, Digitaler Nachlass, AcP 218 (2018), 558–593.

Bundeskartellamt, Fallbericht v. 15.2.2019, Az. B6–22/16 (*Facebook; Konditionenmissbrauch gemäß § 19 Abs. 1 GWB wegen unangemessener Datenverarbeitung*), abrufbar unter https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.html (abgerufen am 8.3.2019).

Bundesregierung, Questionnaire on the implementation of the Article 5(3) of the ePrivacy Directive, KommDok. COCOM11–20 vom 4.10.2011.

Bundesverband der digitalen Wirtschaft, Data Economy, Berlin 2018.

Buocz, *Thomas*, *et al.*, Bitcoin and the GDPR: Allocating responsibility in distributed networks, 35 Computer Law & Security Review 2019, 182–198.

Burrell, *Jenna*, How the machine thinks: Understanding opacity in machine learning algorithms, 3(1) Big Data & Society 2016, 1–12.

Burri, *Mira*, Understanding the Implications of Big Data and Big Data Analytics for Competition Law, in: Klaus Mathis und Avishalom Tor, New Developments in Competition Law and Economics, Cham 2019, 241–263.

Burrows, *Michael/Abadi*, *Martin/Needham*, *Roger Michael*, A logic of authentication, 426.1871 Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences 1989, 233–271.

Busch, *Christoph*, Implementing Personalized Law, 86 The University of Chicago Law Review 2019, 309–332.

Busche, *Jan*, Privatautonomie und Kontrahierungszwang, Tübingen 1999.

Buttarelli, *Giovanni*, The EU GDPR as a clarion call for a new global digital gold standard, 6 International Data Privacy Law 2016, 77–78.

Butterworth, *Michael*, The ICO and artificial intelligence: The role of fairness in the GDPR framework, 34 Computer Law & Security Review 2018, 257–268.

Bydlinski, *Franz*, Die Suche nach der Mitte als Daueraufgabe der Privatrechtswissenschaft, AcP 204 (2004), 309–395.

Bydlinski, *Franz*, Privatautonomie und objektive Grundlagen des verpflichtenden Rechtsgeschäfts, Wien/New York 1967.

–, Erklärungsbewußtsein und Rechtsgeschäft, JZ 1975, 1–6.

–, Juristische Methodenlehre und Rechtsbegriff, 2. Aufl., Wien/New York 1991.

–, System und Prinzipien des Privatrechts, Wien 1996.

Bygrave, *Lee*, Data Protection Law. Approaching Its Rationale, Logic, and Limits, Alphen aan den Rijn 2002.

–, Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements, 4 Oslo Law Review 2017, 105–120.
Cabinakova, *Johana/Zimmermann*, *Christian/Mueller*, *Guenter*, An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case, 24th European Conference on Information Systems (ECIS) 2016, 1–18.
Cahn, *Andreas*, Zum Begriff der Nichtigkeit im Bürgerlichen Recht, JZ 1997, 8–19.
Calders, *Toon/Žliobaitė*, *Indrė*, Why unbiased computational processes can lead to discriminative decision procedures, in: Custers, Bart, et al. (Hrsg.), Discrimination and Privacy in the Information Society, Berlin/Heidelberg 2013, 43–57.
Calliess, *Christian/Ruffert*, *Matthias*, EUV/AEUV, 5. Aufl., München 2016.
Calo, *Ryan*, Against Notice Skepticism in Privacy (And Elsewhere), 87 Notre Dame Law Review 2012, 1027–1072.
–, Digital Market Manipulation, 82 George Washington Law Review, 2014, 995–1051.
Camenisch, *Jan/Lysyanskaya*, *Anna*, An efficient system for non-transferable anonymous credentials with optional anonymity revocation, in: Pfitzmann, Birgit (ed.), International Conference on the Theory and Applications of Cryptographic Techniques, Berlin/Heidelberg 2001, 93–118.
Camenisch, *Jan/Van Herreweghen*, *Els*, Design and implementation of the idemix anonymous credential system, Proceedings of the 9th ACM Conference on Computer and Communications Security 2002, 21–30.
Camerer, *Colin F./Loewenstein*, *George/Rabin*, *Matthew* (Hrsg.), Advances in Behavioral Economics, Princeton/Oxford 2004.
Canaris, *Claus-Wilhelm*, Die Vertrauenshaftung im deutschen Privatrecht, München 1971.
–, Anmerkung zu BGH, Urteil v. 30. 5. 1975 – V ZR 206/73, JZ 1976, 132–34.
–, Schranken der Privatautonomie zum Schutze des Kreditnehmers, ZIP 1980, 709–722.
–, Die Feststellung von Lücken im Gesetz. Eine methodologische Studie über Voraussetzungen und Grenzen der richterlichen Rechtsfortbildung praeter legem, 2. Aufl., Berlin 1983.
–, Gesetzliches Verbot und Rechtsgeschäft, Heidelberg 1983.
–, Systemdenken und Systembegriff in der Jurisprudenz entwickelt am Beispiel des deutschen Privatrechts, 2. Aufl., Berlin 1983.
–, Anmerkung zu BGH: Ohne Erklärungsbewußtsein erfolgte tatsächliche Mitteilung als Willenserklärung, NJW 1984, 2281–2282.
–, Grundrechte und Privatrecht, AcP 184 (1984), 201–246.
–, Anmerkung zu BGH: Gültiger Werkvertrag bei einseitigem Verstoß gegen Schwarzarbeitsverbot, NJW 1985, 2404–2405.
–, Zinsberechnungs- und Tilgungsverrechnungsklauseln beim Annuitätendarlehen – Zugleich ein Beitrag zur Abgrenzung von § 8 und § 9 AGB-Gesetz, NJW 1987, 609–617.
–, Wandlungen des Schuldvertragsrechts – Tendenzen zu seiner „Materialisierung", AcP 200 (2000), 273–364.
–, Die Reform des Rechts der Leistungsstörungen, JZ 2001, 499–524.
– Die richtlinienkonforme Auslegung und Rechtsfortbildung im System der juristischen Methodenlehre, in: Festschrift Bydlinski, 2002, 47–103.
–, Handelsrecht, 24. Aufl., München 2006.
Cao, *Yinzhi*, *et al.*, (Cross-) Browser Fingerprinting via OS and Hardware Level Features, NDSS 2017, 1–15.

Carroll, *Gabriel D.*, *et al.*, Optimal defaults and active decisions, 124 The Quarterly Journal of Economics 2009, 1639–1674.

Caspar, *Johannes*, Klarnamenpflicht versus Recht auf pseudonyme Nutzung, ZRP 2015, 233–236.

Castelfranchi/Falcone, Founding Autonomy: The Dialectics Between (Social) Environment and Agent's Architecture and Powers, in: Nickles, Matthias (Hrsg.), Agents and Computational Autonomy, Berlin 2005, 40–54.

Cavoukian, *Ann*, Privacy by Design – The 7 Foundational Principles, Ontario 2009/2011.

Center for Information Policy Leadership, Multi-Layered Notices Explained, First Data Privacy Subgroup Meeting, Seoul 2005.

–, Ten steps to develop a multilayered privacy notice, o. O. 2006.

Charniak, *Eugene/McDermott*, *Drew*, Introduction to Artificial Intelligence, Reading, MA 1985.

Charrow, *Robert P./Charrow*, *Veda R.*, Making legal language understandable: A psycholinguistic study of jury instructions, 79 Columbia Law Review 1979, 1306–1374.

Chaudhuri, *Kamalika/Monteleoni*, *Claire*, Privacy-preserving logistic regression, Advances in Neural Information Processing Systems 2009, 289–296.

Chaum, *David*, Security without identification: Transaction systems to make big brother obsolete, 28(10) Communications of the ACM 1985, 1030–1044.

Chen, *Cindy*, United States and European Union Approaches to Internet Jurisdiction and Their Impact on E-Commerce, 25 University of Pennsylvania Journal of International Law 2004, 423–454.

Chittaranjan, *Gokul/Blom*, *Jan/Gatica-Perez*, *Daniel*, Mining large-scale smartphone data for personality studies, 17 Personal and Ubiquitous Computing 2013, 433–450.

Christidis, *Konstantinos/Apostolou*, *Dimitris/Mentzas*, *Gregoris*, Exploring customer preferences with probabilistic topics models, European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases 2010, 12–24.

Christl, *Wolfie/Kopp*, *Katharina/Riechert*, *Patrick Urs*, Corporate Surveillance in Everyday Life, Wien 2017.

Christl, *Wolfie/Spiekermann*, *Sarah*, Networks of Control. A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy, Wien 2016.

Christman, *John*, Autonomy in Moral and Political Philosophy, The Stanford Encyclopedia of Philosophy, 2015, https://plato.stanford.edu/archives/spr2018/entries/autonomy-moral/.

Ciacchi, *Aurelia Colombi*, Book Review, Max Fabian Starke, EU-Grundrechte und Vertragsrecht, 15 European Review of Contract Law 2018, 84–87.

Ciacchi, *Aurelia Colombi*, Egenberger and Comparative Law: A Victory of the Direct Horizontal Effect of Fundamental Rights, 5 European Journal of Comparative Law and Governance 2018, 207–211.

Classen, *Claus Dieter*, Joined Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk*, 41 Common Market Law Review 2004, 1377–1385.

–, Das kirchliche Arbeitsrecht unter europäischem Druck – Anmerkungen zu den Urteilen des EuGH (jeweils GK) vom 17.04.2018 in der Rs. C-414/16 (Egenberger) und vom 11.09.2018 in der Rs. C-68/17 (IR), EuR 2018, 752–767.

–, Zuviel des Guten? Unionsrechtliche Neuakzentuierungen beim Grundrechtsschutz, JZ 2019, 1057–1066.

Clifford, *Damian*, EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster-Tracking the Crumbs of Online User Behavior, 5 JIPITEC 2014, 194–212.
–, The Legal Limits to the Monetisation of Online Emotions, PhD Thesis, Leuven 2019.
Clifford, *Damian/Ausloos*, *Jef*, Data Protection and the Role of Fairness, 37 Yearbook of European Law 2018, 130–187.
Clifford, *Damian/Graef*, *Inge/Valcke*, *Peggy*, Pre-Formulated Declarations of Data Subject Consent – Citizen-Consumer Empowerment and the Alignment of Data, Consumer and Competition Law Protections, 20 German Law Journal 2019, 679–721.
CNIL, How Can Humans Keep the Upper Hand? The Ethical Matters Raised by Algorithms and Artificial Intelligence, Report on the Public Debate Led by the French Data Protection Authority (CNIL) as Part of the Ethical Discussion Assignment Set by the Digital Republic Bill, Paris 2017.
–, Deliberation of the Restricted Committee SAN-2019–001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, Paris 2019.
Cobbe, *Jennifer/Morison*, *John*, Understanding the Smart City: Framing the Challenges for Law and Good Governance, in: E. Slautsky (Hrsg.), The Conclusions of the Chaire Mutations de l'Action Publique et du Droit Public, Paris 2019.
Cockfeld, *Arthur*, Protecting the social value of privacy in the context of state investigations using new technologies, 40 University of British Colombia Law Review 2007, 41–68.
Coester, *Ulla/Fuhlert*, *Bernd*, Gesichtserkennung – eine Frage der Ethik?, DuD 2020, 48–51.
Coester-Waltjen, *Dagmar*, Die Inhaltskontrolle von Verträgen außerhalb des AGBG, AcP 190 (1990), 1–33.
Coglianese, *Cary/Lazer*, *David*, Management-Based Regulatory Strategies, in: Donahue, John D./Nye, Joseph S. (Hrsg.), Market-Based Governance, Washington, DC 2002, 201–224.
Coglianese, *Cary/Mendelson*, *Evan*, Meta-Regulation and Self-Regulation, in: Baldwin, Robert, et al. (Hrsg.), The Oxford Handbook of Regulation, Oxford 2010, 146–169.
Cognizant, The Rise of the Smart Product Economy, Teaneck 2015.
Colangelo, *Giuseppe*, Facebook and Bundeskartellamt's Winter of Discontent, Competition Policy International, 2019, https://ssrn.com/abstract=3458922.
Colangelo, *Giuseppe/Maggiolino*, *Mariateresa*, Antitrust *über alles*. Whither Competition Law After *Facebook*? 42(3) World Competition Law and Economics Review 2019, 355–376.
Collins, *Hugh*, Regulating Contracts, Oxford 1999.
–, The impact of human rights law on contract law in Europe, 22 European Business Law Review 2011, 425–435.
Colombi Ciacchi, *Aurelia*, Party Autonomy as a Fundamental Right in the European Union, 6 European Review of Contract Law 2010, 303–318.
Columbus, *Louis*, 2018 Roundup of Internet of Things Forecasts and Market Estimates, Forbes (13.12.2018), https://www.forbes.com/sites/louiscolumbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/.
ConPolicy, Wege zur besseren Informiertheit im Datenschutz, Bonn 2018.
Conti, *Gregory/Sobiesk*, *Edward*, Malicious interface design: exploiting the user, Proceedings of the 19th International Conference on World Wide Web 2010, 271–280.

Contissa, *Giuseppe*, *et al.*, Automated Processing of Privacy Policies Under the EU General Data Protection Regulation, Legal Knowledge and Information Systems (JURIX) 2018, 51–60.

Contissa, *Giuseppe*, *et al.*, CLAUDETTE Meets GDPR: Automating the Evaluation of Privacy Policies Using Artificial Intelligence, Report, 2018, https://ssrn.com/abstract=3208596.

Conway, *Gerard*, The Limits of Legal Reasoning and the European Court of Justice, Cambridge, UK, 2012.

Cornelius, *Kai*, Vertragsabschluss durch autonome elektronische Agenten, MMR 2002, 353–358.

Costa-Cabral, *Francisco/Lynskey*, *Orla*, Family Ties: The Intersection between Data Protection and Competition in EU Law, 54 Common Market Law Review 2017, 11–50.

Cowan, *Nelson*, The magical number 4 in short-term memory: A reconsideration of mental storage capacity, 24 Behavioral and Brain Sciences 2000, 87–114.

Craig, *Paul/de Burca*, *Gráinne*, EU Law. Texts, Cases, and Materials, 6th ed., Oxford 2015.

Crane, *Daniel A./Logue*, *Kyle D./Pilz*, *Bryce C.*, A survey of legal issues arising from the deployment of autonomous and connected vehicles, 23 Michigan Telecommunications and Technology Law Review, 2016, 191–320.

Cranor, *Lorrie Faith*, Necessary but not sufficient: Standardized mechanisms for privacy notice and choice, 10 Journal on Telecommunications & High Technology Law 2012, 273–307.

von Craushaar, *Götz*, Die Bedeutung der Rechtsgeschäftslehre für die Problematik der Scheinvollmacht, AcP 174 (1974), 2–25.

Crémer, *Jacques/de Montjoye*, *Yves-Alexandre/Schweitzer*, *Heike*, Competition Policy for the Digital Era, Bericht, Brüssel 2019.

Culik, *Nicolai/Döpke*, *Christian*, Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen, ZD 2017, 226–230.

Cunche, *Mathieu/Le Métayer*, *Daniel/Morel*, *Victor*, A Generic Information and Consent Framework for the IoT (Extended Version), Research Report 9234, Saint Ismier 2018.

Custers, *Bart*, *et al.*, Informed Consent in Social Media Use – The Gap between User Expectations and EU Personal Data Protection Law, 10 SCRIPTed 2013 435–457.

Dahl, *Robert A.*, A Preface to Democratic Theory, Expanded Edition, Chicago and London 2006.

Dai, *Andrew M./Le*, *Quoc V.*, Semi-supervised sequence learning, Advances in Neural Information Processing Systems 2015, 3079–3087.

Dalton, *George*, Barter, 16 Journal of Economic Issues 1982, 181–190.

Damm, *Reinhard*, Europäisches Verbrauchervertragsrecht und AGB-Recht: Zur Umsetzung der EG-Richtlinie über mißbräuchliche Klauseln in Verbraucherverträgen, JZ 1994, 161–178.

Dammann, *Ulrich*, Erfolge und Defizite der EU-Datenschutzgrundverordnung – Erwarteter Fortschritt, Schwächen und überraschende Innovationen, ZD 2016, 307–314.

Danezis, *George*, *et al.*, Privacy and Data Protection by Design – from policy to engineering, ENISA Report, Heraklion 2014.

Das, *Anupam*, *et al.*, Assisting users in a world full of cameras: A privacy-aware infrastructure for computer vision applications, IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW) 2017, 1387–1396.

Das, *Anupam*, *et al.*, Personalized Privacy Assistants for the Internet of Things: Providing Users with Notice and Choice, 17 (3) IEEE Pervasive Computing 2018, 35–46.

Data Protection Commissioner, Facebook Ireland Ltd, Report of Audit v. 21.12.2011.

Datenethikkommission, Gutachten der Datenethikkommission, Berlin 2019.

Datta, *Amit/Lu*, *Jianan/Tschantz*, *Michael Carl*, Evaluating Anti-Fingerprinting Privacy Enhancing Technologies, The World Wide Web Conference 2019, 351–362.

Dauses, *Manfred/Ludwigs*, *Markus* (Hrsg.), Handbuch des EU-Wirtschaftsrechts, 48. EL, München 2019.

Day, *Matt/Turner*, *Giles/Drozdiak*, *Natalia*, Amazon Workers Are Listening to What You Tell Alexa, Bloomberg (11.4.2019), https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio.

Degeling, *Martin*, *et al.*, We Value Your Privacy … Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy, 26th Annual Network and Distributed System Security Symposium (NDSS '19), 1–15.

DeJoy, *David M.*, The optimism bias and traffic accident risk perception. 21 Accident Analysis & Prevention, 1989, 333–340.

DeNardis, *Laura*, The Internet in Everything. Freedom and Security in a World with No Off Switch, New Haven/London 2020.

Denga, *Michael*, Gemengelage privaten Datenrechts, NJW 2018, 1371–1376.

–, KI im Kontext des IoT, in: Bräutigam, Peter/Kraul, Torsten (Hrsg.), Internet of Things. Rechtshandbuch, München 2020.

Department of Defense, Defense Science Board, Summer Study on Autonomy, Washington D.C. 2016.

–, Defense Science Board, The Role of Autonomy in DoD Systems, Washington D.C. 2012.

Deschamps-Sonsino, *Alexandra*, What Makes a Good Connected Product?, in: DZone, DZone's 2019 Guide to Internet of Things, 2019, 12–13.

Di Martino, *Beniamino*, *et al.*, Trends and Strategic Researches in Internet of Everything, in: Di Martino, Beniamino, et al. (Hrsg.), Internet of Everything, 2018, 1–12.

Dickmann, *Roman*, Nach dem Datenabfluss: Schadenersatz nach Art. 82 der Datenschutz-Grundverordnung und die Rechte des Betroffenen an seinen personenbezogenen Daten(r+s 2018, 345–355.

Dieterich, *Thomas*, Canvas Fingerprinting – Rechtliche Anforderungen an neue Methoden der Nutzerprofilerstellung, ZD 2015, 199–204.

Dietz, *Rolf*, Anspruchskonkurrenz bei Vertragsverletzung und Delikt, Bonn/Köln 1934.

Dietz, *Sara*, Die europarechtsfreundliche Verfassungsidentität in der Kontrolltrias des Bundesverfassungsgerichts, AöR 142 (2017), 78–132.

Diffie, *Whitfield/Hellman*, *Martin*, New directions in cryptography, 22 IEEE Transactions on Information Theory 1976, 644–654.

Dimitropoulos, *Georgios/Hacker*, *Philipp*, Learning and the law: improving behavioral regulation from an international and comparative perspective, 25 Journal of Law and Policy 2017, 473–548.

DIVSI, Daten – Ware und Währung, Hamburg 2014.

Dix, *Alexander*, Daten als Bezahlung – Zum Verhältnis zwischen Zivilrecht und Datenschutzrecht, ZEuP 2017, 1–5

Djeffal, *Christian*, IT-Sicherheit 3.0: Der neue IT-Grundschutz, MMR 2019, 289–293.

Dörner, *Heinrich*, Rechtsgeschäfte im Internet, AcP 202 (2002), 363–396.

Dougan, *Michael*, When worlds collide! Competing visions of the relationship between direct effect and supremacy, 44 Common Market Law Review 2007, 931–963.

DPA, So schlägt sich der smarte Radio-Wecker von Amazon, t-online.de (8.2.2018), https://www.t-online.de/digital/id_83196654/amazon-echo-spot-im-test-eine-kamera-im-schlafzimmer-.html

Draper, *Kevin*, Madison Square Garden Has Used Face-Scanning Technology on Customers, New York Times (13.3.2018), https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html.

Dressel, *Julia/Farid*, *Hany*, The accuracy, fairness, and limits of predicting recidivism, 4 Science Advances 2018, Article eaao5580, 1–5.

Drewes, *Stefan*, Kritische Betrachtung der DSK-Orientierungshilfe zu Direktwerbung, ZD 2019, 296–301.

Drexl, *Josef*, Die wirtschaftliche Selbstbestimmung des Verbrauchers, Tübingen 1998.

–, Neue Regeln für die Europäische Datenwirtschaft? Ein Plädoyer für einen wettbewerbspolitischen Ansatz – Teil 2, NZKart 2017, 415–421.

Drexl, *Josef*, *et al.*, Data Ownership and Access to Data – Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate, Max Planck Institute for Innovation & Competition Research Paper No. 16–10, 2016, https://ssrn.com/abstract=2833165.

Dropbox, Wieviel kostet Dropbox, https://www.dropbox.com/de/help/billing/cost (zuletzt abgerufen am 9.5.2019).

Drygala, *Tim*, Die Reformdebatte zum AGB-Recht im Lichte des Vorschlags für ein einheitliches europäisches Kaufrecht, JZ 2012, 983–992.

DSK, Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, Positionsbestimmung, 2018.

–, Kurzpapier Nr. 20 – Einwilligung nach der DS-GVO, 2019.

–, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, 2019.

Ducato, *Rossana/Strowel*, *Alain*, Limitations to Text and Data Mining and Consumer Empowerment: Making the Case for a Right to „Machine Legibility", IIC 2019, 649–684.

de la Durantaye, *Katharina*, Allgemeine Bildungs- und Wissenschaftsschranke, Berlin 2014.

–, Wille und Erklärung, Tübingen 2020.

Durumeric, *Zakir*, *et al.*, Analysis of the HTTPS certificate ecosystem, Proceedings of the 2013 Conference on Internet Measurement Conference 2013, 291–304.

Dwork, *Cynthia*, Differential privacy, in: van Tilborg, Henk C.A./Jajodia, Sushil (Hrsg.), Encyclopedia of Cryptography and Security, Boston 2011, 338–340.

Dworkin, *Gerald*, The Theory and Practice of Autonomy, Cambridge, UK, u. a. 1988.

Ebers, *Martin*, EuGH: Hypothekenvollstreckungsverfahren und Inhaltskontrolle, LMK 2013, 345483.

–, Rechte, Rechtsbehelfe und Sanktionen im Unionsprivatrecht, Tübingen 2016.

Ebinger, *Peter*, *et al.*, Privacy in smart metering ecosystems, 1st International Workshop on Smart Grid Security 2012, 120–131.

Eckhardt, *Diederich*, Die ‚Vergleichsfalle' als Problem der Auslegung adressatenloser Annahmeerklärungen nach § 151 S. 1 BGB, BB 1996, 1945–1953.

Edwards, *Lilian*, Privacy, security and data protection in smart cities: A critical EU law perspective, 2 European Data Protection Law Review 2016, 28–58.
Efroni et al., Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing, 5 European Data Protection Law Review 2019, 352–366.
Egelman, *Serge*, *et al.*, Timing is everything? The effects of timing and placement of online privacy indicators, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2009, 319–328.
Egelman, *Serge/Felt*, *Adrienne Porter/Wagner*, *David*, Choice architecture and smartphone privacy: There'sa price for that, in: Böhme, Rainer (Hrsg.), The Economics of Information Security and Privacy, Berlin u. a. 2013, 211–236.
Ehinger, *Patrick/Stiemerling*, *Oliver*, Die urheberrechtliche Schutzfähigkeit von Künstlicher Intelligenz am Beispiel von Neuronalen Netzen, CR 2018, 761–770.
Ehmann, *Eugen/Selmayr*, *Martin* (Hrsg.), Datenschutz-Grundverordnung, 2. Aufl., München 2018.
Ehmann, *Horst*, Informationsschutz und Informationsverkehr im Zivilrecht, AcP 188 (1988), 230–380.
Eichenhofer, *Johannes*, Privatheit im Internet als Vertrauensschutz. Eine Neukonstruktion der Europäischen Grundrechte auf Privatleben und Datenschutz, Der Staat 55 (2016), 41–67.
Eidenmüller, *Horst*, Der homo oeconomicus und das Schuldrecht: Herausforderungen durch Behavioral Law and Economics, JZ 2005, 216–224.
Eifert, *Martin*, Regulierungsstrategien, in: Hoffmann-Riem, Wolfgang/Schmidt-Aßmann, Eberhard/Voßkuhle, Andreas (Hrsg.), Grundlagen des Verwaltungsrechts – Band I, 2. Aufl., München 2012, 1319–1394.
Eisenbarth, *Thomas*, *et al.*, A survey of lightweight-cryptography implementations, 24 IEEE Design & Test of Computers 2007, 522–533.
Eisenberg, *Melvin Aron*, The Limits of Cognition and the Limits of Contract, 47 Stanford Law Review 1995, 211–259.
Eisenhardt, *Ulrich*, Zum subjektiven Tatbestand der Willenserklärung – Aktuelle Probleme der Rechtsgeschäftslehre, JZ 1986, 875–881.
Eisner, *Marc Allen/Worsham*, *Jeff/Ringquist*, *Evan J.*, Contemporary Regulatory Policy, Boulder u. a. 2000.
El Haddouti, *Samia/El Kettani*, *Mohamed Dafir Ech-Cherif*. Towards an Interoperable Identity Management Framework: a Comparative Study, 12 IJCSI International Journal of Computer Science Issues 2015, 98–106.
Elvy, *Stacy-Ann*, Paying for Privacy and the Personal Data Economy, 117 Columbia Law Review 2017, 1369–1454.
Emami-Naeini, *Pardis*, *et al.*, Privacy expectations and preferences in an IoT world, Thirteenth Symposium on Usable Privacy and Security (SOUPS) 2017, 399–412.
Enck, *William*, *et al.*, TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones, 32 ACM Transactions on Computer Systems (TOCS) 2014, 5–20.
Engel, *Andreas*, Internationales Kapitalmarktdeliktsrecht. Eine Untersuchung zum anwendbaren Recht der Prospekthaftung und der Haftung für fehlerhafte *Ad-hoc*-Publizität in den USA und der EU, Tübingen 2019.
Engeler, *Malte*, Das überschätzte Kopplungsverbot, ZD 2018, 55–62.
Engeler, *Malte/Felber*, *Wolfram*, Entwurf der ePrivacy-VO aus Perspektive der aufsichtsbehördlichen Praxis, ZD 2017, 251–257.

Engert, *Andreas*, Regelungen als Netzgüter: Eine Theorie der Rechtsvereinheitlichung im Vertragsrecht, AcP 213 (2013), 321–365.
–, Digitale Plattformen, AcP 218 (2018) 304–376.
Engisch, *Karl*, Die Einheit der Rechtsordnung, Heidelberg 1935.
Englehardt, *Steven/Narayanan*, *Arvind*, Online tracking: A 1-million-site measurement and analysis, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 1388–1401.
Ennöckl, *Daniel*, Der Schutz der Privatsphäre in der elektronischen Datenverarbeitung, Wien 2014.
Entschließung der 25. Internationalen Konferenz der Datenschutzbeauftragten, Sydney, 2003, zur Verbesserung der Bekanntmachung der Praktiken zum Datenschutz, in: LDA/BBDI, Dokumente zu Datenschutz und Informationsfreiheit 2003, Potsdam 2004, 91–95.
Epping, *Volker/Hillgruber*, *Christian* (Hrsg.), BeckOK Grundgesetz, 39. Ed. 15.11.2018, München 2018.
Eppler, *Martin J./Mengis*, *Jeanne*, The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, MIS, and Related Disciplines, 20 Information Society 2004, 325–344.
Ernst, *Stefan*, Social Plugins: Der „Like-Button" als datenschutzrechtliches Problem, NJOZ 2010, 1917–1919.
–, Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, 110–114.
Etro, *Federico*, Search Advertising, Vox CEPR Policy Portal (11.6.2011), https://voxeu.org/article/search-advertising.
Europäische Kommission, Strategie für einen digitalen Binnenmarkt für Europa, COM(2015) 192 final.
–, Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte, COM(2015) 634 final.
–, Aufbau einer Europäischen Datenwirtschaft, COM(2017) 9 final.
–, Weißbuch zur Künstlichen Intelligenz, COM(2020) 65 final.
European Commission, Cookies, in: The EU Internet Handbook, http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm (zuletzt besucht am 30.5.2020).
–, Attitudes on Data Protection and Electronic Identity in the European Union, Special Eurobarometer 359, Brüssel 2011.
–, A Digital Single Market Strategy for Europe – Analysis and Evidence, Commission Staff Working Document, SWD (2015) 100 final.
–, Advancing the Internet of Things in Europe, Commission Staff Working Document, COM(2016) 180 final.
–, An emerging offer of „personal information management services". Current state of service offers and challenges, Report, Brüssel 2016.
–, Building a European Data Economy, COM(2017) 9 final.
European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, Brüssel, 8.10.2019.
European Data Protection Supervisor, Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, Preliminary Opinion, Brüssel 2014.

–, Opinion on Personal Information Management Systems: Towards more user empowerment in managing and processing personal data, Opinion 9/2016, Brüssel 2016.
–, On the coherent enforcement of fundamental rights in the age of big data, Opinion 8/2016, Brüssel 2016.
–, EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation), Opinion 6/2017, Brüssel 2017.
–, Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, Brüssel 2017.
Evans, *Dave*, The Internet of Everything. How More Relevant and Valuable Connections Will Change the World, Cisco Internet Business Solutions Group (IBSG), Report, San Jose, CA 2012.
Evans, *David S./Schmalensee*, *Richard*, The industrial organization of markets with two-sided platforms, 3 Competition Policy International 2007, 151–179.
Everling, *Ulrich*, Zur Auslegung des durch EG-Richtlinien angeglichenen nationalen Rechts, ZGR 1992, 376–395.
Evers, *Jürgen*, Die Nichtigkeit von Handelsvertreterverträgen wegen zu geringer Verdienstmöglichkeiten und ihre Rückabwicklung, BB 1992, 1365–1374.
Ezrachi, *Ariel/Stucke*, *Maurice E.*, Is Your Digital Assistant Devious?, Oxford Legal Studies Research Paper No. 52/2016, University of Tennessee Legal Studies Research Paper No. 304, https://ssrn.com/abstract=2828117.
Fabian, *Benjamin/Ermakova*, *Tatiana/Lentz*, *Tino*, Large-scale readability analysis of privacy policies, Proceedings of the International Conference on Web Intelligence 2017, 18–25.
Fairfield, *Joshua A.T./Engel*, *Christoph*, Privacy as a Public Good, 65 Duke Law Journal 2015, 385–457.
Faragher, *Ramsey/Harle*, *Robert*, Location fingerprinting with bluetooth low energy beacons, 33 IEEE Journal on Selected Areas in Communications 2015, 2418–2428.
Fastrich, *Lorenz*, Richterliche Inhaltskontrolle im Privatrecht, München 1992.
Faust, *Florian*, EuGH: Zivilrecht – Allgemeines Schuldrecht, JuS 2009, 1049–1054.
–, Digitale Wirtschaft – Analoges Recht: Braucht das BGB ein Update?, Gutachten zum 71. Deutschen Juristentag, 2016.
Fechner, *Frank*, Anmerkung zu *Lindqvist*, JZ 2004, 246–248.
Federal Trade Commission, Mobile Privacy Disclosures. Building trust through transparency. FTC staff report, Washington D.C. 2013.
–, Data Brokers. A Call for Transparency and Accountability, Washington D.C. 2014.
–, Internet of Things. Privacy & Security in a Connected World, Washington D.C. 2015.
–, Putting Disclosures to the Test: Staff Summary, Washington D.C. 2016.
–, Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act, Presseerklärung (8.1.2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.
Fezer, *Karl-Heinz*, Dateneigentum, MMR 2017, 3–5.
Fikentscher, Wolfgang/Hacker, Philipp/Podszun, Rupprecht, FairEconomy. Crises, Culture, Competition and the Role of Law, Berlin/Heidelberg 2013.
Filistrucchi, *Lapo*, Market definition in multi-sided markets, in: OECD (Hrsg.), Rethinking Antitrust Tools for Multi-Sided Platforms, Paris 2018, 37–54.
de Filippi, *Primavera/Wright*, *Aaron*, Blockchain and the Law, Cambridge, MA 2018.

Financial Conduct Authority, Stimulating interest: Reminding savers to act when rates decrease, Occasional Paper No.7, London 2015.

Finck, *Michèle/Pallas*, *Frank*, They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data Under the GDPR, International Data Privacy Law (im Erscheinen), https://ssrn.com/abstract=3462948.

Fischel, *Daniel R./Easterbrook*, *Frank*, The Economic Structure of Corporate Law, Cambridge, MA/London 1996.

Fischer-Hübner, *Simone/Berthold*, *Stefan*, Privacy Enhancing Technologies, in: Vacca, John R. (Hrsg.), Computer and Information Security Handbook, 3. Aufl. 2017, 759–778.

Fischer-Hübner, *Simone/Wästlund*, *Erik/Zwingelberg*, *Harald*, UI prototypes: Policy administration and presentation, Version 1, Deliverable D4. 3.1 of the EC FP7 project PrimeLife, o. O. 2009.

Fisher, *Tom*, Social media intelligence and profiling in the insurance industry, Medium (24.4.2017), https://medium.com/privacy-international/social-media-intelligence-and-profiling-in-the-insurance-industry-4958fd11f86f.

Fleischer, *Holger*, Der Rechtsmißbrauch zwischen Gemeineuropäischem Privatrecht und Gemeinschaftsprivatrecht JZ 2003, 865–874.

Fleischer, *Victor*, Regulatory Arbitrage, 89 Texas Law Review 2010, 227–289.

Fluitt, *J. Aaron*, *et al.*, Data Protection's Composition Problem, 5 European Data Protection Law Review 2019, 285–292.

Flume, *Werner*, Rechtsgeschäft und Privatautonomie, in: von Cammerer, Ernst, et al. (Hrsg.), Hundert Jahre deutsches Rechtsleben. Festschrift zum hundertjährigen Bestehen des deutschen Juristentages 1860–1960, Karlsruhe 1960, 135–238

–, Zur Anwendung der Saldotheorie im Fall der Nichtigkeit eines Grundstücks-Kaufvertrags nach § 138 Abs. 1 BGB wegen verwerflicher Gesinnung des Käufers, ZIP 2001, 1621–1623.

–, Allgemeiner Teil des Bürgerlichen Rechts, Zweiter Band: Das Rechtsgeschäft, 4. Aufl., Heidelberg/New York 1992.

Foerster, *Max*, Automatisierung und Verantwortung im Zivilrecht, ZfPW 2019, 418–435.

Föhlisch, *Carsten*, Der „New Deal for Consumers" der EU-Kommission, CR 2018, 583–588.

Föhlisch, *Carsten/Pilous*, *Madeleine*, Der Facebook Like-Button – datenschutzkonform nutzbar? – Analyse und Risikoeinschätzung des „Gefällt mir"-Buttons auf Webseiten, MMR 2015, 631–636.

Föhlisch, *Carsten/Stariradeff*, *Tanya*, Zahlungsmittel und Vertragsschluss im Internet, NJW 2016, 353–358.

Fokusgruppe Verbrauchersouveränität und Transparenz, Nationaler IT-Gipfel 2015, One-Pager Datenschutzhinweise, Berlin 2015.

Forbes Technology Council, Looking Ahead: The Industries that Will Change the most as Machine Learning Grows, Forbes (8.3.2017), https://www.forbes.com/sites/forbestechcouncil/2017/03/08/looking-ahead-the-industries-that-will-change-the-most-as-machine-learning-grows/.

Forbrukerrådet, Deceived by Design, Bericht, 2018, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

Forgó, *Nikolaus/Helfrich*, *Markus/Schneider*, *Jochen* (Hrsg.), Betrieblicher Datenschutz, 3. Aufl., München 2019.

Fornasier, *Matteo*, Freier Markt und zwingendes Vertragsrecht, Baden-Baden 2013.

–, The Impact of EU Fundamental Rights on Private Relationships: Direct or Indirect Effect?, 23 European Review of Private Law 2015, 29–46.
–, Entwicklungen in der Rechtsprechung zum Europäischen Arbeitsrecht 2018, GPR 2019, 141–148.
Forst, *Gerrit*, Die Rechte des Arbeitnehmers infolge einer rechtswidrigen Datenverarbeitung durch den Arbeitgeber, AuR 2010, 106–112.
de Franceschi, *Alberto*, in: Schmidt-Kessel, Martin/Kramme, Malte (Hrsg.), Geschäftsmodelle in der digitalen Welt, Jena 2017, 113–138.
Franck, *Jens-Uwe*, Eine Frage des Zusammenhangs: Marktbeherrschungsmissbrauch durch rechtswidrige Konditionen, ZWeR 2016, 137–164.
Franken, *Gertjan/Van Goethem*, *Tom/Joosen*, *Wouter*, Who left open the cookie jar? A comprehensive evaluation of third-party cookie policies, 27th USENIX Security Symposium (USENIX Security 18) 2018, 151–168.
Frankfurt, *Harry G.*, Freedom of the Will and the Concept of a Person, 68 The Journal of Philosophy 1971, 5–20.
Franzen, *Martin*, Privatrechtsangleichung durch die Europäische Gemeinschaft, Berlin/New York 1999.
Franzen, *Martin/Gallner*, *Inken/Oetker*, *Hartmut*, Kommentar zum europäischen Arbeitsrecht, 2. Aufl., München 2018.
Fraunhofer-Allianz Big Data, Zukunftsmarkt Künstliche Intelligenz. Potenziale und Anwendungen, Sankt Augustin/Leipzig 2017.
Freund, *Renate/Shagdar*, *Ariunzaya*, Sozialdatenschutz – europäisch?, SGb 2018, 195–205.
Fries, Martin, PayPal Law und Legal Tech – Was macht die Digitalisierung mit dem Privatrecht?, NJW 2016, 2860–2865.
Frings, *Michael*, Annahme des Erlaßangebotes durch Scheckeinlösung?, BB 1996, 809–812.
Fritsch, *Michael/Wein*, *Thomas/Ewers*, *Hans-Jürgen*, Marktversagen und Wirtschaftspolitik, 7. Aufl., München 2007.
Frömming, *Jens/Peters*, *Butz*, Die Einwilligung im Medienrecht, NJW 1996, 958–962.
Furrer, *Andreas*, Die Sperrwirkung des sekundären Gemeinschaftsrechts auf die nationalen Rechtsordnungen. Die Grenzen des nationalen Gestaltungsspielraums durch sekundärrechtliche Vorgaben unter besonderer Berücksichtigung des „nationalen Alleingangs", Baden-Baden 1994.
Fuster, *Andreas*, *et al.*, Predictably Unequal? The Effects of Machine Learning on Credit Markets, Working Paper, 2018, https://ssrn.com/abstract=3072038.
Gabel, *Sebastian/Guhl*, *Daniel/Klapper*, *Daniel*, P2V-MAP: Mapping Market Structures for Large Retail Assortments, 56 Journal of Marketing Research 2019, 557–580.
Gal, *Michal S.*, Algorithmic Challenges to Autonomous Choice, 25 Michigan Technology Law Review 2018, 59–104.
Gal, *Michal S./Elkin-Koren*, *Niva*, Algorithmic Consumers, 30 Harvard Journal of Law and Technology 2016, 309–353.
Gallé, *Matthias/Christofi*, *Athena/Elsahar*, *Hady*, The Case for a GDPR-specific Annotated Dataset of Privacy Policies, Proceedings of the PAL: Privacy-Enhancing Artificial Intelligence and Language Technologies 2019, 21–23.
Gamba, *Julien*, *et al.*, An Analysis of Pre-installed Android Software, Working Paper, 2019, https://arxiv.org/abs/1905.02713.

Gambaro, *Antonio*, Abuse of rights in civil law tradition, 4 European Review of Private Law 1995, 561–570.

Gambs, *Sébastien/Killijian*, *Marc-Olivier/Del Prado Cortez*, *Miguel Núñez*, De-anonymization attack on geolocated data, 80 Journal of Computer and System Sciences 2014, 1597–1614.

Gänswein, *Olivier*, Der Grundsatz unionsrechtskonformer Auslegung nationalen Rechts, Frankfurt a. M. 2009.

Garvie, *Clare*, Garbage In, Garbage Out. Face Recognition on Flawed Data, Center on Privacy & Technology, Georgetown Law, Report, Washington D.C. 2019.

Garvie, *Clare/Bedoya*, *Alvaro/Frankle*, *Jonathan*, The Perpetual Line-Up: Unregulated Police Face Recognition in America, Center on Privacy & Technology, Georgetown Law, Report, Washington D.C. 2016.

Gavison, *Ruth*, Privacy and the Limits of Law, 89 Yale Law Journal 1980, 421–471.

Geiger, *Christophe/Frosio*, *Giancarlo/Bulayenko*, *Oleksandr*, The Exception for Text and Data Mining (TDM) in the Proposed Directive on Copyright in the Digital Single Market – Legal Aspects, Briefing for the JURI committee of the European Parliament, Brüssel 2018.

Gellert, *Raphaël*, Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative, 5 International Data Privacy Law 2015, 3–19.

Genzsch, *Madeleine*, Harmonie durch Kontrolle? Chinas Sozialkreditsystem, in: Loitsch, Tobias (Hrsg.), China im Blickpunkt des 21. Jahrhunderts, Berlin/Heidelberg 2019, 129–142.

Geppert, *Martin/Schütz*, *Raimund* (Hrsg.), Beck'scher TKG-Kommentar, 4. Aufl., München 2013.

Geradin Damien/Katsifis, *Dimitrios*, An EU competition law analysis of online display advertising in the programmatic age, European Competition Journal 2019, DOI: 10.1080/17441056.2019.1574440, 1–42.

Gershenfeld, *Neil/Krikorian*, *Raffi/Cohen*, *Danny*, The Internet of Things, 291 Scientific American 2004, 76–81.

Gesellschaft für Informatik, Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen, Berlin 2018.

Gideon, *Julia*, *et al.*, Power strips, prophylactics, and privacy, oh my!. Proceedings of the Second Symposium on Usable Privacy and Security (SOUPS) 2006, 133–144.

Gierschmann, *Sibylle*, Positionsbestimmung der DSK zur Anwendbarkeit des TMG, ZD 2018, 297–301.

Gierschmann, *Sibylle*, Was „bringt" deutschen Unternehmen die DS-GVO? – Mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD 2016, 51–55.

Gierschmann, *Sybille/Schlender*, *Katharina/Stentzel*, *Rainer/Veil*, *Winfried* (Hrsg.), Kommentar Datenschutz-Grundverordnung, Köln 2017.

Gillis, *Talia B./Spiess*, *Jann L.*, Big Data and Discrimination, 86 University of Chicago Law Review 2019, 459–488.

Giocoli, *Nicola*, When low is no good: Predatory pricing and US antitrust law (1950–1980), 18 The European Journal of the History of Economic Thought 2011, 777–806.

Globocnik, *Jure*, On Joint Controllership for Social Plugins and Other Third-Party Content – a Case Note on the CJEU Decision in Fashion ID, 50 ICC 2019, 1033–1044.

Gluck, *Joshua*, *et al.*, How short is too short? Implications of length and framing on the effectiveness of privacy notices, Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016, 321–340.
Gola, *Peter* (Hrsg.), DS-GVO. Kommentar, 2. Aufl., München 2018.
Gola, *Peter/Klug*, *Christoph*, Die Entwicklung des Datenschutzrechts im zweiten Halbjahr 2018, NJW 2019, 639–642.
Gola, *Peter/Piltz*, *Carlo*, Die Datenschutz-Haftung nach geltendem und zukünftigem Recht – ein vergleichender Ausblick auf Art. 77 DS-GVO, RDV 2015, 279–285.
Goldfarb, *Avi/Greenstein*, *Shane/Tucker*, *Catherine*, Introduction, in: Avi Goldfarb/Shane Greenstein/Catherine Tucker (Hrsg.), Economic Analysis of the Digital Economy, Chicago/London 2015, 1–17.
Goldhammer, *Klaus/Wiegand*, *André*, Ökonomischer Wert von Verbraucherdaten für Adress- und Datenhändler, Gutachten für das BMJV, Berlin 2017.
Golland, *Alexander*, Das Kopplungsverbot in der Datenschutz-Grundverordnung, MMR 2018, 130–135.
–, Datenverarbeitung in sozialen Netzwerken, Frankfurt a. M. 2019.
Good, *Nathaniel*, *et al.*, Stopping spyware at the gate: a user study of privacy, notice and spyware, Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS) 2005, 43–52.
Goodfellow, *Ian/Bengio*, *Yoshua/Courville*, *Aaron*, Deep Learning, Cambridge, MA 2016.
Goodfellow, *Ian/McDaniel*, *Patrick/Papernot*, *Nicolas*, Making machine learning robust against adversarial inputs, 61(7) Communications of the ACM 2018, 56–66.
Goodman, *Ellen P./Powles*, *Julia*, Urbanism under Google: Lessons from Sidewalk Toronto, Fordham Law Review (im Erscheinen), https://www.ssrn.com/abstract=3390610.
Google, Nutzungsbedingungen für Google Analytics, https://www.google.com/analytics/terms/de.html (zuletzt abgerufen am 14.6.2019).
Gopavaram, *Shakthidhar Reddy*, *et al.*, IoTMarketplace: Informing Purchase Decisions with Risk Communication, Working Paper, 2019, ftp://svn.soic.indiana.edu/pub/techreports/TR742.pdf.
Gordon, *Michael I.*, *et al.* Information flow analysis of android applications in DroidSafe, Network and Distributed System Security (NDSS) Symposium 2015, 110–125.
Gottschalk, *Eckart*, Das Transparenzgebot und allgemeine Geschäftsbedingungen, AcP 206 (2006), 555–597.
Grabitz, *Eberhard/Hilf*, *Meinhard*, Das Recht der Europäischen Union, 40. Aufl., München 2009.
Grabitz, *Eberhard/Hilf*, *Meinhard/Nettesheim*, *Martin*, Das Recht der Europäischen Union: EUV/AEUV, 65. EL, München, August 2018.
Graef, *Inge/Clifford*, *Damian/Valcke*, *Peggy*, Fairness and enforcement: bridging competition, data protection, and consumer law, 8 International Data Privacy Law 2018, 200–223.
Graef, *Inge/Verschakelen*, *Jeroen/Valcke*, *Peggy*, Putting the right to data portability into a competition law perspective, 4 Law: The Journal of the Higher School of Economics, Annual Review 2013, 53–63.
Graf von Westphalen, *Friedrich*, AGB-Recht im Jahr 2011, NJW 2012, 2243–2250.
–, Unionsrechtliche Folgen des AGB-Missgriffs, NJW 2012, 1770–1773.
–, Richtlinienentwurf der Kommission betreffend die Bereitstellung digitaler Inhalte und das Recht des Verbrauchers auf Schadensersatz, BB 2016, 1411–1418.

–, Nutzungsbedingungen von Facebook – Kollision mit europäischem und deutschem AGB-Recht, VuR 2017, 323–332.
–, Der (unzulässige) Rückgriff auf die ergänzende Vertragsauslegung bei unwirksamen Zinsänderungsklauseln, MDR 2019, 76–82.
–, Ersetzung einer missbräuchlichen Klausel durch dispositives nationales Recht? – Spannungsverhältnis zwischen EuGH- und BGH-Judikatur, BB 2019, 67–74.
Graf von Westphalen, *Friedrich/Wendehorst*, *Christiane*, Hergabe personenbezogener Daten für digitale Inhalte, BB 2016, 2179–2187.
von Grafenstein, *Maximilian*, Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit, DuD 2015, 789–795.
–, Co-Regulation and the Competitive Advantage in the GDPR: data protection certification mechanisms, codes of conduct and the „state of the art" of data protection-by-design, in: González Fuster, Gloria, et al. (Hrsg.), Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics, Cheltenham 2020 (im Erscheinen).
Gray, *Stacey*, Always On: Privacy Implications of Microphone-Enabled Devices, Future of Privacy Forum, Washington, D.C. 2016.
Grimm, *Anna*, Telematiktarife Existierende [sic] Tarifmodelle und ihre Funktionsweisen im Kfz-Bereich, in: Schmidt-Kessel/Grimm (Hrsg.), Telematiktarife & Co. – Versichertendaten als Prämienersatz, 2018, 47–60.
Grimmelmann, *James/Westreich*, *Daniel*, Incomprehensible Discrimination, 7 California Law Review Online 2016, 164–177.
Groß, *Nadja/Gressel*, *Jacqueline*, Entpersonalisierte Arbeitsverhältnisse als rechtliche Herausforderung – Wenn Roboter zu Kollegen und Vorgesetzten werden, NZA 2016, 990–996.
Grossklags, *Jens/Acquisti*, *Alessandro*, When 25 Cents is too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information, Proceedings of the Sixth Workshop on Economics of Information Security 2007, 1–22.
Grosz, *Barbara*, What question would Turing pose today?. 33(4) AI Magazine 2012, 73–81.
Grünberger, *Michael*, Verträge über digitale Güter, AcP 218 (2018), 213–296.
–, Responsive Rechtsdogmatik – Eine Skizze, AcP 219 (2019), 924–942.
Grünberger, *Michael/Jansen*, *Nils*, Perspektiven deutscher Privatrechtstheorie in: Grünberger, Michael/Jansen, Nils (Hrsg.), Privatrechtstheorie heute, Tübingen 2017, 1–44.
Grünberger, *Michael/Washington*, *Jermaine*, Anmerkung, JZ 2019, 1104–1108.
Grundmann, *Stefan*, Richtlinienkonforme Auslegung im Bereich des Privatrechts – insbesondere: der Kanon der nationalen Auslegungsmethoden als Grenze?, ZEuP 1996, 399–424.
–, Europäisches Schuldvertragsrecht, ZGR-Sonderheft 15, Berlin/New York 1999.
–, Das Thema Systembildung im Europäischen Privatrecht – Gesellschafts-, Arbeits- und Schuldvertragsrecht, in: Grundmann (Hrsg.), Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts, Tübingen 2000, 1–49.
–, Privatautonomie im Binnenmarkt, JZ 2000, 1133–1143.
–, Die Dogmatik der Vertragsnetze, AcP 207 (2007), 718–767.
–, On the Unity of Private Law from a Formal to a Substance-Based Concept of Private Law, 6 European Review of Private Law 2010, 1055–1078.
–, Europäisches Gesellschaftsrecht, 2. Aufl., Heidelberg 2011.

–, Gesellschaftsordnung und Privatrecht, in: Grundmann, Stefan/Micklitz, Hans-W./Renner, Moritz (Hrsg.), Privatrechtstheorie, Band I, Tübingen 2015, 405–443.
–, Privatautonomie, Vertragsfunktion und „Richtigkeitschance"?, in: Grundmann, Stefan/Micklitz, Hans-W./Renner, Moritz (Hrsg.), Privatrechtstheorie, Band I, Tübingen 2015, 875–902.
–, Wissen und Information, in: Grundmann, Stefan/Micklitz, Hans-W./Renner, Moritz (Hrsg.), Privatrechtstheorie, Band I, Tübingen 2015, 968–984.
–, Privatrecht und Regulierung, in: Auer, Marietta, *et al.*, Privatrechtsdogmatik im 21. Jahrhundert: Festschrift für Claus-Wilhelm Canaris zum 80. Geburtstag, Berlin/Boston, 2017, 907–948.
– (Hrsg.), Staub, HGB, Bd. 11/1, Bankvertragsrecht/Investment Banking I, 5. Aufl., Berlin 2017.
–, Decision Making in Chains and Networks of Contracts, in: Grundmann, Stefan/Hacker, Philipp (Hrsg.), Theories of Choice. The Social Science and the Law of Decision Making, Oxford 2020, (im Erscheinen).
–, Pluralistische Privatrechtstheorie, Working Paper, 2020.
Grundmann, *Stefan/Hacker*, *Philipp*, Digital technology as a challenge to European Contract Law, 13 European Review of Contract Law 2017, 255–293.
Grundmann, *Stefan/Kerber*, *Wolfgang/Weatherill*, *Stephen*, Party Autonomy and the Role of Information – an Overview, in: Grundmann, Stefan, et al. (Hrsg.), Party Autonomy and the Role of Information in the Internal Market, Berlin/New York 2001, 3–38.
Grundmann, *Stefan/Micklitz*, *Hans-W./Renner*, *Moritz*, Privatrechtstheorie – Eine Einführung, in: Grundmann, Stefan/Micklitz, Hans-W./Renner, Moritz (Hrsg.), Privatrechtstheorie, Band I, Tübingen 2015, 1–38.
Grünwald, *Andreas/Nüßing*, *Christoph*, Machine To Machine (M2M)-Kommunikation – Regulatorische Fragen bei der Kommunikation im Internet der Dinge, MMR 2015, 378–383.
Grunwald, *Armin*, Technikgestaltung – Eine Einführung in die Thematik, in: Grunwald, Armin (Hrsg.), Technikgestaltung zwischen Wunsch und Wirklichkeit, Berlin/Heidelberg 2003, 1–16.
Gsell, *Beate*, Der europäische Richtlinienvorschlag zu bestimmten vertragsrechtlichen Aspekten der Bereitstellung digitaler Inhalte, ZUM 2018, 75–82.
Guggenberger, *Nikolas*, Datenverarbeitung durch Banken im Endkundengeschäft: Grundsätze, Forderungsabtretung und Scoring, ZBB 2019, 254–261.
Guha, *Saikat/Cheng*, *Bin/Francis*, *Paul*, Privad: Practical Privacy in Online Advertising, 8th USENIX Symposium on Networked Systems Design and Implementation 2011, 169–182.
Guihot, *Michael*, Coherence in technology law, 11 Law, Innovation and Technology 2019, 311–342.
–, Neue Grenzlinien für die Direktwirkung nicht umgesetzter EG-Richtlinien unter Privaten. Zur Unanwendbarkeit richtlinienwidriger nationaler Verbotsgesetze im Konflikt unter Privaten, EuZW 2001, 143–149.
Gundel, *Jörg*, EuGH: Strengere nationale Regelungen für Lebensmittelzusatzstoffe, EuZW 2003, 334–344.
Günther, *Jan-Philipp*, Roboter und rechtliche Verantwortung, München 2016.
Guo, *Mengzhuo*, *et al.*, An interpretable machine learning framework for modelling human decision behavior, Working Paper, 2019, https://arxiv.org/abs/1906.01233.

Haag, *Nils Christian*, Direktmarketing mit Kundendaten aus Bonusprogrammen, Wiesbaden 2010.

Habersack, *Mathias/Mayer*, *Christian*, Die überschießende Umsetzung von Richtlinien, in: Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 3. Aufl., Berlin 2015, 297–325.

Hacker, *Philipp*, The Behavioral Divide, 11 European Review of Contract Law 2015, 299–345.

–, Nudge 2.0 – The Future of Behavioural Analysis of Law, in Europe and Beyond, 24 European Review of Private Law 2016, 297–322.

–, Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things, 7 International Data Privacy Law 2017, 266–286.

–, Verhaltensökonomik und Normativität. Die Grenzen des Informationsmodells im Privatrecht und seine Alternativen, Tübingen 2017.

–, Mehrstufige Informationsanbieterverhältnisse zwischen Datenschutz und Störerhaftung, MMR 2018, 779–784.

–, Nudging and Autonomy. A Philosophical and Legal Appraisal, in: Micklitz, Hans-W., et al. (Hrsg.), Research Methods in Consumer Law. A Handbook, Cheltenham 2018, 77–118.

–, Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies against Algorithmic Discrimination under EU Law, 55 Common Market Law Review 2018, 1143–1185.

–, Verhaltens- und Wissenszurechnung beim Einsatz von Künstlicher Intelligenz, RW 9 (2018), 243–288.

–, Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht, ZfPW 2019, 148–197.

–, Exploitative Contracts im Zeitalter maschinellen Lernens. Eine rechtsökonomische Analyse, in: Faust, Florian/Schäfer, Hans-Bernd (Hrsg.), Zivilrechtliche und rechtsökonomische Probleme des Internet und der künstlichen Intelligenz, Tübingen 2019, 97–129.

–, Personalized Law and the Behavioural Sciences, in: Busch, Christoph/de Franceschi, Alberto (Hrsg.), Data Economy and Algorithmic Regulation: A Handbook on Personalized Law, Baden-Baden 2020 (im Erscheinen).

–, Regulating the Economic Impact of Data as Counter-Performance: From the Illegality Doctrine to the Unfair Contract Terms Directive, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, Oxford/Baden-Baden 2020 (im Erscheinen), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3391772.

–, A Legal Framework for AI Training Data, Working Paper, 2020, https://ssrn.com/abstract=3556598.

–, Digitale Marktordnung durch Urheber- und Datenschutzrecht, in: Hanno Merkt, Hanno, et al. (Hrsg.), Festschrift Hopt, Berlin 2020, 351–379.

Hacker, *Philipp/Petkova*, *Bilyana*, Reining in the Big Promise of Big Data. Transparency, Inequality, and New Regulatory Frontiers, 15 Northwestern Journal of Technology and Intellectual Property 2017, 1–42.

Hacker, *Philipp/Krestel*, *Ralf/Grundmann*, *Stefan/Naumann*, *Felix*, Explainable AI under Contract and Tort Law: Legal Incentives and Technical Challenges, 28 Artificial Intelligence and the Law 2020, DOI: https://doi.org/10.1007/s10506-020-09260-6.

Hacker, *Philipp/Lianos*, *Ioannis/Dimitropoulos*, *Georgios/Eich*, *Stefan*, Regulating Blockchain. Techno-Social and Legal Challenges – An Introduction, in: *Hacker*, *Philipp/Lianos*, *Ioannis/Dimitropoulos*, *Georgios/Eich*, *Stefan*, (Hrsg.), Regulating Blockchain. Techno-Social and Legal Challenges, Oxford 2019, 1–24.

Hacker, *Philipp/Lianos*, *Ioannis/Dimitropoulos*, *Georgios/Eich*, *Stefan* (Hrsg.), Regulating Blockchain. Techno-Social and Legal Challenges, Oxford 2019.

Hackl, *Karl*, Äquivalenzstörung und Sittenwidrigkeit, BB 1977, 1412–1415.

Hahn, *Hartmut*, Kein allgemeiner Rechtsgrundsatz des Missbrauchs- bzw. Umgehungsverbots, jurisPR-SteuerR 15/2006 Anm. 1.

Hall, *Joseph Lorenzo/Hans*, *G.S./Henry*, *Lauren*, Comments for November 2013 Workshop on the „Internet of Things" (1.6.2013), https://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00028-86211.pdf.

Hallinan, *Dara*, Data Protection without Data: Could Data Protection Law Apply without Personal Data Being Processed?, 5 European Data Protection Law Review 2019, 293–299.

Han, *Seungyeop/Jung*, *Jaeyeon/Wetherall*, *David*, A study of third-party tracking by mobile apps in the wild, University of Washington Technical Report UW-CSE-12–03–01, 2012.

Hanloser, *Stefan*, Anmerkung zu BGH: Opt-out durch Streichen der Einwilligungsklausel – HappyDigits, MMR 2010, 140–141.

–, Geräte-Identifier im Spannungsfeld von DS-GVO, TMG und ePrivacy-VO, ZD 2018, 213–218.

–, Anmerkung zu Fashion ID, ZD 2019, 458–460.

–, DSK-Orientierungshilfe für Anbieter von Telemedien, ZD 2019, 287–290.

–, Keine gemeinsame Verantwortlichkeit für Datenspeicherung durch Facebook – Fashion ID, ZD 2019, 122–124.

–, Umsetzungslücken bei der ePrivacy-RL – Planet49, ZD 2019, 264–266.

Hans-Bredow-Institut, Study on Co-Regulation Measures in the Media Sector, Study for the European Commission, Directorate Information Society and Media, Hamburg 2006.

Hansen, *Marit*, *et al.* Privacy-enhancing identity management, 9 Information Security Technical Report 2004, 35–44.

Hansen, *Marit/Hoepman*, *Jaap-Henk/Jensen*, *Meiko*, Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, ENISA Report, Heraklion 2015.

Hansen, *Marit/Limniotis*, *Konstantinos*, Recommendations on shaping technology according to GDPR provisions. Exploring the notion of data protection by default, ENISA Report, Attiki 2018.

Harder, *Manfred*, Minderjährige Schwarzfahrer, NJW 1990, 857–864.

Harkous, *Hamza*, *et al.*, Polisis: Automated analysis and presentation of privacy policies using deep learning, 27th USENIX Security Symposium 2018, 531–548.

Härting, *Niko*, EuGH: Auslegung von „Verarbeitung personenbezogener Daten", CR 2009, 229–233.

–, Fanpages auf Facebook, ITRB 2012, 109–111.

–, „Dateneigentum" – Schutz durch Immaterialgüterrecht?, CR 2016, 646–649.

–, Datenschutz-Grundverordnung, 2016 *Härting*, Datenschutz-Grundverordnung, Köln 2016.

–, Internetrecht, 6. Aufl., Köln 2017.

–, Joint Controllership nach der DSGVO, ITRB 2018, 167–170.

Haucap, *Justus/Heimeshoff*, *Ulrich*, Google, Facebook, Amazon, eBay: Is the Internet driving competition or market monopolization?, 11 International Economics and Economic Policy 2014, 49–61.

Haugeland, *John*, Introduction, in: id. (Hrsg.), Artificial Intelligence. The Very Idea, Cambridge, MA 1985, 1–12.

Hausman, *Daniel M./Welch*, *Brynn*, Debate: To Nudge or Not to Nudge, 18 Journal of Political Philosophy 2010, 123–136.

Hayek, *Friedrich A.*, The Constitution of Liberty. The Definitive Edition, hg. von Ronald Hamowy, The Collected Works of F.A. Hayek, Vol. XVII, Chicago 2011 [1960].

Hayek, *Friedrich A.*, The Use of Knowledge in Society, 35 American Economic Review 1945, 519–530.

Heinrich, *Christian*, Formale Freiheit und materiale Gerechtigkeit, Tübingen 2000.

Heinrichs, *Helmut*, Das Gesetz zur Änderung des AGB-Gesetzes Umsetzung der EG-Richtlinie über mißbräuchliche Klauseln in Verbraucherverträgen durch den Bundesgesetzgeber, NJW 1996, 2190–2197.

Heinze, *Christian*, BGH: Keine Bereicherungsansprüche des Werkunternehmers bei Schwarzarbeit, LMK 2014, 360329.

–, Schadensersatz im Unionsprivatrecht. Eine Studie zu Effektivität und Durchsetzung des Europäischen Privatrechts am Beispiel des Haftungsrechts, Tübingen 2017.

Heinzke, *Philippe/Engel*, *Lennart*, Datenverarbeitung zur Vertragserfüllung – Anforderungen und Grenzen, ZD 2020, 189–194.

Helberger, *Natali*, Profiling and Targeting Consumers in the Internet of Things, in: Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Digital Revolution: Challenges for Contract Law in Practice, Baden-Baden 2016, 135–162.

Helberger, *Natali/Zuiderveen Borgesius*, *Frederik/Reyna*, *Agustin*, The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law, 54 Common Market Law Review 2017, 1427–1466.

Heldt, *Amélie*, Anmerkung, MMR 2018, 333.

Helle, *Jürgen*, Die Einwilligung beim Recht am eigenen Bild, AfP 1985, 93–101.

Hellgardt, *Alexander*, Regulierung und Privatrecht, Tübingen 2016.

–, Wer hat Angst vor der unmittelbaren Drittwirkung?, JZ 2018, 901–911.

Hellman, *Martin E.*, An Overview of Public Key Cryptography, 40(5) IEEE Communications Magazine 2002, 42–49.

Hennigs, *Stefan*, Anmerkung zu EuGH: Höheres nationales Schutzniveau bei missbräuchlichen Klauseln, GRUR 2012, 641–642.

Hennrichs, *Joachim/Pferdmenges*, *Stefanie*, BGH: Abtretung von Darlehensforderungen zwischen Bankgeheimnis und Datenschutz – Arbeitsplatzbegriff, LMK 2007, 233564.

Hepburn, *Glen*, Alternatives to Traditional Regulation, OECD Report, Paris 2006.

Herbert, *Manfred*, 100 Jahre Doppelwirkungen im Recht, JZ 2011, 503–513.

Herbst, *Tobias*, Was sind personenbezogene Daten?, NVwZ 2016, 902–906.

Herfurth, *Constantin*, Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO, ZD 2018, 514–520.

Hermstrüwer, *Yoan*, Informationelle Selbstgefährdung. Zur rechtsfunktionalen, spieltheoretischen und empirischen Rationalität der datenschutzrechtlichen Einwilligung und des Rechts auf informationelle Selbstbestimmung, Tübingen 2016.

–, Contracting Around Privacy: The (Behavioral) Law and Economics of Consent and Big Data, 8 JIPITEC 2017, 9–26.

Hermstrüwer, *Yoan/Dickert*, *Stephan*, Sharing is daring: An experiment on consent, chilling effects and a salient privacy nudge, 51 International Review of Law and Economics 2017, 38–49.

Herresthal, *Carsten*, Rechtsfortbildung im europarechtlichen Bezugsrahmen, München 2006.

De Hert, *Paul*, *et al.*, The right to data portability in the GDPR: Towards user-centric interoperability of digital services, 34 Computer Law & Security Review 2018, 193–203.

Hesselink, *Martijn*, The General Principles of Civil Law, in: Leczykiewicz, Dorota/Weatherill, Stephen (Hrsg.), The Involvement of EU Law in Private Law Relationships, 2013, 131–180.

Hetcher, *Steven A.*, Norms in a Wired World, Cambridge, UK 2004.

Heuer-James, *Jens-Uwe/Chibanguza*, *Kuuya/Stücker*, *Benedikt*, Industrie 4.0 – vertrags- und haftungsrechtliche Fragestellungen, BB 2018, 2818–2832.

Heun, *Sven-Erik/Assion*, *Simon*, Internet(recht) der Dinge, CR 2015, 812–818.

–, Smart Services: IT- und datenschutzrechtliche Herausforderungen, BB 2018, 579–584.

Heun-Rehn, *Stefan/Lang*, *Sonja/Ruf*, *Isabelle*, Neue (Un-)Klarheit bezüglich Innenprovisionen und Rückvergütungen bei Kapitalanlagen, NJW 2014, 2909–2913.

Hildebrandt, *Mireille*, Smart Technologies and the End(s) of Law, Cheltenham 2015.

Hill, *Kashmir*, The Secretive Company That Might End Privacy as We Know It, New York Times (18.1.2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Hill, *Thomas*, Autonomy and Self-Respect, Cambridge, UK 1991.

Hinton, *Geoffrey E.*, Learning distributed representations of concepts, Proceedings of the Eighth Annual Conference of the Cognitive Science Society 1986, 1–12.

Hinton, *Geoffrey E./Osindero*, *Simon/Teh*, *Yee-Whye*, A fast learning algorithm for deep belief nets, 18 Neural Computation 2006, 1527–1554.

Hintze, *Mike*, In defense of the long privacy statement, 76 Maryland Law Review 2017, 1044–1085.

von Hippel, *Fritz*, Das Problem der rechtsgeschäftlichen Privatautonomie. Beiträge zu einem Natürlichen System des privaten Verkehrsrechts und zur Erforschung der Rechtstheorie des 19. Jahrhunderts, Tübingen 1936.

Hoepman, *Jaap-Henk*, Privacy Design Strategies, IFIP International Information Security Conference 2014, 446–459.

Hoeren, *Thomas*, Internet und Recht – Neue Paradigmen des Informationsrechts, NJW 1998, 2849–2854.

–, Big Data und Datenqualität – ein Blick auf die DS-GVO, ZD 2016, 459–463.

–, Thesen zum Verhältnis von Big Data und Datenqualität – Erstes Raster zum Erstellen juristischer Standards, MMR 2016, 8–11.

–, Kartell- oder Datenschutzrecht: BKartA untersagt Facebook die Zusammenführung von Nutzerdaten, MMR 2019, 137–138.

Hoffmann, *Christian*, Die Verletzung der Vertraulichkeit informationstechnischer Systeme durch Google Street View, CR 2010, 514–518.

Holl, *Jürgen/Kernbeiß*, *Günter/Wagner-Pinter*, *Michael*, Das AMS-Arbeitsmarktchancen-Modell. Dokumentation zur Methode, Wien 2018.

Holtz, *Leif-Erik/Nocun*, *Katharina/Hansen*, *Marit*, Towards displaying privacy information with icons, IFIP PrimeLife International Summer School on Privacy and Identity Management for Life, 2011, 338–348.

Hommelhoff, *Peter/Wiedenmann*, *Kai-Udo*, Allgemeine Geschäftsbedingungen gegenüber Kaufleuten und unausgehandelte Klauseln in Verbraucherverträgen, ZIP 1993, 562–572.

Hoofnagle, *Chris Jay/Kesari*, *Aniket/Perzanowski*, *Aaron*, The Tethered Economy, 87 George Washington Law Review 2019, 783–874.

Hoofnagle, *Chris Jay/Whittington*, *Jan*, Free: Accounting for the Costs of the Internet's Most Popular Price, 61 UCLA Law Review 2014, 606–670.

Hooker, *Brad*, Fairness, in: Honderich, Ted (Hrsg.), The Oxford Companion to Philosophy, 2. Aufl., Oxford 2005, 287–288.

Höpfner, *Clemens*, Die systemkonforme Auslegung, Tübingen 2008.

Hornung, *Gerrit*, Anmerkung zu Schecke, MMR 2011, 127–128.

Horowitz, *John K./McConnell*, *Kenneth E.*, A review of WTA/WTP studies, 44 Journal of Environmental Economics and Management 2002, 426–447.

Hu, *Jie/Shen*, *Li/Sun*, *Gang*, Squeeze-and-excitation networks, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2018, 7132–7141.

Hundepool, *Anco*, *et al.*, Statistical Disclosure Control, West Sussex 2012.

Hustinx, *Peter*, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, Working Paper, 2014, https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en.

Huthmacher, *Karl Eugen*, Der Vorrang des Gemeinschaftsrechts bei indirekten Kollisionen, Köln 1985.

Iglesias Sánchez, *Sara*, Unfair terms in mortgage loans and protection of housing in times of economic crisis: *Aziz* v. *Catalunyacaixa*, 51 Common Market Law Review 2014, 955–974.

Indenhuck, *Moritz/Britz*, *Thomas*, Vom Datenschutzrecht zum Datenschuldrecht – Neue Leitlinien zur Verarbeitung personenbezogener Daten bei Online-Dienstleistungen, BB 2019, 1091–1096.

Independent Centre for Privacy Protection Schleswig-Holstein/Studio Notarile Genghini, Identity Management Systems (IMS): Identification and Comparison, Study prepared under contract for Institute for Prospective Technological Studies, Sevilla 2003.

Information Commissioner's Office/Alan Turing Institute, Explaining decisions made with AI, Draft Guidance, 2019.

International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy by Design, Jerusalem 2010.

Irion, *Kristina/Luchetta*, *Giacomo*, Online Personal Data Processing and EU Data Protection Reform, CEPS Task Force Report, Brüssel 2013.

Islam, *Mohammad Badiul*, Privacy by Design for Social Networks, PhD Thesis, Brisbane 2014, https://eprints.qut.edu.au/71389/1/Mohammad%20Badiul_Islam_Thesis.pdf.

Iyengar, *Sheena S./Lepper*, *Mark R.*, When choice is demotivating: Can one desire too much of a good thing?, 79 Journal of Personality and Social Psychology, 2000, 995–1006.

J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, hrsg. v. Baldus, Christian, et al., Berlin, unterschiedliche Jahre (zit.: *Bearbeiter*, in: Staudinger, BGB).

Jacobs, *Matthias*, Aktuelle Entwicklungen im deutschen und europäischen Antidiskriminierungsrecht, RdA 2018, 263–270.

Jacquemain, *Tobias*, Haftung privater Stellen bei Datenschutzverstößen, RDV 2017, 227–235.

James, *Gareth*, *et al.*, An Introduction to Statistical Learning, New York 2013.

Jandt, *Silke/Roßnagel*, *Alexander*, Datenschutz in Social Networks – Kollektive Verantwortlichkeit für die Datenverarbeitung, ZD 2011, 160–166.

–, Social Networks für Kinder und Jugendliche – Besteht ein ausreichender Datenschutz?, MMR 2011, 637–642.

Jansen, *Nils*, Die Struktur des Haftungsrechts, Tübingen 2003.

Jara, *Antonio J./Ladid*, *Latif/Gómez-Skarmeta*, *Antonio Fernandez*, The Internet of Everything through IPv6: An Analysis of Challenges, Solutions and Opportunities, 4 Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 2013, 97–118.

Jarass, *Hans D.*, Das allgemeine Persönlichkeitsrecht im Grundgesetz, NJW 1989, 857–862.

– (Hrsg.), Charta der Grundrechte der EU, 3. Aufl., München 2016.

Jarass, *Hans D./Beljin*, *Saša*, Die Bedeutung von Vorrang und Durchführung des EG-Rechts für die nationale Rechtsetzung und Rechtsanwendung, NVwZ 2004, 1–11.

Jarovsky, *Luiza*, Improving Consent in Information Privacy through Autonomy-Preserving Protective Measures (APPMs), 4 European Data Protection Law Review 2018, 447–458.

Jentzsch, *Nicola/Preibusch*, *Sören/Harasser*, *Andreas*, Study on Monetising Privacy: An Economic Model for Pricing Personal Information, European Network and Information Security Agency, Heraklion 2012.

Joachim, *Katharina*, Besonders schutzbedürftige Personengruppen. Einordnung gruppenspezifischer Schutzbedürftigkeit in der DS-GVO, ZD 2017, 414–418.

John, *Leslie K./Acquisti*, *Alessandro/Loewenstein*, *George*, Strangers on a plane: Context-dependent willingness to divulge sensitive information, 37 Journal of Consumer Research 2011, 858–873.

Johannes, *Paul C./Roßnagel*, *Alexander*, Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt, Kassel 2016.

Jolls, *Christine/Sunstein*, *Cass R.*, Debiasing through Law, 35 The Journal of Legal Studies 2006, 199–242.

Jolls, *Christine/Sunstein*, *Cass R./Thaler*, *Richard*, A Behavioral Approach to Law and Economics, 50 Stanford Law Review 1998, 1471–1550.

Jones, *Meg Leta/Meurer*, *Kevin*, Can (and should) Hello Barbie keep a secret?, 2016 IEEE International Symposium on Ethics in Engineering, Science and Technology (ETHICS), 2016, 1–6.

Jordan, *M.I./Mitchell*, *Tom M.*, Machine learning: Trends, perspectives and prospects, 349 Science 2015, 255–260.

Joshi, *Karuna P.*, *et al.*, Alda: Cognitive assistant for legal document analytics, 2016 AAAI Fall Symposium Series 2016, 149–152.

Jung, *Alexander*, Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO, ZD 2018, 208–213.

Junglas, *Benjamin*, Bankenhaftung bei der Finanzierung von Schrottimmobilien, NJOZ 2013, 49–76.

Kahn, *David*, The Codebreakers. The Story of Secret Writing, New York 1973.

Kahneman, *Daniel/Knetsch*, *Jack L./Thaler*, *Richard H.*, Experimental tests of the endowment effect and the Coase theorem, 98 Journal of Political Economy 1990, 1325–1348.

Kaijser, *Per/Markwitz*, *Wernhard*, Quantenphysik und die Zukunft der Kryptographie, DuD 2008, 396–399.
Kainer, *Friedemann*, Privatrecht zwischen Richtlinien und Grundrechten. Zu den Grenzen richtlinienkonformer Auslegung und horizontalen Richtlinienwirkungen, GPR 2016, 262–270.
–, Rückkehr der unmittelbar-horizontalen Grundrechtswirkung aus Luxemburg?, NZA 2018, 894–900.
Kamann, *Hans-Georg/Miller*, *Robin*, Kartellrecht und Datenschutzrecht – Verhältnis einer „Hass-Liebe"?, NZKart 2016, 405–412.
Kamp, *Johannes*, Personenbewertungsportale, München 2011.
Kampert, *David*, Datenschutz in sozialen Online-Netzwerken de lege lata und de lege ferenda, Hamburg 2016.
Kapsner, *Andreas/Sandfuchs*, *Barbara*, Nudging as a threat to privacy, 6 Review of Philosophy and Psychology, 2015, 455–468.
Karg, *Moritz*, Anwendbares Datenschutzrecht bei Internet-Diensteanbietern – TMG und BDSG vs. Konzernstrukturen?, ZD 2013, 371–375.
–, Anmerkung zu Google Spain, ZD 2014, 359–361.
Karg, *Moritz/Kühn*, *Ulrich*, Datenschutzrechtlicher Rahmen für „Device Fingerprinting" – Das klammheimliche Ende der Anonymität im Internet, ZD 2014, 285–290.
Katz, *Michael L./Shapiro*, *Carl*, Network Externalities, Competition, and Compatibility, 75 American Economic Review 1985, 424–440.
Keirsbilck, *Bert*, The interaction between consumer protection rules on unfair contract terms and unfair commercial practices: *Pereničová und Perenič*, 50 Common Market Law Review 2013, 247–263.
Kelley, *Patrick Gage*, *et al.*, Standardizing privacy notices: An online study of the nutrition label approach, Proceedings of the 28th International Conference on Human Factors in Computing Systems 2010, 1573–1582.
Kerber, *Wolfgang*, Digital Markets, Data and Privacy: Competition Law, Consumer Law and Data Protection, GRUR Int. 2016, 639–647.
Kerkmann, *Christoph*, Wer hat die Macht über den Werbeblock?, Handelsblatt (12.8.2016), https://www.handelsblatt.com/unternehmen/it-medien/facebook-vs-adblock-plus-wer-hat-die-macht-ueber-den-werbeblock/14005570-all.html.
Kersten, *Jens*, Menschen und Maschinen, JZ 2015, 1–8.
Kervizic, *Julien*, Cookies, Tracking and pixels: Where does your Web data comes from?, Medium (22.10.2018), https://medium.com/analytics-and-data/cookies-tracking-and-pixels-where-does-your-web-data-comes-from-ff5d9b8bc8f7
Kesan, *Jay P./Shah*, *Rajiv C.*, Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics, 82 Notre Dame Law Review 2006, 583–634.
Keßler, *Oliver*, Intelligente Roboter – neue Technologien im Einsatz, MMR 2017, 589–594.
Kessler, *Ronald*, Anmerkung, BB 1981, 931–934.
Kilian, *Wolfgang*, Arbeitsrechtliche Probleme automatisierter Personalinformationssysteme, JZ 1977, 481–486.
Kilian, *Wolfgang*, Äußeres und inneres System in einem noch fragmentarischen Europäischen Schuldvertragsrecht?, in: Grundmann (Hrsg.), Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts, 2000, 427–441.
Kim, *Pauline T.*, Data-Driven Discrimination at Work, 58 William & Mary Law Review 2016, 857–936.

Kinast, *Karsten/Kühnl*, *Christina*, Telematik und Bordelektronik – Erhebung und Nutzung von Daten zum Fahrverhalten, NJW 2014, 3057–3061.
Kipker, *Dennis-Kenji/Kubis*, *Marcel*, Anmerkung zu Breyer, MMR 2017, 608–610.
Kipp, *Theodor*, Über Doppelwirkungen im Recht, insbesondere über die Konkurrenz von Nichtigkeit und Anfechtbarkeit, in: Festschrift der Berliner Juristischen Fakultät für Ferdinand von Martitz zum fünfzigjährigen Doktorjubiläum am 24. Juli 1911, Berlin 1911, 211–234.
Kirchhof, *Paul*, Nationale Grundrechte und Unionsgrundrechte. Die Wiederkehr der Frage eines Anwendungsvorrangs unter anderer Perspektive, NVwZ 2014, 1537–1541.
Klar, *Manuel*, Räumliche Anwendbarkeit des (europäischen) Datenschutzrechts – Ein Vergleich am Beispiel von Satelliten-, Luft- und Panoramastraßenaufnahmen, ZD 2013, 109–115.
Klass, *Nadine*, Die zivilrechtliche Einwilligung als Instrument zur Disposition über Persönlichkeitsrechte, AfP 2005, 507–518.
–, Das Recht auf Vergessen(-werden) und die Zeitlichkeit der Freiheit, ZUM 2020, 265–279.
Kleimann Communication Group, Know Before You Owe: Evolution of the Integrated TILA-RESPA Disclosures, Rockville, MD 2012.
Kleinberg, *Jon/Mullainathan*, *Sendhil/Raghavan*, *Manish*, Inherent Trade-Offs in the Fair Determination of Risk Scores, 8th Innovations in Theoretical Computer Science Conference (ITCS 2017) 2017, Article 43, 1–23.
Kleinschmidt, *Jens*, Annahme eines Erlassangebots durch Einlösung eines mit dem Angebot übersandten Verrechnungsschecks?, NJW 2002, 346–348.
Klement, *Jan Henrik*, Öffentliches Interesse an Privatheit, JZ 2017, 161–170.
Klimke, *Dominik*, Telematik-Tarife in der Kfz-Versicherung, r+s 2015, 217–225.
Klinck, *Fabian/Riesenhuber*, *Karl* (Hrsg.), Verbraucherleitbilder: interdisziplinäre und europäische Perspektiven, Berlin 2015.
Kment, *Martin*, Die Stellung nationaler Unbeachtlichkeits-, Heilungs- und Präklusionsvorschriften im europäischen Recht, EuR 2006, 201–235.
Knijnenburg, *Bart/Kobsa*, *Alfred*, Helping Users with Information Disclosure Decisions: Potential for Adaptation, Proceedings of the 2013 ACM International Conference on Intelligent User Interfaces, 407–416.
Knopp, *Michael*, Datenschutzherausforderung Webtracking, DuD 2010, 783–786.
Koch, *Elisabeth*, Vertragsgerechtigkeit – Rechtshistorische Betrachtungen, in: Festschrift Kanzleiter, Köln 2010, 237–246.
Koenig, *Christian/Neumann*, *Andreas*, Standardisierung – ein Tatbestand des Kartellrechts?, WuW 2009, 382–394.
Köhler, *Helmut*, Schwarzarbeitsverträge: Wirksamkeit, Vergütung, Schadensersatz, JZ 1990, 466–472.
–, Wettbewerbsverstoß und Vertragsnichtigkeit, JZ 2010, 767–774.
Köhler, *Helmut/Bornkamm*, *Joachim/Feddersen*, *Jörn* (Hrsg.), Gesetz gegen den unlauteren Wettbewerb (UWG), 38. Aufl., München 2020.
Kohn, *Joachim*, Der Schadensersatzanspruch nach Art. 82 DS-GVO, ZD 2019, 498–502.
Kohno, *Tadayoshi/Broido*, *Andre/Claffy*, *Kimberly C.*, Remote physical device fingerprinting, 2 IEEE Transactions on Dependable and Secure Computing 2005, 93–108.
Kohte, *Wolfhard*, Die Rechtsfolgen der Mietpreisüberhöhung – Ein Beitrag zur Differenzierung der Rechtsfolgen unerlaubter Rechtsgeschäfte, NJW 1982, 2803–2807.

–, Die rechtfertigende Einwilligung, AcP 185 (1985), 105–161.
–, Rechtsschutz gegen die Vollstreckung des wucherähnlichen Rechtsgeschäfts nach § 826 BGB – Ein Beitrag zur Normzwecklehre bei sittenwidriger Schädigung, NJW 1985, 2217–2230.
Kokol, *Peter/Verlic*, *Mateja/Krizmaric*, *Miljenko*, Modeling teens clothing fashion preferences using machine learning, 3 WSEAS Transactions on Information Science and Applications 2006, 2054–2065.
Kokolakis, *Spyros*, Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, 64 Computers & Security 2017, 122–134.
Komendera, *Wolfram*, Normenkonflikte zwischen EWG- und BRD-Recht, Heidelberg 1974.
Köndgen, *Johannes*, Grund und Grenzen des Transparenzgebots im AGB-Recht – Bemerkungen zum „Hypothekenzins-" und zum „Wertstellungs-Urteil" des BGH, NJW 1989, 943–952.
Kondor, *Daniel*, *et al.*, Towards matching user mobility traces in large-scale datasets, IEEE Transactions on Big Data 2018, 1–10.
König, *Julia*, Der Äquivalenz- und Effektivitätsgrundsatz in der Rechtsprechung des EuGH, Baden-Baden 2011.
Konrad, *Lasse*, Verbotene Klarnamenpflicht bei Facebook und die DSGVO, K&R 2018, 275–276.
Koops, *Bert-Jaap*, The (in)flexibility of techno-regulation and the case of purpose-binding, 5 Legisprudence 2011, 171–194.
–, The Trouble with European Data Protection Law, 4 International Data Privacy Law 2014, 250–261.
Koops, *Bert-Jaap/Leenes*, *Ronald*, Privacy regulation cannot be hardcoded. A critical comment on the „privacy by design" provision in data-protection law, 28 International Review of Law, Computers & Technology 2014, 159–171.
Körber, *Torsten*, Grundfreiheiten und Privatrecht, Tübingen 2004.
–, „Ist Wissen Marktmacht?" Überlegungen zum Verhältnis von Datenschutz, „Datenmacht" und Kartellrecht – Teil 2, NZKart 2016, 348–356.
–, Die Facebook-Entscheidung des Bundeskartellamtes – Machtmissbrauch durch Verletzung des Datenschutzrechts?, NZKart 2019, 187–195.
Korobkin, *Russell B./Ulen*, *Thomas S.*, Law and behavioral science: Removing the rationality assumption from law and economics, 88 California Law Review 2000, 1051–1144.
Korobkin, *Russell*, The Status Quo Bias and Contract Default Rules, 83 Cornell Law Review 1998, 608–687.
Kosinski, *Michal/Stillwell*, *David/Graepel*, *Thore*, Private traits and attributes are predictable from digital records of human behavior, 110 Proceedings of the National Academy of Sciences 2013, 5802–5805.
Kosta, *Eleni*, Peeking into the cookie jar: the European approach towards the regulation of cookies, 21 International Journal of Law and Information Technology 2013, 380–406.
Kötz, *Hein*, Zur Wirksamkeit von Freizeichnungsklauseln, NJW 1984, 2447–2448.
–, Der Schutzzweck der AGB-Kontrolle – Eine rechtsökonomische Skizze, JuS 2003, 209–214.
Koziol, *Helmut*, Sonderprivatrecht für Konsumentenkredite?, AcP 188 (1988), 183–229.

Kraft, *Mirko/Hering*, *Julia*, Potenziale von Telematik-Tarifen in der Kfz-Versicherung in Deutschland, ZVersWiss 106 (2017), 503–524.
Kring, *Markus/Marosi*, *Johannes*, Ein Elefant im Porzellanladen – Der EuGH zu Personenbezug und berechtigtem Interesse K&R 2016, 773–776.
Krizhevsky, *Alex/Sutskever*, *Ilya/Hinton*, *Geoffrey E.*, Imagenet classification with deep convolutional neural networks, Advances in Neural Information Processing Systems 2012, 1097–1105.
Krohm, *Niclas*, Abschied vom Schriftformgebot der Einwilligung – Lösungsvorschläge und künftige Anforderungen, ZD 2016, 368–373.
Krohm, *Niclas/Müller-Peltzer*, *Philipp*, Auswirkungen des Kopplungsverbots auf die Praxistauglichkeit der Einwilligung, ZD 2017, 551–556.
Krönke, *Christoph*, Datenpaternalismus. Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung, Der Staat 55 (2016), 319–351.
Krügel, *Tina*, Das personenbezogene Datum nach der DS-GVO, ZD 2017, 455–460.
Krüger, *Ulrich*, Aufklärung und Beratung bei Kapitalanlagen – Nebenpflicht statt Beratungsvertrag, NJW 2013, 1845–1850.
Krusche, *Jan*, Kumulation von Rechtsgrundlagen zur Datenverarbeitung, ZD 2020, 232–237.
Kuempel, *Ashley*, The Invisible Middleman: A Critique and Call for Reform of the Data Broker Industry, 36 Northwestern Journal of International Law & Business 2016, 207–234.
Kühling, *Jürgen*, Rückkehr des Rechts: Verpflichtung von „Google & Co." zu Datenschutz, EuZW 2014, 527–532.
–, Das „Recht auf Vergessenwerden" vor dem BVerfG – November(r)evolution für die Grundrechtsarchitektur im Mehrebenensystem, NJW 2020, 275–280.
Kühling, *Jürgen/Buchner*, *Benedikt* (Hrsg.), DS-GVO/BDSG, 2. Aufl., München 2018.
Kühling, *Jürgen/Klar*, *Manuel*, Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität, NJW 2013, 3611–3617.
–, Anmerkung zu Breyer, ZD 2017, 27–29.
Kühling, *Jürgen/Klar*, *Manuel/Sackmann*, *Florian*, Datenschutzrecht, 4. Aufl., Heidelberg 2018.
Kühling, *Jürgen/Martini*, *Mario*, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448–454.
Kühling, *Jürgen/Sackmann*, *Florian*, Das Mehrebenensystem der Datenschutzgrundrechte im Lichte der Rechtsprechung von BVerfG und EuGH, JURA 2018, 364–377.
–, Irrweg Dateneigentum", ZD 2020, 24–30.
Kulms, *Katrin*, Der Effektivitätsgrundsatz, Baden-Baden 2013.
Kumar, *Eupuri Prasanna*, Cloud and Edge Computing for an IoT-Based Smart Grid, DZone (19.3.2017), https://dzone.com/articles/cloud-computing-and-edge-computing-for-an-iot-base.
Kumar, *Vineet*, Making ‚Freemium' Work: Many Start-ups Fail to Recognize the Challenges of This Popular Business Model, 92(5) Harvard Business Review 2014, 27–29.
Kumaraguru, *Ponnurangam/Cranor*, *Lorrie F.*, Privacy Indexes: A Survey of Westin's Studies, Working Paper, Institute for Software Research International, School of Computer Science, Carnegie Mellon University, Pittsburgh 2005.

Kummer, *Michael/Schulte*, *Patrick*, When private information settles the bill: Money and privacy in Google's market for smartphone applications, 65 Management Science 2019, 3470–3494.

Kuner, *Christopher/Cate*, *Fred H./Millard*, *Christopher/Svantesson*, *Dan Jerker B./Lynskey*, *Orla*, When Two Worlds Collide: The Interface Between Competition Law And Data Protection, 4 International Data Privacy Law 2014, 247–248.

Kuntz, *Wolfgang*, Selbstdatenschutz als wichtiges Instrument für Datenschutz, ZD-Aktuell 2016, 05177.

Künzler, *Adrian*, Direct Consumer Influence – The Missing Strategy to Integrate Data Privacy Preferences into the Market, Working Paper, 2019, https://ssrn.com/abstract=3395928.

Kuschel, *Linda*, Der Erwerb digitaler Werkexemplare zur privaten Nutzung, Tübingen 2019.

Kwet, *Michael*, In Stores, Secret Surveillance Tracks Your Every Move, New York Times (14.6.2019), https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html.

Laibson, *David*, Golden Eggs and Hyperbolic Discounting, 112 Quarterly Journal of Economics 1997, 443–475.

Lang, *Sonja/Peintinger*, *Stefan*, Die wirksame Einwilligung im Datenschutzrecht, ELR 2013, 206–215.

Langhanke, *Carmen*, Daten als Leistung, Tübingen 2018.

Langhanke, *Carmen/Schmidt-Kessel*, *Martin*, Consumer Data as Consideration, EuCML 2015, 218–223.

Langheinrich, *Marc*, Privacy by Design – principles of privacy-aware ubiquitous systems, in: Abowd, Gregory D., et al. (Hrsg.), Ubicomp 2001: Ubiquitous Computing, Berlin/Heidelberg 2001, 273–291.

–, A privacy awareness system for ubiquitous computing environments, International Conference on Ubiquitous Computing 2002, 237–245.

Larenz, *Karl*, Lehrbuch des Schuldrechts, Band 1, Allgemeiner Teil, 14. Aufl., München 1987.

Larenz, *Karl/Canaris*, *Claus-Wilhelm*, Methodenlehre der Rechtswissenschaft, 3. Aufl., Berlin/Heidelberg 1995.

Larrick, *Richard P.*, Debiasing, in: Koehler, Derek J./Harvey, Nigel (Hrsg.), Blackwell Handbook of Judgment and Decision Making, Malden, MA u. a. 2004, 316–338.

Laue, *Philip*, Öffnungsklauseln in der DS-GVO – Öffnung wohin?, ZD 2016, 463–467.

Laue, *Philip/Kremer*, *Sascha*, Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl., Baden-Baden 2019.

Lauf, *Niclas/Birck*, *Leon*, Minderjährige als Partei des Behandlungsvertrags, NJW 2018, 2230–2235.

Lawrence, *Steve*, *et al.*, Face recognition: A convolutional neural-network approach, 8 IEEE Transactions on Neural Networks 1997, 98–113.

Le Grand, *Gwendal/Barrau*, *Emilie*, Prior Checking, a Forerunner to Privacy Impact Assessments, in: Wright, David/De Hert, Paul (Hrsg.), Privacy Impact Assessment, Dordrecht u. a. 2012, 97–116.

Le Métayer, *Daniel*, Whom to Trust? Using Technology to Enforce Privacy, in: Wright, David/De Hert, Paul (Hrsg.), Enforcing Privacy, Cham 2016, 395–437.

LeCun, *Yann/Bengio*, *Yoshua/Hinton*, *Geoffrey*, Deep Learning, 521 Nature 2015, 436–444.

Lee, *Laureen/Cross*, *Samuel*, (Gemeinsame) Verantwortlichkeit beim Einsatz von Drittinhalten auf Websites, MMR 2019, 559–562.

Leenes, *Ronald/Lucivero*, *Federica*, Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design, 6 Law, Innovation and Technology 2014, 193–220.

LegalCommDesign, PrivacyFix: Online Privacy Dashboard for social networks, http://www.legaltechdesign.com/communication-design/privacyfix-online-privacy-dashboard-for-social-networks/. Alle in dieser Arbeit zitierten Webseiten wurden, sofern nichts anderes angegeben ist, zuletzt abgerufen am 30.4.2020.

Lessig, *Lawrence*, Code. And Other Laws of Cyberspace, New York 1999.

Lessmann, *Stefan*, *et al.*, Benchmarking state-of-the-art classification algorithms for credit scoring: An update of research, 247 European Journal of Operational Research 2015, 124–136.

Leuschner, *Lars*, Gebotenheit und Grenzen der AGB-Kontrolle: Weshalb M&A-Verträge nicht der Inhaltskontrolle der §§ 305 ff. AGB unterliegen, AcP 207 (2007), 491–529.

von Lewinski, *Kai*, Europäisierung des Datenschutzrechts, DuD 2012, 564–570.

von Lewinski, *Kai/Herrmann*, *Christoph*, Cloud vs. Cloud – Datenschutz im Binnenmarkt, ZD 2016, 467–474.

Lewis, *Randall/Rao*, *Justin/Reiley*, *David*, Measuring the Effects of Advertising. The Digital Frontier, in: Avi Goldfarb/Shane Greenstein/Catherine Tucker (Hrsg.), Economic Analysis of the Digital Economy, Chicago/London 2015, 191–218.

Leyens, *Patrick*, Informationsintermediäre des Kapitalmarkts, Tübingen 2017.

Leyens, *Patrick C./Böttcher*, *Henning*, Anfängerhausarbeit Zivilrecht: Computergenerierte Willenserklärungen, Anfechtbarkeit und Erklärungsrisiken, JuS 2019, 133–138.

Leyens, *Patrick C./Schäfer*, *Hans-Bernd*, Inhaltskontrolle allgemeiner Geschäftsbedingungen: Rechtsökonomische Überlegungen zu einer einheitlichen Konzeption von BGB und DCFR, AcP 210 (2010), 771–803.

Li, *Yuxi*. Deep reinforcement learning: An overview, Working Paper, 2017, https://arxiv.org/abs/1701.07274.

Liang, *Fan*, *et al.*, Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure, 10 Policy & Internet 2018, 415–453.

Lianos, *Ioannis*, Polycentric Competition Law, 71 Current Legal Problems 2018, 161–213.

Lianos, *Ioannis/Motchenkova*, *Evgenia*, Market dominance and search quality in the search engine market, 9 Journal of Competition Law & Economics 2013, 419–455.

Libert, *Timothy*, An automated approach to auditing disclosure of third-party data collection in website privacy policies, Proceedings of the 2018 World Wide Web Conference, 207–216.

Liepina, *Ruta*, *et al.*, GDPR Privacy Policies in CLAUDETTE: Challenges of Omission, Context and Multilingualism, Proceedings of the Third Workshop on Automated Semantic Analysis of Information in Legal Text (ASAIL 2019) 2019, 1–7.

Limniotis, *Konstantinos/Hansen*, *Marit*, Recommendations on shaping technology according to GDPR provisions. An overview on data pseudonymisation, ENISA Report, Attiki 2018.

Lin, *Henry W./Tegmark*, *Max/Rolnick*, *David*, Why does deep and cheap learning work so well?. 168 Journal of Statistical Physics 2017, 1223–1247.

Lin, *Jialiu*, *et al.*, Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing, Proceedings of the 2012 ACM Conference on Ubiquitous Computing 2012, 501–510.
–, Modeling users' mobile app privacy preferences: Restoring usability in a sea of permission settings, 10th Symposium on Usable Privacy and Security (SOUPS) 2014, 199–212.
Lindacher, *Walter*, Grundsätzliches zu § 138 BGB: Zur Frage der Relevanz subjektiver Momente, AcP 173 (1973), 124–136.
Linden, *Thomas*, *et al.* The privacy policy landscape after the GDPR, Working Paper, 2019, https://arxiv.org/abs/1809.08396.
Lindner, *Roland*, Für Amazon wird Werbung wichtiger, FAZ (20. September 2018), http://www.faz.net/aktuell/wirtschaft/diginomics/unternehmen-investieren-werbebudget-vermehrt-bei-amazon-15796306.html.
LinkedIn, Kostenlose LinkedIn Konten und kostenpflichtige Premium-Mitgliedschaften, https://www.linkedin.com/help/linkedin/answer/1412/kostenlose-linkedin-konten-und-kostenpflichtige-premium-mitgliedschaften?lang=de.
Linnenkohl, *Karl R.H.*, *et al.*, Das Recht auf „informationelle Selbstbestimmung" und die Drittwirkungsproblematik im Arbeitsrecht, BB 1988, 57–63.
Lippi, *Marco*, *et al.*, Automated Detection of Unfair Clauses in Online Consumer Contracts, Legal Knowledge and Information Systems (JURIX) 2017, 145–154.
–, CLAUDETTE: an automated detector of potentially unfair clauses in online terms of service, 27 Artificial Intelligence and Law 2019, 117–139.
–, Consumer protection requires artificial intelligence, 1 Nature Machine Intelligence 2019, 168–169.
Liptak, *Andrew*, Amazon's Alexa started ordering people dollhouses after hearing its name on TV, The Verge (7.1.2017), https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse.
Lipton, *Zachary C.*, The mythos of model interpretability, 61(10) Communications of the ACM 2018, 36–43.
Little, *Kayla*, IoT Systems: Sensors and Actuators, DZone (30.6.2017), https://dzone.com/articles/iot-systems-sensors-and-actuators.
Littman, *Michael L.*, Reinforcement learning improves behaviour from evaluative feedback, 521 Nature 2015, 445–451.
Liu, *Bin*, *et al.*, Follow my recommendations: A personalized privacy assistant for mobile app permissions, Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016, 27–41.
Liu, *Fei*, *et al.*, A step towards usable privacy policy: Automatic alignment of privacy statements, Proceedings of COLING 2014, the 25th International Conference on Computational Linguistics: Technical Papers 2014, 884–894.
Loewenstein, *George*, *et al.*, Warning: You are about to be nudged, 1 Behavioral Science & Policy 2015, 35–42.
Lölfing, *Nils*, Die App-Ökonomie des Schenkens, Münster 2017.
Loomans, *Dirk/Matz*, *Manuela/Wiedemann*, *Michael*, Praxisleitfaden zur Implementierung eines Datenschutzmanagementsystems. Ein risikobasierter Ansatz für alle Unternehmensgrößen, Wiesbaden 2014.
Loos, *Marco/Luzak*, *Joasia*, Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers, 39 Journal of Consumer Policy 2016, 63–90.
Lorenz, *Stephan*, Der Schutz vor dem unerwünschten Vertrag, München 1997.

–, BGH: Wucherähnliches Rechtsgeschäft beim Internetkauf, LMK 2012, 332201.
Lu, *Yang*, *et al.*, From Data Disclosure to Privacy Nudges: A Privacy-aware and User-centric Personal Data Management Framework, Proceedings of 5th International Conference on Dependability in Sensor, Cloud, and Big Data Systems and Applications 2019.
Lucas, *John Randolph*, The Principles of Politics, Oxford 1966.
Luck, *Michael/McBurney*, *Peter*, Computing as interaction: agent and agreement technologies, IEEE SMC Conference on Distributed Human-Machine Systems 2008, 1–6.
Lüdemann, *Volker*, Connected Cars – Das vernetzte Auto nimmt Fahrt auf, der Datenschutz bleibt zurück, ZD 2015, 247–254,
Ludwigs, *Markus/Sikora*, *Patrick*, Grundrechtsschutz im Spannungsfeld von Grundgesetz, EMRK und Grundrechtecharta, JuS 2017, 385–393.
Lüttringhaus, *Jan*, Das internationale Datenprivatrecht: Baustein des Wirtschaftskollisionsrechts des 21. Jahrhunderts. Das IPR der Haftung für Verstöße gegen die EU-Datenschutzgrundverordnung, ZVglRWiss 117 (2018), 50–82.
–, Mehr Freiheit wagen im Versicherungsrecht durch daten- und risikoadjustierte Versicherungstarife. „Pay-as-you-drive"-, „Pay-as-you-live"- und „Smart-Home"-Tarife als Herausforderung für das Versicherungsvertragsrecht, in: Festschrift Basedow, Tübingen 2018, 55–72.
–, Vertragsfreiheit und ihre Materialisierung im Europäischen Binnenmarkt, Tübingen 2018.
Lynskey, *Orla*, The Foundations of EU Data Protection Law, Oxford 2015.
–, Delivering Data Protection: The Next Chapter, 21 German Law Journal 2020, 80–84.
MacCarthy, *Mark*, New directions in privacy: Disclosure, unfairness and externalities, 6 I/S: A Journal of Law and Policy 2011, 425–512.
MacCormick, *Neil*, Legal Reasoning and Legal Theory, Oxford 1994.
Madaan, *Aastha/Nurse*, *Jason/de Roure*, *David/O'Hara*, *Kieron/Hall*, *Wendy/Creese*, *Sadie*, A Storm in an IoT Cup: The Emergence of Cyber-Physical Social Machines, Working Paper, 2018, https://ssrn.com/abstract=3250383.
Madaan, *Nishtha/Ahad*, *Mohd Abdul/Sastry*, *Sunil M.*, Data integration in IoT ecosystem: Information linkage as a privacy threat, 34 Computer Law & Security Review 2018, 125–133.
Madakam, *Somayya/Ramaswamy*, *R/Tripathi*, *Siddharth*, Internet of Things (IoT): A literature review, 3 Journal of Computer and Communications 2015, 164–173.
Maier, *Helena*, Marktortanknüpfung im internationalen Kartelldeliktsrecht, Frankfurt a. M. 2011.
Maier, *Natalie/Schaller*, *Fabian*, ePrivacy-VO – alle Risiken der elektronischen Kommunikation gebannt?, ZD 2017, 373–377.
Mainetti, *Luca/Mighali*, *Vincenzo/Patrono*, *Luigi*. An IoT-based user-centric ecosystem for heterogeneous smart home environments, IEEE International Conference on Communications (ICC) 2015, 704–709.
Majer, *Christian F.*, Sittenwidrigkeit und Äquivalenzstörungen – das wucherähnliche Geschäft, DNotZ 2013, 644–657.
Maler, *Eve*, Extending the power of consent with user-managed access: A standard architecture for asynchronous, centralizable, internet-scalable consent, 2015 IEEE Security and Privacy Workshops 2015, 175–179.

Malgieri, *Gianclaudio*, The concept of fairness in the GDPR: a linguistic and contextual interpretation, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 154–166.
Malgieri, *Gianclaudio/Custers*, *Bart*, Pricing privacy – the right to know the value of your personal data, 34 Computer Law & Security Review 2018, 289–303.
Malzer, *Matthias*, Vertragsverbünde und Vertragssysteme, Baden-Baden 2013.
Mangold, *Anna Katharina*, Gemeinschaftsrecht und deutsches Recht, Tübingen 2011.
–, Das Böckenförde-Diktum, VerfBlog (9.5.2019), https://verfassungsblog.de/das-boeckenfoerde-diktum/.
Mankiw, *N. Gregory*, Macroeconomics, 9. Aufl., New York 2015.
Mankowski, *Peter*, Anmerkung zum Urteil des OLG Frankfurt vom 24.1.2018, Az. 13 U 165/16, EWiR 2018, 209–210.
Manne, *Geoffrey A./Wright*, *Joshua D.*, Google and the limits of antitrust: The case against the case against Google, 34 Harvard Journal of Law & Public Policy 2011, 171–244.
Manning, *Christopher*, *et al.*, The Stanford CoreNLP natural language processing toolkit, Proceedings of 52nd Annual Meeting of the Association for Computational Linguistics: System Demonstrations 2014, 55–60.
Mansour, *Yishay/Muthukrishnan*, *S./Nisan*, *Noam*, Doubleclick Ad Exchange Auction, Working Paper, 2012, https://arxiv.org/pdf/1204.0535.
Mantz, *Reto*, Störerhaftung für Datenschutzverstöße Dritter – Sperre durch DS-RL und DS-GVO?, ZD 2014, 62–66.
Mantz, *Reto/Spittka*, *Jan*, Anmerkung zu Breyer, NJW 2016, 3582–3583.
Marín López, *Manuel Jesús*, La „voluntad virtual" del consumidor, ¿un nuevo test para determinar la abusividad de una cláusula no negociada en contratos con consumidores?, Revista CESCO de Derecho de Consumo 2013 (5), 35–40.
Marosi, *Johannes/Matthé*, *Luisa*, Anmerkung zu Wirtschaftsakademie Schleswig-Holstein, ZD 2018, 361–363.
Marotta-Wurgler, *Florencia*, Does ‚Notice and Choice' Disclosure Regulation Work? An Empirical Study of Privacy Policies, Michigan Law: Law and Economics Workshop, 2015, www.law.umich.edu/centersandprograms/lawandeconomics/workshops/Documents/Paper13.Marotta-Wurgler.Does%20Notice%20and%20Choice%20Disclosure%20Work.pdf.
Marsch, *Nikolaus*, Das europäische Datenschutzgrundrecht, Tübingen 2018.
Marsden, *Christopher T.*, Internet Co-Regulation. European law, regulatory governance and legitimacy in cyberspace, Cambridge, UK 2011.
Martens, *Klaus-Peter*, Rechtsgeschäft und Drittinteressen, AcP 177 (1977), 113–188.
Martinelli, *Silvia*, Sharing Data and Privacy in the Platform Economy: The Right to Data Portability and „Porting Rights", in: Reins, Leonie (Hrsg.), Regulating New Technologies in Uncertain Times, The Hague *et al.* 2019, 133–152.
Martini, *Mario*, Do it yourself im Datenschutzrecht. Der „GeoBusiness Code of Conduct" als Erprobungsfeld regulierter Selbstregulierung, NVwZ-Extra 6/2016, 1–13.
Martini, *Mario/Fritzsche*, *Saskia*, Mitverantwortung in sozialen Netzwerken, NVwZ 2015, 1497–1499.
Mäsch, *Gerald*, Kein bereicherungsrechtlicher Wertersatzanspruch des Schwarzarbeiters, JuS 2014, 1123–1125.
Matheson, *Rob*, The privacy risks of compiling mobility data, MIT News (7.12.2018), https://news.mit.edu/2018/privacy-risks-mobility-data-1207.

Maxwell, *Winston*, Principles-based regulation of personal data: the case of ‚fair processing', 5 International Data Privacy Law 2015, 205–216.
Mayer-Maly, *Theo*, Renaissance der laesio enormis?, in: Festschrift Larenz, München 1983, 395–409.
–, Was leisten die guten Sitten, AcP 194 (1994), 105–176.
–, Anmerkung zu BGH, 19. 9. 1995 – VI ZR 377/94, JZ 1996, 419–419.
Mayer-Schönberger, *Viktor*, delete. The Virtue of Forgetting in the Digital Age, Princeton/Oxford 2009.
Mayer-Schönberger, *Viktor/Cukier*, *Kenneth*, Big Data: A revolution that will transform how we live, work, and think, Boston/New York 2013.
McCarthy, *John*, *et al.*, A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, Hanover, NH 1955.
McCulloch, *Warren S./Pitts*, *Walter*, A logical calculus of the ideas immanent in nervous activity, 5 Bulletin of Mathematical Biophysics 1943, 115–133.
McDonald, *Aleecia M./Cranor*, *Lorrie Faith*, The Cost of Reading Privacy Policies, 4 I/O Journal of Law and Policy for the Information Society 2008, 543–568.
McDonald, *Aleecia M.*, *et al.*, A Comparative Study of Online Privacy Policies and Formats, Proceedings of the 9th Symposium on Usable Privacy and Security 2009, 37–55.
McFarland, *David*, Autonomy and self-sufficiency in robots, in: Steels, Luc/Brooks, Rodney (Hrsg.), The Artificial Life Route to Artificial Intelligence, London 2018, 187–214.
McKay, *Kerry A.*, *et al.*, Report on Lightweight Cryptography, NISTIR 8114, Gaithersburg 2017.
McKinsey Global Institute, The Age of Analytics, Report, London u. a. 2016.
Medicus, *Dieter/Petersen*, *Jens*, Allgemeiner Teil des BGB, 11. Aufl., Heidelberg 2016.
Mell, *Peter/Grance*, *Timothy*, The NIST Definition of Cloud Computing, Special Publication (NIST SP) – 800–145, Gaithersburg 2011.
Mellet, *Kevin/Beauvisage*, *Thomas*, Cookie monsters. Anatomy of a digital market infrastructure, Consumption Markets & Culture 2019, 1–20.
Menezes, *Alfred J.*, Overview of Cryptography, in: *Menezes*, *Alfred J.*, et al. (Hrsg.), Handbook of Applied Cryptography, West Palm Beach 1996, 1–48.
Menzel, *Hans-Joachim*, Datenschutzrechtliche Einwilligungen, DuD 2008, 400–408.
Merener, *Martin M*, Theoretical results on de-anonymization via linkage attacks, 5 Transactions on Data Privacy 2012, 377–402.
Merkt, *Hanno*, Das Informationsmodell im Gesellschafts- und Kapitalmarktrecht, zfbf Sonderheft 55/06, 24–60.
Mestmäcker, *Ernst-Joachim*, Über die normative Kraft privatrechtlicher Verträge, JZ 1964, 441–446.
Metzger, *Axel*, Rechtsgeschäfte über das Droit moral im deutschen und französischen Urheberrecht, München 2002.
–, Extra legem, intra ius. Allgemeine Rechtsgrundsätze im Europäischen Privatrecht, Tübingen 2009.
–, Dienst gegen Daten: Ein synallagmatischer Vertrag, AcP 216 (2016), 817–865.
–, Mehr Freiheit wagen auf dem Markt der Daten, in: Dutta, Anatol/Heinze, Christian (Hrsg.), „Mehr Freiheit wagen". Beiträge zur Emeritierung von Jürgen Basedow (zitiert als: Festschrift Basedow), Tübingen 2018, 131–152.
–, Digitale Mobilität – Verträge über Nutzerdaten, GRUR 2019, 129–136.

–, Verträge über digitale Inhalte und digitale Dienstleistungen: Neuer BGB-Vertragstypus oder punktuelle Reform? JZ 2019, 577–586.
–, A Market Model for Personal Data: State of the Play under the New Directive on Digital Content and Digital Services, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, Oxford/Baden-Baden 2020 (im Erscheinen).
Metzger, *Axel*, *et al.*, Data-Related Aspects of the Digital Content Directive, 9 JIPITEC 2018, 90–109.
Meyer, *Jürgen* (Hrsg.), Charta der Grundrechte der Europäischen Union, 4. Aufl., Baden-Baden 2014.
Meyer, Jürgen/Hölscheidt, Sven (Hrsg.), Charta der Grundrechte der Europäischen Union, 5. Aufl., Baden-Baden 2019.
Meyer, *Sebastian*, Einbindung des Facebook-"Gefällt mir"-Buttons, MMR 2017, 254–258.
Michalski, *Lutz*, Die Berücksichtigung von vertragsabschlußbegleitenden Umständen nach § 24a Nr. 3 AGB-Gesetz, DB 1999, 677–680.
Michl, *Fabian*, Situativ staatsgleiche Grundrechtsbindung privater Akteure, JZ 2018, 911–918.
Michl, *Walther*, Das Verhältnis zwischen Art. 7 und Art. 8 GRCh – zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht, DuD 2017, 349–353.
Micklitz, *Hans-W.*, Europäisches Regulierungsprivatrecht: Plädoyer für ein neues Denken, Teil 1, GPR 2009, 254–263.
–, A Common Approach to the Enforcement of Unfair Commercial Practices and Unfair Contract Terms, in: van Boom, Willem/Garde, Amanine/Orkun, Akseli (Hrsg.), The European Unfair Commercial Practices Directive, Surrey 2014, 173–200.
–, Eigentumsrechte und Digitalisierung, in: Grundmann, Stefan/Micklitz, Hans-W./Renner, Moritz (Hrsg.), Privatrechtstheorie, Band II, Tübingen 2015, 1221–1238.
–, *et al.*, The Empire Strikes Back: Digital Control of Unfair Terms of Online Services, 40 Journal of Consumer Policy 2017, 367–388.
–, Ungeheuerliche Neuigkeiten, VuR 2017, 43–46.
Micklitz, *Hans-W./Reich*, *Norbert*, „Und es bewegt sich doch"? – Neues zum Unionsrecht der missbräuchlichen Klauseln in Verbraucherverträgen, EuZW 2012, 126–128.
Miller, *Amalia R./Tucker*, *Catherine*, Privacy protection and technology diffusion: The case of electronic medical records, 55 Management Science 2009, 1077–1093.
Miller, *George A.*, The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information, 63 The Psychological Review 1956, 81–97.
Miller, *Lucinda*, The Emergence of EU Contract Law: Exploring Europeanization, Oxford 2011.
Milne, *George R./Culnan*, *Mary J.*, Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices, 18 Journal of Interactive Marketing 2004, 15–29.
mip Consult GmbH, Social Plugins für Unternehmen, Blog Sofortdatenschutz (5.4.2018), https://blog.sofortdatenschutz.de/social-plug-ins/.
Miraz, *Mahdi H.*, *et al.*, A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT), IEEE Internet Technologies and Applications (ITA) 2015, 219–224.

Miraz, *Mahdi H.*, *et al.*, Internet of nano-things, things and everything: future growth trends. 10 Future Internet 2018, Article 68, 1–28.
Mischau, *Lena*, Daten als „Gegenleistung" im neuen Verbrauchervertragsrech, ZEuP 2020, 335–365.
Mitchell, *Tom M.*, Machine Learning, New York u. a. 1997.
Mnih, *Volodymyr*, *et al.*, Human-level control through deep reinforcement learning, 518 Nature 2015, 529–533.
Moerel, *Lokke*, CNIL's Decision Fining Google Violates One-Stop-Shop, Working Paper, 2019, https://ssrn.com/abstract=3337478.
Mohassel, *Payman/Zhang*, *Yupeng*, SecureML: A System for Scalable Privacy-Preserving Machine Learning, IEEE Symposium on Security and Privacy (SP) 2017, 19–38.
Möller, *Mirko*, Anmerkung: Widerrufs- und Rückgaberecht bei nichtigem Fernabsatzvertrag – Radarwarngerät, NJW 2010, 612–612.
Monopolkommission, Wettbewerbspolitik: Herausforderung digitale Märkte, Sondergutachten 68, 2015.
Monreal, *Manfred*, Weiterverarbeitung nach einer Zweckänderung in der DS-GVO, ZD 2016, 507–512.
Monteleone, *Shara*, *et al.*, Nudges to privacy behaviour: Exploring an alternative approach to privacy notices, JRC Science and Policy Report, Luxembourg 2015.
de Montjoye, *Yves-Alexandre*, *et al.*, Unique in the crowd: The privacy bounds of human mobility, 3 Scientific Reports 2013, Article 1376, 1–5.
–, On the privacy-conscientious use of mobile phone data, 5 Nature Scientific Data 2018, 180286 (1–6).
Moos, *Flemming/Rothkegel*, *Tobias*, Anmerkung zu Breyer, MMR 2016, 845–847.
–, Anmerkung zu Wirtschaftsakademie Schleswig-Holstein, MMR 2018, 596–600.
–, Anmerkung zu Fashion ID, MMR 2019, 584–587.
–, Anmerkung zu Planet49, MMR 2019, 736–740.
Morais Carvalho, *Jorge*, Sale of Goods and Supply of Digital Content and Digital Services – Overview of Directives 2019/770 and 2019/771, EuCML 2019, 194–201.
Mörsdorf, *Oliver*, Europäisierung des Privatrechts durch die Hintertür?, JZ 2019, 1066–1074.
Möslein, *Florian*, Dispositives Recht. Zwecke, Strukturen und Methoden, Tübingen 2011.
Mowery, *Keaton/Shacham*, *Hovav*, Pixel perfect: Fingerprinting canvas in HTML5, Proceedings of W2SP 2012, 1–12.
Mugdan, *Benno*, Die gesammten Materialien zum Bürgerlichen Gesetzbuch für das Deutsche Reich, Band 2, Berlin 1899.
Münchener Kommentar zum BGB, hrsg. v. Säcker, Franz Jürgen, et al., 8. Aufl., München, unterschiedliche Jahre (zit.: *Bearbeiter*, in: MüKo, BGB).
Murphy, *James J.*, *et al.*, A meta-analysis of hypothetical bias in stated preference valuation, 30 Environmental and Resource Economics 2005, 313–325.
Murray-Rust, *Peter/Molloy*, *Jennifer/Cabell*, *Diane*, Open Content Mining, in: Moore, Samuel A. (Hrsg.), Issues in Open Research Data, London, 2014, 11–30.
Musielak, *Hans-Joachim*, Zum Verhältnis von Wille und Erklärung, AcP 211 (2011), 769–802.
Muth, *Max*, Dieser Anti-Tracking-Browser will Nutzer fürs Werbungschauen belohnen, SZ (19.11.2019), https://www.sueddeutsche.de/digital/brave-browser-chrome-werbung-netz-javascript-tracking-1.4688866.
Narayanan, *Arvind*, *et al.*, Bitcoin and Cryptocurrency Technologies, Princeton 2016.

Narayanan, *Arvind/Shmatikov*, *Vitaly*, Robust De-anonymization of Large Sparse Datasets, Proceedings of the 2008 IEEE Symposium on Security and Privacy 2008, 111–125.

Nassall, *Wendt*, EuGH: Rechtsfolgen der Klauselunwirksamkeit nach der Klauselrichtlinie, LMK 2012, 333461.

National Highway Traffic Safety Administration, Preliminary Statement of Policy Concerning Automated Vehicles, Washington D.C. 2013.

Nationale Akademie der Wissenschaften Leopoldina/acatech – Deutsche Akademie der Technikwissenschaften/Union der deutschen Akademien der Wissenschaften, Individualisierte Medizin – Voraussetzungen und Konsequenzen, Halle (Saale) 2014.

NBC News, Facial Recognition's ‚Dirty Little Secret': Millions of Online Photos Scraped Without Consent, Communications of the ACM (15.3.2019), https://cacm.acm.org/news/235455-facial-recognitions-dirty-little-secret-millions-of-online-photos-scraped-without-consent/fulltext.

Nebbia, *Paolisa*, Unfair Contract Terms in European Law, Oxford/Portland 2007.

Netzer, *Oded*, *et al.*, Mine your own business: Market-structure surveillance through text mining, 31 Marketing Science 2012, 521–543.

Neun, *Andreas/Lubitzsch*, *Katharina*, Die neue EU-Datenschutz-Grundverordnung – Rechtsschutz und Schadensersatz, BB 2017, 2563–2569.

Neuner, *Jörg*, Die Rechtsfortbildung, in: Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 3. Aufl., Berlin 2015, 245–262.

Neunhoeffer, *Friederike*, Das Presseprivileg im Datenschutzrecht, Tübingen 2005.

Niedermeier, *Robert/Schröcker*, *Stefan*, Ersatzfähigkeit immaterieller Schäden aufgrund rechtswidriger Datenverarbeitung, RDV 2002, 217–224.

Niedobitek, *Matthias*, Kollisionen zwischen EG-Recht und nationalem Recht, VerwArch 2001, 58–90.

Nielsen, *Michael/Chuang*, *Isaac*, Quantum Computation and Quantum Information, 10th Anniversary Edition, Cambridge, UK 2010.

Nietsch, *Thomas*, Zur Überprüfung der Einhaltung des Datenschutzrechts durch Verbraucherverbände, CR 2014, 272–278.

Nikiforakis, *Nick*, *et al.*, Cookieless monster: Exploring the ecosystem of web-based device fingerprinting, IEEE Symposium on Security and Privacy 2013, 541–555.

Nilsson, *Nils J.*, Artificial Intelligence. A New Synthesis, San Francisco 1998.

Ning, *Huansheng*, Unit and Ubiquitous Internet of Things, Boca Raton u. a. 2013.

Nink, *Judith/Pohle*, *Jan*, Die Bestimmbarkeit des Personenbezugs – Von der IP-Adresse zum Anwendungsbereich der Datenschutzgesetze, MMR 2015, 563–567.

Nissenbaum, *Helen*, Privacy in Context: Technology, Policy and the Integrity of Social Life, Stanford 2010.

Nitzsche, *Manfred*, Graphen für Einsteiger, 3. Aufl., Wiesbaden 2009.

Norberg, *Patricia A./Horne*, *Daniel R./Horne*, *David A.*, The privacy paradox: Personal information disclosure intentions versus behaviors, 41 Journal of Consumer Affairs 2007, 100–126.

Nord, *Jantina/Manzel*, *Martin*, „Datenschutzerklärungen" – misslungene Erlaubnisklauseln zur Datennutzung – „Happy-Digits" und die bedenklichen Folgen im E-Commerce, NJW 2010, 3756–3578.

Novotny, *Alexander/Spiekermann*, *Sarah*, Personal Information Markets AND Privacy: A New Model to Solve the Controversy, in: Hildebrandt, Mireille, et al. (Hrsg.), Digital Enlightenment Yearbook 2013, Amsterdam u. a. 2013, 102–120.

Obar, *Jonathan/Oeldorf-Hirsch*, *Anne*, The biggest lie on the Internet, 21 Information, Communication & Society 2018, 1–20.

Obergfell, *Eva Inés*, Verträge über digitale Inhalte als Lizenzverträge, in: Verhandlungen des 71. Deutschen Juristentages, Band II/1, München 2017, K 53-K 72.

–, Big Data und Urheberrecht, in: Ahrens, Hans Jürgen, et al. (Hrsg.), Festschrift Büscher, Köln 2018, 223–232.

Obermeyer, *Ziad*, *et al.*, Dissecting racial bias in an algorithm used to manage the health of populations, 366 Science 2019, 447–453.

OECD, Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, Paris 2013.

Oechsler, *Jürgen*, Gerechtigkeit im modernen Austauschvertrag. Die theoretischen Grundlagen der Vertragsgerechtigkeit und ihr praktischer Einfluß auf Auslegung, Ergänzung und Inhaltskontrolle des Vertrages, Tübingen 1997.

Office of the Privacy Commissioner of Canada, The Internet of Things. An introduction to privacy issues with a focus on the retail and home environments, Research Paper, Gatineau 2016.

Oglaza, *Arnaud*, *et al.*, A recommender-based system for assisting non-technical users in managing android permissions, 11th International Conference on Availability, Reliability and Security (ARES) 2016, 1–9.

Ohly, *Ansgar*, „Volenti non fit iniuria" – Die Einwilligung im Privatrecht, Tübingen 2002.

–, Das neue Geschäftsgeheimnisgesetz im Überblick, GRUR 2019, 441–451.

–, UWG-Rechtsschutz bei Verstößen gegen die Datenschutz-Grundverordnung?, GRUR 2019, 686–693.

Ohm, *Paul*, Broken promises of privacy: Responding to the surprising failure of anonymization, 57 UCLA Law Review 2009, 1701–1777.

Omlor, *Sebastian*, BGH: Pflicht zur Aufklärung über Innenprovisionen, LMK 2014, 361191.

Omrani, *Tasnime/Rhouma*, *Rhouma/Sliman*, *Layth*. Lightweight Cryptography for Resource-Constrained Devices: A Comparative Study and Rectangle Cryptanalysis, in: Tobji, Mohamed Anis Bach, et al. (Hrsg.), International Conference on Digital Economy, Cham 2018, 107–118.

Ory, *Stephan/Sorge*, *Christoph*, Schöpfung durch Künstliche Intelligenz?, NJW 2019, 710–713.

Ory, *Stephan/Weth*, *Stephan*, Betroffenenrechte in der Justiz – Die DS-GVO auf Konfrontationskurs mit der ZPO?, NJW 2018, 2829–2834.

Ossowski, Sascha (Hrsg.). Agreement Technologies, Dordrecht 2013.

Ossowski, *Sascha/Sierra*, *Carles/Botti*, *Vicente*, Agreement technologies: a computing perspective, in: Ossowski, Sascha (Hrsg.), Agreement Technologies, Dordrecht 2013, 3–16.

Ostveen, *Manon*, Identifiability and the applicability of data protection to big data, 6 International Data Privacy Law 2016, 299–309.

Ott, *Stephan*, Das Internet vergisst nicht – Rechtsschutz für Suchobjekte?, MMR 2009, 158–163.

Paal, *Boris*, Schadensersatzansprüche bei Datenschutzverstößen, MMR 2020, 14–19.

Paal, *Boris/Pauly*, *Daniel A.* (Hrsg.), DS-GVO BDSG. Kommentar, 2. Aufl., München 2018.

Pagallo, *Ugo*, On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law, in: Gutwirth, Serge, et al. (Hrsg.), European Data Protection: In Good Health?, Dordrecht u. a. 2012, 331–346.

Pagallo, *Ugo/Durante*, *Massimo/Monteleone*, *Shara*, What Is New with the Internet of Things in Privacy and Data Protection? Four Legal Challenges on Sharing and Control in IoT, in: Leenes et al. (Hrsg.), Data Protection and Privacy: (In)visibilities and Infrastructures, 2017, 59–78.

Pałka, *Przemysław*, Terms of Service are Not Contracts, in: Grundmann, Stefan (Hrsg.), European Contract Law in the Digital Age, Cambridge, UK, u. a. 2018, 135–161.

–, Data Management Law for the 2020s: The Lost Origins and the New Needs, 68 Buffalo Law Review 2020 (im Erscheinen), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3435608.

Pałka, *Przemysław/Lippi*, *Marco*, Big Data Analytics, Online Terms of Service and Privacy Policies, in: Vogl, Roland (Hrsg.), Research Handbook on Big Data Law, im Erscheinen, https://ssrn.com/abstract=3347364.

Palzer, *Christoph*, Anmerkung zu BGH, Urteil v. 12. 3. 2013 – II ZR 179/12, JZ 2013, 691–692.

Pappachan, *Primal*, *et al.*, Towards privacy-aware smart buildings: Capturing, communicating, and enforcing privacy policies and preferences, IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW) 2017, 193–198.

Pardo, *Raúl/Le Métayer*, *Daniel*, Analysis of Privacy Policies to Enhance Informed Consent, Working Paper, 2019, https://arxiv.org/abs/1903.06068.

Patrick, *Andrew S./Kenny*, *Steve*, From privacy legislation to interface design: Implementing information privacy in human-computer interactions, in: Roger Dingledine (Hrsg.), Privacy Enhancing Technologies, Berlin und Heidelberg 2003, 107–124.

Patzak, *Andrea/Beyerlein*, *Thorsten*, Adressdatenhandel zu Telefonmarketingzwecken, MMR 2007, 687–691.

Paulus, *David*, Die automatisierte Willenserklärung, JuS 2019, 960–965.

Paulus, *David/Matzke*, *Robin*, Smart Contracts und das BGB – Viel Lärm um nichts? –, ZfPW 2018, 431–465.

Pauly, *Daniel/Ritzer*, *Christoph/Geppert*, *Nadine*: Gilt europäisches Datenschutzrecht auch für Niederlassungen ohne Datenverarbeitung? – Weitreichende Folgen für internationale Konzerne, ZD 2013, 423–426.

Peifer, *Karl-Nikolaus*, Das Recht auf Vergessenwerden – ein neuer Klassiker vom Karlsruher Schlossplatz, GRUR 2020, 34–37.

Peifer, *Karl-Nikolaus/Kamp*, *Johannes*, Datenschutz und Persönlichkeitsrecht, ZUM 2009, 185–190.

Penney, *Jon*, Internet surveillance, regulation, and chilling effects online: A comparative case study, 6(2) Internet Policy Review 2017, 1–39.

Peppet, *Scott R.*, Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future, 105 Northwestern University Law Review 2011, 1153–1203.

–, Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent, 93 Texas Law Review 2014, 85–178.

Pertot, *Tereza*, Die Auslegung des datenschutzrechtlichen Koppelungsverbots – Lockerung durch den Corte di Cassazione, GPR 2019, 54–57.

–, (Hrsg.), Rechte an Daten, Tübingen (im Erscheinen).

Petersen, *Jens*, Gesetzliches Verbot und Rechtsgeschäft, Jura 2003, 532–535.
Peterson, *George*, Car Owners Select Trump Over Other Candidates, Forbes (19.2.2016), https://www.forbes.com/sites/georgepeterson1/2016/02/19/car-owners-select-trump/
Petri, *Thomas*, Datenschutzrechtliche Verantwortlichkeit im Internet – Überblick und Bewertung der aktuellen Rechtsprechung, ZD 2015, 103–106.
–, Datenschutzrechtliche Verantwortlichkeit im Internet – Überblick und Bewertung der aktuellen Rechtsprechung, ZD 2015, 103–106.
–, Anmerkung zu Wirtschaftsakademie Schleswig-Holstein, EuZW 2018, 540–541.
Pew Research Center, Public Perceptions of Privacy and Security in the Post-Snowden Era, Washington, D.C. 2014.
Picard, *Rosalind W.*, Affective Computing, Cambridge, MA/London 1997.
Piepenbrock, *Andreas*, Der Urlaub, der Tod und die Methodik des Unionsprivatrechts. Zugleich Anmerkung zu EuGH, Urt. v. 6.11.2018 – C-569/16 und C-570/16, Bauer und Willmeroth, GPR 2019, 93–98.
Pieper, *Fritz-Ulli*, Wenn Maschinen Verträge schließen: Willenserklärungen beim Einsatz von Künstlicher Intelligenz, GRUR-Prax 2019, 298–300.
Piltz, *Carlo*, Die Datenschutz-Grundverordnung. Teil 1: Anwendungsbereich, Definitionen und Grundlagen der Datenverarbeitung, K&R 2016, 557–567.
–, Die Datenschutz-Grundverordnung. Teil 5: Internationale Zusammenarbeit, Rechtsbehelfe und Sanktionen, K&R 2017, 85–93.
–, Einbindung des Facebook-„Gefällt mir"-Buttons, ZD 2017, 336–338.
Pinnick, *Travis*, Privacy Short Notice Design, TrustArc Blog (17.2.2011), https://www.trustarc.com/blog/2011/02/17/privacy-short-notice-design/.
Piwek, *Lukasz/Joinson*, *Adam*, Automatic tracking of behavior with smartphones: Potential for behavior change interventions, in: Little, Linda, et al. (Hrsg.), Behavior Change Research and Theory, London u. a. 2017, 137–165.
Plath, *Kai-Uwe* (Hrsg.), DSGVO/BDSG. Kommentar zu DSGVO, BDSG und den Datenschutzbestimmungen des TMG und TKG, 3. Aufl., Köln 2018.
Poese, *Ingmar*, *et al.*, IP geolocation databases: Unreliable?. 41 ACM SIGCOMM Computer Communication Review 2011, 53–56.
Poland, *G.A./Ovsyannikova*, *I.G./Kennedy*, *Richard B.*, Personalized vaccinology: a review, 36 Vaccine 2018, 5350–5357.
Polania, *Rafael/Woodford*, *Michael/Ruff*, *Christian C.*, Efficient coding of subjective value, 22 Nature Neuroscience 2019, 134–142.
Policy and Research Group of the Office of the Privacy Commissioner of Canada, Consent and privacy – A discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act, Gatineau 2016.
Pollmann, *Maren/Kipker*, *Dennis-Kenji*, Informierte Einwilligung in der Online-Welt, DuD, 2016, 378–381.
Polzehl, *Tim*, Personality in Speech, Cham u. a. 2015.
Poole, *David L./Mackworth*, *Alan K.*, Artificial Intelligence. Foundations of Computational Agents. Cambridge, UK 2010.
Posner, *Richard A.*, Privacy, in: Peter Newman (Hrsg.), The New Palgrave Dictionary of Economics and the Law, Band 3, London 1998, 103–107.
Post, *Robert C.*, The Social Foundations of Privacy: Community and Self in the Common Law Tort, 77 California Law Review 1989, 957–1010.

Preis, *Ulrich*, Verbot der Altersdiskriminierung als Gemeinschaftsgrundrecht. Der Fall „Mangold" und die Folgen, NZA 2006, 401–410.

Privacy International, Buying a smart phone on the cheap? Privacy might be the price you have to pay, Privacy International (20.9.2019), https://privacyinternational.org/long-read/3226/buying-smart-phone-cheap-privacy-might-be-price-you-have-pay.

Prütting, *Jens*, Rechtsgebietsübergreifende Normenkollisionen, RW 9 (2018), 289–331.

–, Rechtsgebietsübergreifende Normenkollisionen, Tübingen 2020.

Purtova, *Nadezhda*, The law of everything. Broad concept of personal data and future of EU data protection law, 10 Law, Innovation and Technology 2018, 40–81.

Qian, *Jianwei*, *et al.*, Social network de-anonymization and privacy inference with knowledge graph model, 16 IEEE Transactions on Dependable and Secure Computing 2017, 679–692.

Qiu, *Lina/Wang*, *Yingying/Rubin*, *Julia*, Analyzing the Analyzers: FlowDroid/IccTA, AmanDroid, and DroidSafe, Proceedings of the 27th ACM SIGSOFT International Symposium on Software Testing and Analysis 2018, 176–186.

Quelle, *Claudia*, The ‚Risk Revolution' in EU Data Protection Law: We can't [sic] Have our Cake and Eat it, Too, in: Leenes, Ronald, et al. (Hrsg.), Data Protection and Privacy: The Age of Intelligent Machines, 33–62.

Rachels, *James*, God and Human Attitudes, 7 Religious Studies 1971, 325–337.

Raiser, *Ludwig*, in: von Caemmerer et al. (Hrsg.), Hundert Jahre deutsches Rechtsleben. Festschrift zum hundertjährigen Bestehen des deutschen Juristentages 1860–1960, Karlsruhe 1960, 101–134.

Ranjan, *Rajeev*, *et al.*, Deep learning for understanding faces: Machines may be just as good, or better, than humans, 35 IEEE Signal Processing Magazine 2018, 66–83.

Rannenberg, *Kai/Camenisch*, *Jan/Sabouri*, *Ahmad* (Hrsg.), Attribute-based Credentials for Trust, Cham u. a. 2015.

Rao, *Ashwini*, *et al.*, Expecting the unexpected: Understanding mismatched privacy expectations online, Twelfth Symposium on Usable Privacy and Security (SOUPS) 2016, 77–96.

Raschke, *Philip*, *et al.*, Designing a GDPR-Compliant and Usable Privacy Dashboard, Proceedings of the IFIP International Summer School on Privacy and Identity Management 2017, 221–236.

Rasmus, *Antti*, *et al.*, Semi-supervised learning with ladder networks, Advances in Neural Information Processing Systems 2015, 3546–3554.

Raue, *Benjamin*, Meinungsfreiheit in sozialen Netzwerken, JZ 2018, 961–970.

–, Rechtssicherheit für datengestützte Forschung, ZUM 2019, 684–693.

Rauer, *Nils/Ettig*, *Diana*, Aktuelle Entwicklungen zum rechtskonformen Einsatz von Cookies – Die Rechtslage auf dem Prüfstand von Kommission und Gerichten, ZD 2016, 423–427.

Rawls, *John*, Political Liberalism, New York 1993.

–, A Theory of Justice, rev. Aufl., Cambridge, MA 1999.

Raz, *Joseph*, The Morality of Freedom, Oxford and New York 1986.

Rebhahn, *Robert*, Europäisches Arbeitsrecht, in: Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 2015, 395–424.

Reed, *Stephen K.*, Cognition. Theory and Applications, 7. Aufl., Belmont 2006.

Regan, *Priscilla*, Legislating Privacy: Technology, Social Values, and Public Policy, Chapel Hill/London 1995.

Reidenberg, *Joel R.*, *et al.*, Trustworthy Privacy Indicators: Grades, Labels, Certifications, and Dashboards, 96 Washington University Law Review 2019, 1409–1460.
Reidenberg, *Joel R.*, Privacy in Public, 69 University of Miami Law Review 2014, 141–160.
Reifert, *Natascha*, Codes of Conduct nach der DS-GVO, ZD 2019, 305–310.
Reiners, *Wilfried*, Datenschutz in der Personal Data Economy – Eine Chance für Europa, ZD 2015, 51–55.
Reinhardt, *Rudolf*, Die Vereinigung subjektiver und objektiver Gestaltungskräfte im Vertrage, in: Rechts- und Staatswissenschaftliche Fakultät der Rheinischen Friedrich-Wilhelms-Universität Bonn (Hrsg.), Festschrift zum 70. Geburtstag von Walter Schmidt-Rimpler, Karlsruhe 1957, 115–138.
Reiserer, *Kerstin/Christ*, *Florian/Heinz*, *Katharina*: Beschäftigten-Datenschutz und EU-Datenschutz-Grundverordnung, DStR 2018, 1501–1508.
Remien, *Oliver*, AGB-Gesetz und Richtlinie über mißbräuchliche Verbraucherverträgsklauseln in ihrem europäischen Umfeld, ZEuP 1994, 34–66.
Renner, *Moritz*, Bankkonzernrecht, Tübingen 2019.
Renz, *Hartmut T./Frankenberger*, *Melanie*, Compliance und Datenschutz – Ein Vergleich der Funktionen unter Berücksichtigung eines risikobasierten Ansatzes, ZD 2015, 158–161.
Repgen, *Tilman*, Abschied von der Willensbetätigung: Die Rechtsnatur der Vertragsannahme nach § 151, AcP 200 (2000), 533–564.
Reuters, Facebook stymies Admiral's plans to use social media data to price insurance premiums (2.11.2016), https://www.reuters.com/article/us-insurance-admiral-facebook/facebook-stymies-admirals-plans-to-use-social-media-data-to-price-insurance-premiums-idUSKBN12X1WP.
–, Amazon ditched AI recruiting tool that favored men for technical jobs, The Guardian (11.10.2018), https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine.
Reyes, *Irwin*, *et al.*, „Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale, Proceedings on Privacy Enhancing Technologies 2018 (3), 63–83.
Rhahla, *Mouna*, *et al.*, A GDPR Controller for IoT Systems: Application to e-Health, IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE) 2019, 170–173.r
Rhoen, *Michiel*, Beyond Consent: Improving Data Protection through Consumer Protection Law, 5(1) Internet Policy Review 2016, 1–15.
Ribeiro, *Marco Tulio/Singh*, *Sameer/Guestrin*, *Carlos*, Why should I trust you? Explaining the predictions of any classifier, Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining 2016, 1135–1144.
Rich, *Elaine/Knight*, *Kevin/Nair*, *Shivashankar B.*, Artificial Intelligence, 3. Aufl., New York u. a. 2009.
Richards, *Neil M./Hartzog*, *Woodrow*, The Pathologies of Digital Consent, 96 Washington University Law Review 2019, 1461–1504.
Richter, *Heiko*, Anmerkung zu Breyer, EuZW 2016, 912–914.
Riechert, *Anne*, Dateneigentum – ein unauflösbarer Interessenkonflikt?, DuD 2019, 353–360.
Riesenhuber, *Karl*, System und Prinzipien des Europäischen Vertragsrechts, Berlin 2003.

–, Die Einwilligung des Arbeitnehmers im Datenschutzrecht, RdA 2011, 257–265.
–, EU-Vertragsrecht, Berlin 2013.
–, Die Auslegung, in: Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 3. Aufl., Berlin 2015, 199–224.
–, Privatautonomie – Rechtsprinzip oder „mystifizierendes Leuchtfeuer", ZfPW 2018, 352–368.
–, Neue Methode und Dogmatik eines Rechts der Digitalisierung?, AcP 219 (2019), 892–923.
Ritter, *Franziska/Schwichtenberg*, *Simon*, Die Reform des UKlaG zur Eliminierung des datenschutzrechtlichen Vollzugsdefizits – neuer Weg, neue Chancen?, VuR 2016, 95–102.
Rittner, *Fritz*, Über das Verhältnis von Vertrag und Wettbewerb, AcP 188 (1988), 101–139.
Rivest, *Ronald L./Shamir*, *Adi/Adleman*, *Leonard*, A method for obtaining digital signatures and public-key cryptosystems, 21 Communications of the ACM 1978, 120–126.
Roberts, *Ian D./Hutcherson*, *Cendri A.*, Affect and Decision Making: Insights and Predictions from Computational Models, 23 Trends in Cognitive Sciences 2019, 602–614.
Robrahn, *Rasmus/Bremert*, *Benjamin*, Interessenskonflikte im Datenschutzrecht, ZD 2018, 291–297.
Rocher, *Luc/Hendrickx*, *Julien M./de Montjoye*, *Yves-Alexandre*, Estimating the success of re-identifications in incomplete datasets using generative models, 10 Nature Communications 2019, Article 3069, 1–9.
Roessler, *Beate/Mokrosinska*, *Dorota* (Hrsg.), Social Dimensions of Privacy: Interdisciplinary Perspectives, Cambridge, UK 2015.
Rogosch, *Patricia Maria*, Die Einwilligung im Datenschutzrecht, Baden-Baden 2013.
Rolnick, *David/Tegmark*, *Max*, The power of deeper networks for expressing natural functions, Working Paper, 2017, https://arxiv.org/abs/1705.05502.
Romei, *Andrea/Ruggieri*, *Salvatore*, A multidisciplinary survey on discrimination analysis, 29 The Knowledge Engineering Review 2014, 582–638.
Rosner, *Gilad/Kenneally*, *Erin*, Clearly Opaque. Privacy Risks of the Internet of Things, Bericht, 2018.
Rosni, *K.V.*, *et al.*, Consent Recommender System: A Case Study on LinkedIn Settings, Proceedings of the PAL: Privacy-Enhancing Artificial Intelligence and Language Technologies 2019, 53–60.
Rosoff, *Matt*, IBM and Salesforce Shake Hands on Artificial Intelligence, CNBC (6.3.2017), https://www.cnbc.com/2017/03/06/ibm-and-salesforce-shake-hands-on-artificial-intelligence.html.
Van Rossum, *Henk*, *et al.*, Privacy-Enhancing Technologies: The Path to Anonymity, Rijswijk u. a. 1995.
Roßnagel, *Alexander*, Anmerkung zu *Lindqvist*, MMR 2004, 95–100.
–, EuGH: Personenbezogene Daten im Internet. Anmerkung, MMR 2004, 95–100.
–, Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung, MMR 2005, 71–75.
–, Big Data – Small Privacy? – Konzeptionelle Herausforderungen für das Datenschutzrecht, ZD 2013, 562–567.
–, Fahrzeugdaten – wer darf über sie entscheiden?, SVR 2014, 281–287.
–, Wie zukunftsfähig ist die Datenschutz-Grundverordnung?, DuD 2016, 561–565.

–, Zukunftsfähigkeit der Datenschutz-Grundverordnung, DuD 2016, 553–554.
–, Datenschutzgesetzgebung für öffentliche Interessen und den Beschäftigungskontext, DuD 2017, 290–294.
–, Datenschutzgrundsätze – unverbindliches Programm oder verbindliches Recht?, ZD 2018, 339–344.
–, Pseudonymisierung personenbezogener Daten, ZD 2018, 243–247.
–, Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht, NJW 2019, 1–5.
Roßnagel, *Alexander*, *et al.*, Datensparsamkeit oder Datenreichtum? Zur neuen politischen Diskussion über den datenschutzrechtlichen Grundsatz der Datensparsamkeit, Policy Paper des Forums „Privatheit und selbstbestimmtes Leben in der digitalen Welt", 2017.
Roßnagel, *Alexander/Pfitzmann*, *Andreas/Garstka*, *Hansjürgen*, Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001.
Roßnagel, *Alexander/Richter*, *Maxi/Nebel*, *Philipp*, Besserer Internetdatenschutz für Europa – Vorschläge zur Spezifizierung der DS-GVO, ZD 2013, 103–108.
Roßnagel, *Alexander/Schnabel*, *Christoph*, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, 3534–3538.
Roth, *Herbert*, Die Einrede des bürgerlichen Rechts, München 1988.
–, Geltungserhaltende Reduktion im Privatrecht, JZ 1989, 411–419.
–, Verzinsungspflichten bei wucherischen und wucherähnlichen Darlehensverträgen, ZHR 153 (1989), 423–445.
Roth, *Wulf-Henning/Jopen*, *Christian*, Die richtlinienkonforme Auslegung, in: Riesenhuber, Karl (Hrsg.), Europäische Methodenlehre, 3. Aufl., Berlin 2015, 263–296.
Rothmann, *Robert/Buchner*, *Benedikt*, Der typische Facebook-Nutzer zwischen Recht und Realität, DuD 2018, 342–346.
Röthel, *Anne*, Normkonkretisierung im Privatrecht, Tübingen 2004.
–, Privatautonomie im Spiegel der Privatrechtsentwicklung: ein mystifizierendes Leuchtfeuer, in: Bumke, Christian/Röthel, Anne (Hrsg.), Autonomie im Recht, Tübingen 2017, 91–115.
Rother, *Werner*, Sittenwidriges Rechtsgeschäft und sexuelle Liberalisierung, AcP 172 (1972), 498–519.
Rott, *Peter*, Unfair Contract Terms, in: Twigg-Flesner, Christian (Hrsg.), Research Handbook on EU Consumer and Contract Law, Cheltenham 2016, 287–313.
Royal Society, Protecting privacy in practice: The current use, development and limits of Privacy Enhancing Technologies in data analysis, Report, 2019.
Rubinstein, *Daniel L./Gal*, *Michal S.*, Access Barriers to Big Data, 59 Arizona Law Review 2017, 339–381.
Rubinstein, *Ira S.*, Regulating Privacy by Design, 26 Berkeley Technology Law Journal 2011, 1409–1456.
Rubinstein, *Ira/Petkova*, *Bilyana*, The International Impact of the General Data Protection Regulation, in: Cole, Marc/Boehm, Franziska (Hrsg.), Commentary on the General Data Protection Regulation, Cheltenham, im Erscheinen, https://ssrn.com/abstract=3167389.
Rudin, *Cynthia*, Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead,1 Nature Machine Intelligence, 2019, 206–215.

Rudkowski, *Lena*, Vertragsrechtliche Anforderungen an die Gestaltung von „Self-Tracking"-Tarifen in der Privatversicherung, ZVersWiss 106 (2017), 453–502.
Ruhenstroth, *Miriam*, Smartphone-Nutzer sollten jetzt ihre Werbe-ID ändern, Mobilsicher (24.5.2018), https://mobilsicher.de/hintergrund/smartphone-nutzer-sollten-jetzt-ihre-werbe-id-aendern#WerbeID3.
Rumelhart, *David E./Hinton*, *Geoffrey E./Williams*, *Ronald J.*, Learning representations by back-propagating errors, 323 Nature 1986, 533–536.
Russell, *Stuart J./Norvig*, *Peter*, Artificial Intelligence. A Modern Approach, 3. Aufl., Upper Saddle River u. a. 2010.
Ryte Wiki, Facebook Fanpage, https://de.ryte.com/wiki/Facebook_Fanpage.
–, Third Party Cookies, https://de.ryte.com/wiki/Third_Party_Cookies.
–, Tracking Pixel, https://de.ryte.com/wiki/Tracking_Pixel.
Sachverständigenrat für Verbraucherfragen, Verbraucherrecht 2.0, Berlin 2016.
–, Verbrauchergerechtes Scoring, Berlin 2018.
Sack, *Rolf*, Sittenwidrigkeit, Sozialwidrigkeit und Interessenabwägung, GRUR 1970, 493–503.
–, Das Anstandsgefühl aller billig und gerecht Denkenden und die Moral als Bestimmungsfaktoren der guten Sitten, NJW 1985, 761–769.
Sackmann, *Florian*, Die Beschränkung datenschutzrechtlicher Schadensersatzhaftung in Allgemeinen Geschäftsbedingungen, ZIP 2017, 2450–2454.
Sadeh, *Norman M./Chan*, *Enoch/Van*, *Linh*, MyCampus: an agent-based environment for context-aware mobile services, Proceedings of UBIAGENTS 2002, 34–39.
Sadeh, *Norman*, *et al.*, The Usable Privacy Policy Project. Combining Crowdsourcing, Machine Learning and Natural Language Processing to Semi-Automatically Answer Those Privacy Questions Users Care About, Technical Report, CMU-ISR-13–119, Pittsburgh 2013.
SAE International, Standard J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, Warrendale 2014.
Sagan, *Adam*, Arbeitsrecht: Unterschiedliche Behandlung von Bewerbern wegen ihrer Konfession im Stellenbesetzungsverfahren eines kirchlichen Arbeitgebers, EuZW 2018, 381–387.
Samara-Krispis, *Anastasia/Steindorff*, *Ernst*, Joined Cases C-19/90 and 20/90, M. Karella and N. Karellas v. Ypourgos viomichanias, energias kai technologias, Organismos Anasygkrotiseos Epicheiriseon AE, Preliminary ruling of 30 January 1991, requested by the Greek Council of State on the interpretation of Articles 25, 41 and 42 of the Second Directive on company law, not yet reported, 29 Common Market Law Review 1992, 615–624.
Samuelson, *Paul A./Nordhaus*, *William D.*, Economics. 19. Aufl., Boston u. a. 2009.
Samuelson, *William/Zeckhauser*, *Richard*, Status quo bias in decision making, 1 Journal of Risk and Uncertainty 1988, 7–59.
Sandrock, *Otto*, Subjektive und objektive Gestaltungskräfte bei der Teilnichtigkeit von Rechtsgeschäften: Ein Beitrag zur Auslegung von § 139 BGB, AcP 159 (1960), 481–546.
Santos, *José-Antonio*, *et al.*, Legal and ethical implications of applications based on agreement technologies: the case of auction-based road intersections, Artificial Intelligence and Law 2019, https://doi.org/10.1007/s10506-019-09259-8, 1–30.
Sartor, *Giovanni*, Contracts in the Infosphere, in: Grundmann, Stefan (Hrsg.), European Contract Law in the Digital Age, Cambridge, UK 2018, 263–278.

Sattler, *Andreas*, Personenbezogene Daten als Leistungsgegenstand, JZ 2017, 1036–1046.
–, Personenbezogene Daten als Leistungsgegenstand, in: Martin Schmidt-Kessel/Anna Grimm (Hrsg.), Telematiktarife & Co. – Versichertendaten als Prämienersatz, 2018, 1–46.
–, Rezension: Carmen Langhanke, Daten als Leistung, JZ 2018, 760–770.
–, Gemeinsame Verantwortlichkeit – getrennte Pflichten, GRUR 2019, 1023–1026.
–, Privatautonomie oder Determinismus – Welchen Weg geht das Datenschuldrecht?, in: Ochs, Carsten, et al. (Hrsg.), Die Zukunft der Datenökonomie, Cham 2019, 1–30.
Satyanarayanan, *Mahadev*, Privacy: The achilles heel of pervasive computing?, IEEE Pervasive Computing 2003, 2–3.
–, The Emergence of Edge Computing, 50 Computer 2017, 30–39.
Savage, *Scott J./Waldman*, *Donald M.*, The Value of Online Privacy: Evidence from Smartphone Applications, Technical Report, Boulder 2014.
von Savigny, *Friedrich Carl*, System des heutigen Römischen Rechts, Band III, Berlin 1840.
Scanlon, *Thomas*, A Theory of Freedom of Expression, 1 Philosophy and Public Affairs 1972, 204–226.
Schaack, *Roger*, Zu den Prinzipien der Privatautonomie im deutschen und französischen Rechtsanwendungsrecht, Berlin 1990.
Schäfer, *Frank*, Schwerpunktbereichshausarbeit – Europäische Privatrechtrechtsgeschichte: Austauschgerechtigkeit in Preistaxen, laesio enormis und § 138 BGB, JuS 2009, 237–242.
Schäfer, *Hans-Bernd/Ott*, *Claus*, Lehrbuch der ökonomischen Analyse des Zivilrechts, 5. Aufl., Berlin/Heidelberg 2012.
Schantz, *Peter*, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841–1847.
Schantz, *Peter/Wolff*, *Heinrich Amadeus*, Das neue Datenschutzrecht, München 2017.
Schaper, *Alexander/Teubert*, *Diana*, Smart Home – große Erwartungen. Teil1: Ab wann wird das Haus smart?, ZfV 2016, 613–615.
Schatsky, *David/Kumar*, *Navya/Bumb*, *Sourabh*, Intelligent IoT. Bringing the power of AI to the Internet of Things, Deloitte Insights, New York u. a. 2017.
Schaub, *Florian/Balabako*, *Rebecca/Durity*, *Adam/Cranor*, *Lorrie Faith*, A Design Space for Effective Privacy Notices, Proceedings of the Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), 2015, 1–17.
Scheffer, *Urban*, Schweigen auf Angebot als stillschweigende Annahme?, NJW 1995, 3166–3168.
Schemmel, *Frank*, Anmerkung zu OLG Frankfurt a. M.: Unwirksamkeit des Verkaufs von Adressdaten wegen fehlender Einwilligung der Adressinhaber, BB 2018, 723.
Schendera, *Christian F.*, Die Verständlichkeit von Rechtstexten: eine kritische Darstellung der Forschungslage, in: Lerch, Kent D. (Hrsg.), Die Sprache des Rechts, Bd. 1: Recht verstehen, Berlin 2004, 321–374.
Scheurle, *Klaus-Dieter/Mayen*, *Thomas* (Hrsg.), TKG, 3. Aufl., München 2018.
Schirmer, *Jan-Erik*, Rechtsfähige Roboter?, JZ 2016, 660–666.
Schlechtriem, *Peter*, Vertragsordnung und außervertragliche Haftung, Frankfurt am Main 1972.
Schleipfer, *Stefan*, Facebook-Like-Buttons, DuD 2014, 318–324.
–, Datenschutzkonformes Webtracking nach Wegfall des TMG, ZD 2017, 460–466.

Schmid, *Christoph*, Die gemeinschaftsrechtliche Überlagerung der Tatbestände des Mißbrauchs der Vertretungsmacht und des Insichgeschäfts, AG 1998, 127.
Schmidt, *Eike*, Von der Privat- zur Sozialautonomie, JZ 1980, 153–161.
Schmidt, *Hubert*, Einbeziehung von AGB im Verbraucherverkehr, NJW 2011, 1633–1639.
Schmidt, *Reimer*, Rationalisierung und Privatrecht, AcP 166 (1966), 1–29.
Schmidt-Kessel, *Martin*, Rechtsmißbrauch im Gemeinschaftsrecht, Jahrbuch junger Zivilrechtswissenschaftler 2000, 61–83.
Schmidt-Kessel, *Martin/Grimm*, *Anna*, Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten, ZfPW 2017, 84–108.
– (Hrsg.), Telematiktarife & Co. – Versichertendaten als Prämienersatz, Karlsruhe 2018.
Schmidt-Kessel, *Martin/Erler*, *Katharina/Grimm*, *Anna/Kramme*, *Malte*, Die Richtlinienvorschläge der Kommission zu Digitalen Inhalten und Online-Handel – Teil 2, GPR 2016, 54–71.
Schmidt-Rimpler, *Walter*, Grundfragen einer Erneuerung des Vertragsrechts, AcP 147 (1941) 130–197.
–, Zum Vertragsproblem, in: Festschrift für Ludwig Raiser, Tübingen 1974, 3–26.
Schmidt-Salzer, *Joachim*, Transformation der EG-Richtlinie über mißbräuchliche Klauseln in Verbraucherverträgen in deutsches Recht und AGB-Gesetz, BB 1995, 733–740.
Schmolke, *Klaus Ulrich*, Grenzen der Selbstbindung im Privatrecht. Rechtspaternalismus und Verhaltensökonomik im Familien-, Gesellschafts- und Verbraucherrecht, Tübingen 2014.
Schnabel, *Christoph/Freund*, *Bernhard*, „Ach wie gut, dass niemand weiß …" – Selbstdatenschutz bei der Nutzung von Telemedienangeboten, CR 2010, 718–721.
Schneewind, *Jerome B.*, The Invention of Autonomy. A History of Modern Moral Philosophy, Cambridge, UK 1998.
Schneider, *Jens-Peter*, Stand und Perspektiven des Europäischen Datenverkehrs- und Datenschutzrechts, DV 44 (2011), 499–524.
Schneider, *Jochen*, Schließt Art. 9 DS-GVO die Zulässigkeit der Verarbeitung bei Big Data aus?, ZD 2017, 303–308.
–, Datenschutz nach der EU-Datenschutz-Grundverordnung, 2. Aufl., München 2019.
Schreiber, *Christoph*, Nichtigkeit und Gestaltungsrechte, AcP 211 (2011), 35–57.
Schröder, *Markus*, Der risikobasierte Ansatz in der DS-GVO, ZD 2019, 503–506.
Schröder, *Michael/Taeger*, *Jürgen* (Hrsg.), Scoring im Fokus: Ökonomische Bedeutung und rechtliche Rahmenbedingungen im internationalen Vergleich, Neuss 2014.
Schroeder, *Werner*, Nationale Maßnahmen zur Durchführung von EG-Recht und das Gebot der einheitlichen Wirkung, AöR 129 (2004), 3–38.
Schulte-Nölke, *Hans/Twigg-Flesner*, *Christian/Ebers*, *Martin*, EC Consumer Law Compendium: The Consumer Acquis and its transposition in the Member States, München 2008.
Schulz, *Sönke*, Anmerkung zu Wirtschaftsakademie Schleswig-Holstein, ZD 2018, 363–365.
Schulze, *Reiner*, Die Digitale-Inhalte-Richtlinie – Innovation und Kontinuität im europäischen Vertragsrecht, ZEuP 2019, 695–721.
Schumacher, *Ulrich*, Materielle Neuregelungen im Recht der Allgemeinen Geschäftsbedingungen, MDR 2002, 973–980.

Schumann, *Daniel*, Pay As You Drive. Die rechtliche Zulässigkeit von Telematik-Tarifen im Privatkundensegment der Kraftfahrzeug-Haftpflichtversicherung, VVW, Karlsruhe 2017.

Schwarcz, *Daniel*, Transparently Opaque: Understanding the Lack of Transparency in Insurance Consumer Protection, 61 UCLA Law Review 2014, 394–462.

Schwartz, *Alan/Wilde*, *Louis L.*, Intervening in Markets on the Basis of Imperfect Information: A Legal and Economic Analysis, 127 University of Pennsylvania Law Review 1979, 630–682.

Schwartz, *Paul M.*, Privacy and Democracy in Cyberspace, 52 Vanderbilt Law Review 1999, 1609–1702.

–, Property, Privacy, and Personal Data, 117 Harvard Law Review 2004, 2055–2128.

–, Global Data Privacy: The EU Way, 94 NYU Law Review 2019, 771–818.

Schwartz, *Paul M./Solove*, *Daniel J*, The PII problem: Privacy and a new concept of personally identifiable information, 86 NYU Law Review, 2011, 1814–1894.

Schwarz, *Norbert/Vaughn*, *Leigh Ann*, The availability heuristic revisited: Ease of recall and content of recall as distinct sources of information, in: Gilovich, Thomas, et al. (Hrsg.), Heuristics and Biases: The Psychology of Intuitive Judgment, Cambridge, UK 2002, 103–119.

Schwarze, *Roland*, Subsidiarität des vertraglichen Drittschutzes?, AcP 203 (2003), 348–365.

Schweitzer, *Heike*, Neue Machtlagen in der digitalen Welt? Das Beispiel unentgeltlicher Leistungen, in: Körber, Torsten/Kühling, Jürgen (Hrsg.), Regulierung-Wettbewerb-Innovation, Baden-Baden 2017, 269–305.

–, Datenzugang in der Datenökonomie: Eckpfeiler einer neuen Informationsordnung, GRUR 2019, 569–580.

Schweitzer, *Heike/Fetzer*, *Thomas/Peitz*, *Martin*, Digitale Plattformen: Bausteine für einen künftigen Ordnungsrahmen, ZEW Discussion Paper No. 16–042, 2016, ftp.zew.de/pub/zew-docs/dp/dpl6042.pdf.

Schweitzer, *Heike/Peitz*, *Martin*, Datenmärkte in der digitalisierten Wirtschaft: Funktionsdefizite und Regelungsbedarf, ZEW Discussion Paper No. 17–043, 2017, http://ftp.zew.de/pub/zew-docs/dp/dp17043.pdf.

Schweitzer, *Heike*, *et al.*, Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, Gutachten für das Bundesministerium für Wirtschaft und Energie, 2018.

Schwenke, *Matthias Christoph*, Individualisierung und Datenschutz, Wiesbaden 2006.

Schwintowski, *Hans-Peter*, Preistransparenz als Voraussetzung funktionsfähigen (digitalen) Marktwettbewerbs, NJOZ 2018, 841–850.

Scudiero, *Lucio/Ziegler*, *Sébastian*, Towards Trustable Internet of Things Certification, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 129–142.

Sein, *Karin/Spindler*, *Gerald*, The new Directive on Contracts for the Supply of Digital Content and Digital Services – Scope of Application and Trader's Obligation to Supply – Part 1, 15 European Review of Contract Law 2019, 257–279.

–, The new Directive on Contracts for the Supply of Digital Content and Digital Services – Conformity Criteria, Remedies and Modifications – Part 2, 15 European Review of Contract Law 2019, 365–391.

Seitz, *Ludwig/Selander*, *Göran/Gehrmann*, *Christian*, Authorization framework for the internet-of-things, IEEE 14th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013, 1–6.

Selbst, *Andrew D.*, Disparate impact in big data policing, 52 Georgia Law Review 2017, 109–195.

Selbst, *Andrew D./Barocas*, *Solon*, The intuitive appeal of explainable machines, 87 Fordham Law Review 2018, 1085–1139.

Sen, *Amartya K.*, Markets and Freedoms: Achievements and Limitations of the Market Mechanism in Promoting Individual Freedoms, 45 Oxford Economic Papers 1993, 519–541.

Senden, *Linda*, Soft Law, Self-Regulation and Co-Regulation in European Law: Where Do They Meet?, 9(1) Electronic Journal of Comparative Law 2005, 1–27.

Sester, *Peter/Nitschke*, *Tanja*, Software-Agent mit Lizenz zum …?, CR 2004, 548–554.

Shadmy, *Tomer*, The New Social Contract: Facebook's Community and Our Rights, 37 Boston University International Law Journal 2019, 307–354.

Shalev-Shwartz, *Shai/Ben-David*, *Shai*, Understanding Machine Learning, New York 2014.

Sharot, *Tali*, The Optimism Bias, 21 Current Biology 2011, R941-R945.

Shi, *Weisong/Cao*, *Jie/Zhang*, *Quan/Li*, *Youhuizi/Xu*, *Lanyu*, Edge Computing: Vision and Challenges, 3 IEEE Internet of Things Journal 2016, 637–646.

Shieber, *Stuart M.* (Hrsg.), The Turing Test, Cambridge, MA 2004.

Shojafar, *Mohammad/Sookhak*, *Mehdi*, Internet of everything, networks, applications, and computing systems (IoENACS), International Journal of Computers and Applications 2019, DOI: 10.1080/1206212X.2019.1575621, 1–3.

Shu, *Kai*, et al, User identity linkage across online social networks: A review, 18 ACM SIGKDD Explorations Newsletter 2017, 5–17.

Shui, *Haiyan/Ausubel*, *Lawrence M.*, Time inconsistency in the credit card market, 14th Annual Utah Winter Finance Conference, 2004, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=586622.

Shy, *Oz*, A short survey of network economics, 38 Review of Industrial Organization 2011, 119–149.

Siemen, *Birte*, Grundrechtsschutz durch Richtlinien/Die Fälle Österreichischer Rundfunk u. a. und Lindqvist – Anmerkungen zu den Urteilen des Europäischen Gerichtshofes in den verbundenen Rechtssachen C-465/00, C-138/01 und C-139/01 und C-101/01, EuR 2004, 306–321.

Silver, *David*, *et al.*, Mastering the game of Go with deep neural networks and tree search, 529 Nature 2016, 484–492.

Simitis, *Spiros*, Datenschutz: Von der legislativen Entscheidung zur richterlichen Interpretation, NJW 1981, 1697–1701.

–, Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 398–405.

–, Reviewing Privacy in an Information Society, 135 University of Pennsylvania Law Review 1989, 707–772.

– (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden 2011.

Simitis, *Spiros/Hornung*, *Gerrit/Spiecker gen. Döhmann*, *Indra* (Hrsg.), Datenschutzrecht, Baden-Baden 2019.

Singer, *Reinhard*, Selbstbestimmung und Verkehrsschutz im Recht der Willenserklärungen, München 1995.

Sittard, *Ulrich/Esser*, *Ilka*, Das Ende der Vertrauensarbeitszeit? Das EuGH-Urteil zur Arbeitszeiterfassung, jm 2019, 284–290.

Soergel, Kommentar zum Bürgerlichen Gesetzbuch, neu hrsg. v. Siebert, Wolfgang, et al., 13. Aufl., Berlin u. a. 1999 (zit.: *Bearbeiter*, in: Soergel, BGB).

Soghoian, *Chris*, End the Charade: Regulators Must Protect Users' Privacy by Default, Paper for the Office of the Privacy Commissioner of Canada, Gatineau 2010.
Solmecke, *Christian/Vondrlik*, *Simon-Elias*, Rechtliche Probleme bei Produkten mit serverbasierten Zusatzdiensten – Was passiert, „wenn der Kühlschrank keine Einkaufsliste mehr schreibt …", MMR 2013, 755–760.
Solomon, *Michael R.*, *et al.*, Consumer Behaviour: A European Perspective, Harlow u. a. 2013.
Solove, *Daniel J.*, I've Got Nothing to Hide and Other Misunderstandings of Privacy, 44 San Diego Law Review 2007, 745–772.
–, Understanding Privacy, Cambridge, MA 2008.
–, Introduction: Privacy self-management and the consent dilemma, 126 Harvard Law Review 2013, 1880–1903.
Soltani, *Ashkan*, *et al.*, Flash Cookies and Privacy, 2010 AAAI Spring Symposium Series, 158–163.
Sørensen, *Jannick Kirk*, *Van den Bulck*, *Hilde/Kosta*, *Sokol*, Privacy Policies Caught Between the Legal and the Ethical: European Media and Third Party Trackers Before and After GDPR, Working Paper, 2019, https://ssrn.com/abstract=3427207.
Sorescu, *Alina*, Data-Driven Business Model Innovation, 34 Journal of Product Innovation Management 2017, 691–696.
Sorge, *Christoph*, Softwareagenten, Karlsruhe 2006.
Sosnitza, *Olaf*, Das Internet der Dinge – Herausforderung oder gewohntes Terrain für das Zivilrecht? CR 2016, 764–772.
Specht, *Louisa*, Konsequenzen der Ökonomisierung informationeller Selbstbestimmung, Köln 2012.
–, Das Verhältnis möglicher Datenrechte zum Datenschutzrecht, GRUR Int. 2017, 1040–1047.
–, Daten als Gegenleistung – Verlangt die Digitalisierung nach einem neuen Vertragstypus?, JZ 2017, 763–770.
–, Diktat der Technik. Regulierungskonzepte technischer Vertragsinhaltsgestaltung am Beispiel von Bürgerlichem Recht und Urheberrecht, Baden-Baden 2019.
Specht, *Louisa/Herold*, *Sophie*, Roboter als Vertragspartner?, MMR 2018, 40–44.
Specht-Riemenschneider, *Louisa*, Herstellerhaftung für nicht-datenschutzkonform nutzbare Produkte – Und er haftet doch!, MMR 2020, 73–78.
Specht-Riemenschneider, *Louisa/Schneider*, *Ruben*, Die gemeinsame Verantwortlichkeit im Datenschutzrecht, MMR 2019, 503–509.
Spindler, *Gerald*, Datenschutz- und Persönlichkeitsrechte im Internet – der Rahmen für Forschungsaufgaben und Reformbedarf, GRUR 2013, 996–1003.
–, Selbstregulierung und Zertifizierungsverfahren nach der DS-GVO, ZD 2016, 407–414.
–, Text und Data Mining – urheber- und datenschutzrechtliche Fragen, GRUR 2016, 1112–1120.
Spindler, *Gerald/Schmitz*, *Peter/Liesching*, *Marc* (Hrsg.), TMG, 2. Aufl., München 2018.
Spindler, *Gerald/Schuster*, *Fabian*, Recht der elektronischen Medien, 4. Aufl., München 2019.
Spindler, *Gerald/Sein*, *Karin*, Die endgültige Richtlinie über Verträge über digitale Inhalte und Dienstleistungen, MMR 2019, 415–420.
–, Die Richtlinie über Verträge über digitale Inhalte, MMR 2019, 488–493.
Spiro, *Karl*, Die Haftung für Erfüllungsgehilfen, Bern 1984.

Spittka, *Jan*, GRUR-Prax 2020, 139.
Spoerr, *Wolfgang/Schlösser*, *Tim*, Sanktionswidrig erteilte Gutschriften im bargeldlosen Zahlungsverkehr: Zivilrechtliche Folgen öffentlich-rechtlicher Vorgaben des Außenwirtschaftsrechts, WM 2016, 1232–1333.
Sriram, *Ram*, Smart Networked Systems and Societies: A Research Agenda, 17(3) IT Professional 2015, 60–62.
Stadler, *Astrid*, Bürgschaftserklärung am Arbeitsplatz, JA 2007, 896–898.
–, Schwarzarbeit ist kein Kavaliersdelikt, JA 2014, 623–625.
Staiano, *Jacopo*, *et al.*, Money walks: a human-centric study on the economics of personal mobile data, Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing 2014, 583–594.
Stamm, *Jürgen*, Die Auflösung der Drittschadensliquidation im Wege der Gesamtschuld, AcP 217 (2017), 165–204.
Stanovich, *Keith E./West*, *Richard F.*, Individual differences in reasoning: Implications for the rationality debate?, 23 Behavioral and Brain Sciences, 2000, 645–665.
Stanovich, *Keith E./West*, *Richard F./Toplak*, *Maggie E.*, The Rationality Quotient: Toward a Test of Rational Thinking, Boston 2016.
Starke, *Max*, EU-Grundrechte und Vertragsrecht, Tübingen 2016.
Staub, *HGB*, hrsg. v. Canaris, Claus-Wilhelm/Habersack, Mathias/Schäfer, Carsten, Band 10/1, Bankvertragsrecht, 1. Teil, 5. Aufl., Berlin 2016 (zit.: *Bearbeiter*, in: Staub, HGB, Band 10/1, Bankvertragsrecht, 1. Teil).
Staudenmayer, *Dirk*, Auf dem Weg zum digitalen Privatrecht – Verträge über digitale Inhalte, NJW 2019, 2497–2501.
Steege, *Hans*, Ist die DS-GVO zeitgemäß für das autonome Fahren?, MMR 2019, 509–513.
Steeves, *Valerie*, Reclaiming the Social Value of Privacy, in: Kerr, Ian, et al. (Hrsg.), Lessons from the Identity Trail. Anonymity, Privacy and Identity in a Networked Society, Oxford 2009, 191–208.
Steidle, *Roland/Pordesch*, *Ulrich*, Im Netz von Google. Web-Tracking und Datenschutz, DuD 2008, 324–329.
Steinbach, *Michael*, *et al.*, A comparison of document clustering techniques, KDD Workshop on Text Mining 2000, 525–526.
Steindorff, *Ernst*, Wirtschaftsordnung und -steuerung durch Privatrecht, in: Baur, Fritz, et al. (Hrsg.), Festschrift für Ludwig Raiser, Tübingen 1974, 621–644.
–, EG-Vertrag und Privatrecht, Baden-Baden 1996.
–, Case C-104/96, *Cooperatieve Rabobank ‚Vecht en Plassengebied' BA* v. *Erik Aarnoud Minderhoud*, Judgment of the Court (sixth chamber) of 16 December 1997, ECR I-7219, 36 Common Market Law Review 191 (1999).
Stempel, *Christian*, Die „Grundsätze des bürgerlichen Rechts", das sekundäre Unionsrecht und der nationale Richter, ZEuP 2010, 925–944.
–, Treu und Glauben im Unionsprivatrecht, Tübingen 2016.
Stieper, *Malte*, Big Brother is watching you – Zum ferngesteuerten Löschen urheberrechtswidrig vertriebener E-Books, AfP 2010, 217–222.
Stiftung Datenschutz, Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, Leipzig 2017.
Stigler, *George J.*, The Economics of Information, 69 Journal of Political Economy 1961, 213–225.
–, The Theory of Price, 4. Aufl., New York/London 1987.
Stoffels, *Markus*, Schranken der Inhaltskontrolle, JZ 2001, 843–849.

Stoffels, *Markus/Lohmann*, *Stefan*, Risikobeherrschung und Versicherbarkeit als Beurteilungsfaktoren im Vertragsrecht, VersR 2003, 1343–1350.

Story, *Peter*, *et al.* Natural Language Processing for Mobile App Privacy Compliance, Proceedings of the PAL: Privacy-Enhancing Artificial Intelligence and Language Technologies 2019, 24–32.

Stoycheff, *Eizabeth/Liu*, *Juan/Xu*, *Kai/Wibowo*, *Kunto*, Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects, 21 New Media & Society 2018, 602–619.

Strandburg, *Katherine J.*, Free fall: The online market's consumer preference disconnect, University of Chicago Legal Forum, 2013, 95–172.

Streinz, *Rudolf* (Hrsg.), EUV/AEUV, 3. Aufl., München 2018.

Streinz, *Rudolf/Michl*, *Walther*, Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht, EuZW 2011, 384–388.

Stucke, *Maurice E.*, Should We Be Concerned About Data-opolies?, 2 Georgetown Law Technology Review 2018, 275–324.

Stürner, *Michael*, Das Verhältnis des Gemeinsamen Europäischen Kaufrechts zum Richtlinienrecht, in: Schulte-Nölke et al. (Hrsg.), Der Entwurf für ein optionales europäisches Kaufrecht, München 2012, 47–84.

–, Amtsprüfung im Mahnverfahren und Unzulässigkeit der Vertragsanpassung bei missbräuchlicher Verzugszinsklausel, ZEuP 2013, 666–680.

Suhr, *Jan*, Richtlinienkonforme Auslegung im Privatrecht und nationale Auslegungsmethodik, Baden-Baden 2011.

Sun, *Chen*, *et al.*, Revisiting unreasonable effectiveness of data in deep learning era, Proceedings of the IEEE International Conference on Computer Vision 2017, 843–852.

Sun, *Yi*, *et al.*, Deepid3: Face recognition with very deep neural networks, Working Paper, 2015, https://arxiv.org/abs/1502.00873.

Sunstein, *Cass R.*, Memorandum for the Heads of Executive Departments and Agencies: Informing Consumers through Smart Disclosure, Washington D.C. 2011.

–, Simpler: The Future of Government, New York 2013.

–, Choosing not to Choose, 64 Duke Law Journal 2014, 1–52.

–, Choosing not to Choose, Oxford u. a. 2015.

Surden, *Harry*, Computable Contracts, 46 UC Davis Law Review 2012, 629–700.

Sutton, *Richard S./Barto*, *Andrew G.*, Reinforcement Learning. An Introduction, 2. Aufl., Cambridge, MA 2018.

Svantesson, *Dan Jerker B.*, Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, 5 International Data Privacy Law 2015, 226–234.

–, Enter the Quagmire – The Complicated Relationship Between Data Protection Law and Consumer Protection Law, 34 Computer Law and Security Review 2018, 25–36.

Sweeney, *Latanya*, Uniqueness of Simple Demographics in the U.S. Population, Laboratory for International Data Privacy, Working Paper LIDAP-WP4, 2000.

–, k-anonymity: A model for protecting privacy, 10 International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 2002, 557–570.

–, Discrimination in online ad delivery, 56(5) Communications of the ACM 2013, 44–54.

Sydow, *Gernot* (Hrsg.), Europäische Datenschutzgrundverordnung. Handkommentar, 2. Aufl. Baden-Baden 2018.

Symantec, Internet Security Threat Report, Volume 24, Mountain View 2019.
Taeger, *Jürgen*, Scoring in Deutschland nach der EU-Datenschutzgrundverordnung, ZRP 2016, 72–75.
Taeger, *Jürgen*, Verbot des Profiling nach Art. 22 DS-GVO und die Regulierung des Scoring ab Mai 2018, RDV 2017, 3–9.
Taeger, *Jürgen/Gabel*, *Detlev* (Hrsg.), DSGVO BDSG, 3. Aufl., Frankfurt a. M. 2019.
Taeger, *Jürgen/Schweda*, *Sebastian*, Die gemeinsam mit anderen Erklärungen erteilte Einwilligung, ZD 2020, 124–129.
Tambou, *Olivia*, France· Lessons from the First Post-GDPR Fines of the CNIL against Google LLC, 5 European Data Protection Law Review 2019, 80–84.
Tanenbaum, *Andrew S./Wetherall*, *David J.*, Computer Networks, 5. Aufl., Harlow 2014.
Tavanti, *Pascal*, Datenverarbeitung zu Werbezwecken nach der Datenschutz-Grundverordnung (Teil 1), RDV 2016, 231–240.
–, Datenverarbeitung zu Werbezwecken nach der Datenschutz-Grundverordnung (Teil 2), RDV 2016, 295–306.
Tene, *Omer/Polonetsky*, *Jules*, Big data for all: Privacy and user control in the age of analytics, 11 Northwestern Journal of Technology and Intellectual Property 2012, 239–273.
Tesfay, *Welderufael B.*, *et al.*, I Read but Don't Agree: Privacy Policy Benchmarking using Machine Learning and the EU GDPR, Companion Proceedings of the The Web Conference 2018, 163–166.
Tesfay, *Welderufael B.*, *et al.*, PrivacyGuide: towards an implementation of the EU GDPR on internet privacy policy evaluation, Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics 2018, 15–21.
Tessier, *Catherine*, Robots Autonomy: Some Technical Issues, in: Lawless, W.F., et al. (Hrsg.), Autonomy and Artificial Intelligence. A Threat or Savior?, Cham 2017, 179–194.
Teubner, *Gunther*, Netzwerk als Vertragsverbund, Baden-Baden 2004.
–, Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten, AcP 182 (2018), 155–205.
Thaler, Richard H. (Hrsg.), Advances in Behavioral Finance, Princeton/Oxford, 2005.
Thaler, *Richard/Sunstein*, *Cass R.*, Nudge: Improving Decisions About Health, Wealth, and Happiness, New Haven/London 2008.
Thiele, *Alexander*, Die Integrationsidentität des Art. 23 Abs. 1 GG als (einzige) Grenze des Vorrangs des Europarechts, EuR 2017, 367–381.
Thon, *Marian*, Transnationaler Datenschutz: Das Internationale Datenprivatrecht der DS-GVO, RabelsZ 84 (2020), 24–61.
Thoma, *Florian*, Risiko im Datenschutz – Stellenwert eines systematischen Risikomanagements in BDSG und DS-GVO-E, ZD 2013, 578–581.
Threema, Cryptography Whitepaper, o. O. 2019.
Thüsing, *Gregor*, Unwirksamkeit und Teilbarkeit unangemessener AGB, BB 2006, 661–664.
–, Rechtsfolgen unwirksamer AGB, VersR 2015, 927–941.
Timpson, *Steve/Troutman*, *Marci*, The Importance of a Layered Privacy Policy on All Mobile Internet Sites and Mobile Marketing Campaigns, 4 International Journal of Mobile Marketing 2009, 57–61.
Tinnefeld, *Marie-Therese/Conrad*, *Isabell*, Die selbstbestimmte Einwilligung im europäischen Recht, ZD 2018, 391, 393–398.

TipTopSecurity, How Does HTTPS Work? RSA Encryption Explained (10.9.2017), https://tiptopsecurity.com/how-does-https-work-rsa-encryption-explained/.

Tomuro, *Noriko/Lytinen*, *Steven/Hornsburg*, *Kurt*, Automatic summarization of privacy policies using ensemble learning, Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy 2016, 133–135.

Topol, *Eric J.*, High-performance medicine: the convergence of human and artificial intelligence, 25 Nature Medicine 2019, 44–56.

Toubiana, *Vincent*, *et al.*, Adnostic: Privacy Preserving Targeted Advertising, Network and Distributed System Security Symposium 2010, o. S. *Traung*, *Peter*, The Proposed New EU General Data Protection Regulation, CRi 2012, 33–49.

Tropina, *Tatiana*, Public – Private Collaboration: Cybercrime, Cybersecurity and National Security, in: *Tropina*, *Tatiana/Callanan*, *Cormac* (Hrsg.), Self- and Co-regulation in Cybercrime, Cybersecurity and National Security, Cham u. a. 2015, 1–41.

Trstenjak, *Verica/Beysen*, *Erwin*, Das Prinzip der Verhältnismäßigkeit in der Unionsrechtsordnung, EuR 2012, 265–284.

Trute, *Hans-Heinrich*, Der Schutz personenbezogener Informationen in der Informationsgesellschaft, JZ 1998, 822–831.

Tsai, *Janice Y.*, *et al.*, The effect of online privacy information on purchasing behavior: An experimental study, 22 Information Systems Research 2011, 254–268.

Tufekci, *Zeynep*, Machines Shouldn't Have to Spy On Us to Learn, Wired (25.3.2019), https://www.wired.com/story/machines-shouldnt-have-to-spy-on-us-to-learn/.

Turing, *Alan M.*, Computing Machinery and Intelligence, 59 Mind 1950, 433–460.

Turing, *Alan M.*, Intelligent Machinery, Report, 1948, zunächst unpubliziert, posthum abgedruckt in Copeland, B. Jack (Hrsg.), The Essential Turing, Oxford 2004, 410–432.

Turow, *Joseph*, *et al.*, The Federal Trade Commission and Consumer Privacy in the Coming Decade, 3 I/S: A Journal of Law and Policy for the Information Society 2008, 723–749.

Tversky, *Amos/Kahneman*, *Daniel*, Availability: A heuristic for judging frequency and probability, 5 Cognitive Psychology 1973, 207–232.

Uebele, *Fabian*, Datenschutzrecht vor Zivilgerichten, GRUR 2019, 694–703.

Uecker, *Philip*, Die Einwilligung im Datenschutzrecht und ihre Alternativen, ZD 2019, 248–251.

–, Extraterritorialer Anwendungsbereich der DS-GVO, ZD 2019, 67–71.

ULD Schleswig-Holstein, Datenschutzrechtliche Bewertung der Reichweitenanalyse durch Facebook, 2011.

Ulmer, *Peter*, Teilunwirksamkeit von teilweise unangemessenen AGB-Klauseln? – Zum Verhältnis von geltungserhaltender Reduktion und ergänzender Vertragsauslegung, NJW 1981, 2025–2033.

Ulmer, *Peter/Brandner*, *Hans E./Hensen*, *Horst-Diether* (Hrsg.), AGB-Recht, 12. Aufl., Köln 2016.

Unabhängiges Landeszentrums für Datenschutz Schleswig-Holstein, Kundenbindungssysteme und Datenschutz, Gutachten, Kiel 2003.

Unberath, *Hannes*, Die Vertragsverletzung, Tübingen 2007.

United States Government Accountability Office, Internet of Things, Technology Assessment, Washington, DC 2017.

University of Maryland, The Buddy System: Human-Computer Teams, IEEE Spectrum (16.4.2019), https://spectrum.ieee.org/robotics/robotics-hardware/the-buddy-system-human-computer-teams.

Unseld, *Christopher*, Zur Bedeutung der Horizontalwirkung von EU-Grundrechten, Tübingen 2019.

Unseld, *Florian*, Die Übertragbarkeit von Persönlichkeitsrechten, GRUR 2011, 982–988.

Urbach, *Nils*, Betriebswirtschaftliche Besonderheiten digitaler Güter, in: Martin Schmidt-Kessel/Malte Kramme, Geschäftsmodelle in der digitalen Welt, Jena 2017, 39–62.

Urquhart, *Lachlan/Sailaja*, *Neelima/McAuley*, *Derek*, Realising the right to data portability for the domestic Internet of things, 22 Personal and Ubiquitous Computing 2018, 317–332.

Utz, *Christine*, (Un)informed Consent: Studying GDPR Consent Notices in the Field, 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), 1–18.

V, *Priyanka*, Demystifying Edge vs. Cloud Computing, DZone (15.3.2019), https://dzone.com/articles/demystifying-the-edge-vs-cloud-computing.

Vanberg, *Viktor J.*, Freiburg School of Law and Economics, in: Newman, Peter (Hrsg.), The New Palgrave Dictionary of Law and Economics, Band 2, 1998, 172–179.

Varian, *Hal*, Intermediate Micro-Economics, 8. Aufl., New York/London 2010.

Veil, *Winfried*, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip – Eine erste Bestandsaufnahme, ZD 2015, 347–352.

–, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ 2018, 686–696.

–, Einwilligung oder berechtigtes Interesse? – Datenverarbeitung zwischen Skylla und Charybdis, NJW 2018, 3337–3344.

Velasquez, *Karima*, *et al.*, Fog orchestration for the Internet of Everything: state-of-the-art and research challenges, 9 Journal of Internet Services and Applications 2018, 14–36.

Veljanovski, *Cento*, Economic Approaches to Regulation, in: Baldwin, Robert/Cave, Martin/Lodge, Martin (Hrsg.), The Oxford Handbook of Regulation, Oxford 2010, 18–38.

Verykios, *Vassilios S.*, *et al.*, State-of-the-art in privacy preserving data mining, 33 ACM Sigmod Record 2004, 50–57.

Voigt, *Paul*, Internationale Anwendbarkeit des deutschen Datenschutzrechts – Eine Darstellung anhand verschiedener Fallgruppen, ZD 2014, 15–21.

Voigt, *Paul/Alich*, *Stefan*, Facebook-Like-Button und Co. – Datenschutzrechtliche Verantwortlichkeit der Webseitenbetreiber, NJW 2011, 3541–3544.

von der Groeben, *Hans/Schwarze*, *Jürgen/Hatje*, *Armin* (Hrsg.), Europäisches Unionsrecht, 7. Aufl., Baden-Baden 2015.

Wachter, *Sandra*, Affinity Profiling and Discrimination by Association in Online Behavioural Advertising, 35 Berkeley Technology Law Journal (im Erscheinen), https://ssrn.com/abstract=3388639.

Wachter, *Sandra/Mittelstadt*, *Brent/Floridi*, *Luciano*, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 International Data Privacy Law 2017, 76–99.

Wachter, *Sandra/Mittelstadt*, *Brent/Russell*, *Chris*, Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GPDR, 31 Harvard Journal of Law and Technology 2017, 841–888.

–, Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI, Working Paper, 2020, https://ssrn.com/abstract=3547922.

Wacke, *Andreas*, Dolo facit qui petit quod (statim) redditurus est, JA 1982, 477–479.
Wagner, *Bernd*, Disruption der Verantwortlichkeit, ZD 2018, 307–310.
Wagner, *Gerhard*, Prozeßverträge. Privatautonomie im Verfahrensrecht, Tübingen 1998.
–, Geldersatz für Persönlichkeitsverletzungen, ZEuP 2000, 200–228.
–, Prävention und Verhaltenssteuerung durch Privatrecht – Anmaßung oder legitime Aufgabe, AcP 206 (2006), 352–476.
–, Materialisierung des Schuldrechts unter dem Einfluss von Verfassungsrecht und Europarecht, in: Blaurock, Uwe/Hager, Günter, Obligationenrecht im 21. Jahrhundert, Baden-Baden 2010, 13–84.
–, Anmerkung, JZ 2017, 522–525.
Wagner, *Gerhard/Eidenmüller*, *Horst*, Down by Algorithms: Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions, 86 University of Chicago Law Review 2019, 581–609.
Wagner, *Gerhard/Potsch*, *Nicolas*, Haftung für Diskriminierungsschäden nach dem Allgemeinen Gleichbehandlungsgesetz, JZ 2006, 1085–1100.
Waldman, *Ari Ezra*, Privacy, Notice, and Design, 21 Stanford Technology Law Review 2018, 129–184.
Wang, *JunPing*, *et al.*, Industrial Big Data Analytics: Challenges, Methodologies, and Applications, Working Paper, 2018, https://arxiv.org/abs/1807.01016.
Wang, *Yang*, *et al.*, Privacy nudges for social media: an exploratory Facebook study, Proceedings of the 22nd International Conference on World Wide Web 2013, 763–770.
–, A field trial of privacy nudges for Facebook, Proceedings of the 32nd annual ACM conference on Human factors in computing systems 2014, 2367–2376.
Wang, *Yilun/Kosinski*, *Michal*, Deep neural networks are more accurate than humans at detecting sexual orientation from facial images, 114 Journal of Personality and Social Psychology 2018, 246–257.
Wank, *Rolf*, Bereitschaftsdienst als Arbeitszeit. Besprechung des Beschlusses BAG v. 18. 2. 2003 – 1 ABR 2/02, NZA 2004, 246–252.
Warner, *Richard/Sloan*, *Robert H.*, Behavioral Advertising: From One-Sided Chicken to Informational Norms, 15 Vanderbilt Journal of Entertainment and Technology Law 2012, 49–83.
Weatherill, *Stephen*, Compulsory Notification of Draft Technical Regulations: The Contribution of Directive 83/189 to the Management of the Internal Market, 16 Yearbook of European Law 1996, 129–204.
Weber, *Rolf H.*, Internet of Things – New security and privacy challenges, 26 Computer Law & Security Review 2010, 23–30.
Weck, *Thomas*, Schutzrechte und Standards aus Sicht des Kartellrechts, NJOZ 2009, 1177–1188.
Wedel, *Michel/Kannan*, *P.K.*, Marketing analytics for data-rich environments, 80 Journal of Marketing 2016, 97–121.
Weichert, *Thilo*, Informationstechnische Arbeitsteilung und datenschutzrechtliche Verantwortung – Plädoyer für eine Mitverantwortlichkeit bei der Verarbeitung von Nutzungsdaten, ZD 2014, 605–610.
–, „Sensitive Daten" revisited, DuD 2017, 538–543.
Weidert, *Stefan/Klar*, *Manuel*, Datenschutz und Werbung – gegenwärtige Rechtslage und Änderungen durch die Datenschutz-Grundverordnung, BB 2017, 1858–1864.

Weinberg, *Gabriel*, Protecting Your Personal Data Has Never Been This Easy, DuckDuckGo (23.1.2018), https://spreadprivacy.com/privacy-simplified/.
Weinstein, *Neil D.*, Optimistic biases about personal risks. 246 Science, 1989, 1232–1234.
Weinstein, *Neil D.*,/*Klein*, *William M.*, Unrealistic Optimism: Present and Future, 15 Journal of Social and Clinical Psychology 1996, 1–8.
Welbourne, *Evan/Battle*, *Leilani/Cole*, *Garret/Gould*, *Kayla/Rector*, *Kyle/Raymer*, *Samuel/Balazinska*, *Magdalena/Borriello*, *Gaetano*, Building the internet of things using RFID: the RFID ecosystem experience, 13(3) IEEE Internet Computing 2009, 48–55.
Wendehorst, *Christiane*, Consumer Contracts and the Internet of Things, in: Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Digital Revolution. Challenges for Contract Law in Practice, Baden-Baden 2016, 189–223.
–, Die Digitalisierung und das BGB, NJW 2016, 2609–2613.
–, Hybride Produkte und hybrider Vertrieb. Sind die Richtlinienentwürfe vom 9. Dezember 2015 fit für den digitalen Binnenmarkt?, in: Wendehorst, Christiane/Zöchling-Jud, Brigitta (Hrsg.), Ein neues Vertragsrecht für den digitalen Binnenmarkt?, Wien 2016, 45–89.
–, Verbraucherrelevante Problemstellungen zu Besitz- und Eigentumsverhältnissen beim Internet der Dinge, Rechtsgutachten für Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz, Berlin 2016.
–, Personal Data in Data Value Chains – Is Data Protection Law Fit for the Data Economy?, in: Lohsse, Sebastian/Schulze, Reiner/Staudenmayer, Dirk (Hrsg.), Data as Counter-Performance: Contract Law 2.0?, Oxford/Baden-Baden 2020 (im Erscheinen).
Wendehorst, *Christiane/Graf von Westphalen*, *Friedrich*, Das Verhältnis zwischen Datenschutz-Grundverordnung und AGB-Recht, NJW 2016, 3745–3750.
Wendland, *Matthias*, Sonderprivatrecht für Digitale Güter, ZvglRWiss 2019, 191–230.
–, Vertragsfreiheit und Vertragsgerechtigkeit, Tübingen 2019.
Wente, *Jürgen*, Informationelles Selbstbestimmungsrecht und absolute Drittwirkung der Grundrechte, NJW 1984, 1446–1447.
Werbach, *Kevin*, The Real Reason for Facebook's New Cryptocurrency, The New York Times, (20.6.2019), https://www.nytimes.com/2019/06/20/opinion/facebook-libra-cryptocurrency.html.
Werkmeister, *Christoph*, Anmerkung zu EuGH: Verbraucherrecht: Gesamtnichtigkeit eines Verbraucherkreditvertrags, EuZW 2012, 303–304.
Wettig, *Steffen*, Vertragsabschluss mittels elektronischer Agenten, Berlin 2010.
Weyrich, *Michael/Schmidt*, *Jan-Philipp/Ebert*, *Christoph*, Machine-to-Machine Communication, 31(4) IEEE Software 2014, 19–23.
WhatsApp, Encryption Overview, Technical White Paper, o. O. 2017.
Whittington, *Jan/Hoofnagle*, *Chris Jay*, Unpacking Privacy's Price, 90 North Carolina Law Review 2011, 1327–1370.
Widrow, *Bernard/Hoff*, *Marcian E.*, Adaptive Switching Circuits, Technical Report No. 1553–1, Stanford, 1960.
Wiebe, *Andreas*, Die elektronische Willenserklärung, Tübingen 2002.
Wiebe, *Andreas/Eichfeld*, *Matthias*, Spannungsverhältnis Datenschutzrecht und Justiz, NJW 2019, 2734–2738.

Wienbracke, *Mike*, Unterschiedliche Behandlung von Bewerbern wegen Ihrer Konfession im Stellenbesetzungsvefahren eines kirchlichen Arbeitgebers, NZA-RR 2018, 349–350.

Wijesekera, *Primal*, *et al.*, The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences, IEEE Symposium on Security and Privacy (SP) 2017, 1077–1093.

Wikipedia, Inlineframe, https://de.wikipedia.org/wiki/Inlineframe (zuletzt aufgerufen am 29.5.2019).

Willenborg, *Leon/De Waal*, *Ton*, Elements of Statistical Disclosure Control, New York 2001.

Willis, *Lauren E.*, Why Not Privacy by Default?, 29 Berkeley Technology Law Journal 2014, 61–133.

Wilson, *Shomir*, *et al.*, Analyzing privacy policies at scale: From crowdsourcing to automated annotations, 13 (1) ACM Transactions on the Web (TWEB) 2018, Article 1.

Wilson, *Shomir*, *et al.*, Crowdsourcing Annotations for Websites' Privacy Policies: Can It Really Work?, Proceedings of the 25th International Conference on World Wide Web 2016, 133–143.

Wind, *Irene*, Haftung bei Verarbeitung personenbezogener Daten, RDV 1991, 16–24.

Windbichler, *Christine*, Neue Vertriebsformen und ihr Einfluß auf das Kaufrecht, AcP 198 (1998), 261–286.

–, Gesellschaftsrecht, 24. Aufl., München 2017.

Windel, *Peter A.*, Unsinnige, rechtlich unmögliche und verbotswidrige Leistungsversprechen, ZGS 2003, 466–472.

Winkelmann, *Thomas*, Falschauskünfte von Auskunfteien: Zum Verhältnis von § 824 BGB zu § 32 Abs. 2 BDSG, MDR 1985, 718–720.

Winston, *Patrick Henry*, Artificial Intelligence, 3. Aufl., Reading, MA 1992.

Winter, *Christian/Battis*, *Verena/Halvani*, *Oren*, Herausforderungen für die Anonymisierung von Daten, ZD 2019, 489–493.

Wintermeier, *Martin*, Inanspruchnahme sozialer Netzwerke durch Minderjährige – Datenschutz aus dem Blickwinkel des Vertragsrechts, ZD 2012, 210–214.

WIPO, Draft Issues Paper on Intellectual Property and Artificial Intelligence, WIPO/IP/AI/2/GE/20/1, Genf 2019.

Wischmeyer, *Thomas*, Regulierung intelligenter Systeme, AöR 143 (2018), 1–66.

Wismer, *Sebastian/Rasek*, *Arno*, Market definition in multi-sided markets, in: OECD (Hrsg.), Rethinking Antitrust Tools for Multi-Sided Platforms, Paris 2018, 55–67.

Wissenschaftliche Dienste – Deutscher Bundestag, Zulässigkeit der Transkribierung und Auswertung von Mitschnitten der Sprachsoftware „Alexa" durch Amazon, WD 10 – 3000 – 032/19, Sachstand, 2019.

Witten, *Ian H.*, *et al.*, Data Mining. Practical Machine Learning Tools and Techniques, 4. Aufl., Amsterdam u. a. 2016.

Wolf, *Manfred*, Rechtsgeschäftliche Entscheidungsfreiheit und vertraglicher Interessenausgleich, Tübingen 1970.

Wolf, *Manfred/Neuner*, *Jörg*, Allgemeiner Teil des Bürgerlichen Rechts, 11. Aufl., München 2016.

Wolff, *Robert Raul*, In Defense of Anarchism, Berkeley u. a. 1970.

Worms, *Christoph/Gusy*, *Christoph*, Verfassung und Datenschutz, DuD 2012, 92–99.

Wright, *David/De Hert*, *Paul*, Introduction to Privacy Impact Assessment, in: Wright, David/De Hert, Paul (Hrsg.), Privacy Impact Assessment, Dordrecht u. a. 2012, 3–32.

Wulfers, *Christian*, Allgemeine Rechtsgrundsätze als ungeschriebenes Recht der supranationalen Gesellschaftsrechtsformen, GPR 2006, 106–114.
Wunner, *Sven Erik*, Die Rechtsnatur der Rückgewährpflichten bei Rücktritt und auflösender Bedingung mit Rückwirkungsklausel, AcP 168 (1968), 425–449.
Würdinger,*Markus*, Doppelwirkungen im Zivilrecht, JuS 2011, 769–774.
Wybitul, *Tim*, DS-GVO veröffentlicht – Was sind die neuen Anforderungen an die Unternehmen?, ZD 2016, 253–254.
Wybitul, *Tim/Böhm*, *Wolf-Tassilo*, Freier Wille auch im Arbeitsverhältnis?, BB 2015, 2101–2105.
Wybitul, *Tim/Haß*, *Detlef/Albrecht*, *Jan Philipp*, Abwehr von Schadensersatzansprüchen nach der Datenschutz-Grundverordnung, NJW 2018, 113–118.
Wybitul, *Tim/Neu*, *Leonie/Strauch*, *Martin*, Schadensersatzrisiken für Unternehmen bei Datenschutzverstößen, ZD 2018, 202–207.
Xiong, *Wayne*, *et al.*, The Microsoft 2017 conversational speech recognition system, IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) 2018, 5934–5938.
Xu, *Heng*, *et al.*, The role of push-pull technology in privacy calculus: the case of location-based services, 26 Journal of Management Information Systems 2009, 135–174.
Xu, *Kaihe*, *et al.*, Privacy-preserving machine learning algorithms for big data systems, IEEE 35th international conference on distributed computing systems 2015, 318–327.
Yang, *Yuchen*, *et al.* A survey on security and privacy issues in Internet-of-Things, 4 IEEE Internet of Things Journal 2017, 1250–1258.
Yanofsky, *David*, Google can still use Bluetooth to track your Android phone when Bluetooth is turned off, Quartz (24.1.2018), https://qz.com/1169760/phone-data/.
Youyou, *Wu/Kosinski*, *Michal/Stillwell*, *David*, Computer-based personality judgments are more accurate than those made by humans, 112 Proceedings of the National Academy of Sciences 2015, 1036–1040.
Zaeem, *Razieh Nokhbeh/German*, *Rachel L./Barber*, *K. Suzanne*, PrivacyCheck: Automatic Summarization of Privacy Policies Using Data Mining, 18(4) ACM Transactions on Internet Technology (TOIT) 2018, Article 53.
Zaglia, *Melanie*, Brand communities embedded in social networks, 66 Journal of Business Research 2013, 216–223.
Zamir, *Eyal/Teichmann*, *Doron*, Behavioral Law and Economics, Oxford 2018.
Zarsky, *Tal Z.*, Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society, 56 Maine Law Review 2004, 13–59.
Zech, *Herbert*, Information als Schutzgegenstand, Tübingen 2012.
–, Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers", CR 2015, 137–146.
–, „Industrie 4.0" – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151–1160.
–, Künstliche Intelligenz und Haftungsfragen, ZfPW 2019, 198–219.
–, Risiken digitaler Systeme: Robotik, Lernfähigkeit und Vernetzung als aktuelle Herausforderungen für das Recht, Weizenbaum Series #2, Berlin 2020.
Zehlike, *Meike/Hacker*, *Philipp/Wiedemann*, *Emil*, Matching code and law: achieving algorithmic fairness with optimal transport, 34 Data Mining and Knowledge Discovery 2020, 163–200.

Zeigler, Bernard P., High autonomy systems: concepts and models, Proceedings of AI, Simulation and Planning in High Autonomy Systems 1990, 2–7.

Zhang, Aston, et al., Dive into Deep Learning, Open Source Manuskript, Release 0.7.1., 2019, https://d2l.ai/.

Zibuschka, Jan/Horsch, Moritz/Kubach, Michael, The ENTOURAGE Privacy and Security Reference Architecture for Internet of Things Ecosystems, Open Identity Summit 2019, 119–130.

Zibuschka, Jan/Nofer, Michael/Hinz, Oliver, Zahlungsbereitschaft für Datenschutzfunktionen intelligenter Assistenten, Multikonferenz Wirtschaftsinformatik (MKWI) 2016, 1391–1402.

Ziebarth, Wolfgang, Google als Geheimnishüter? – Verantwortlichkeit der Suchmaschinenbetreiber nach dem EuGH-Urteil, ZD 2014, 394–399.

Ziegenhorn, Gero, Anmerkung zu Breyer, NVwZ 2017, 216–218.

Ziegenhorn, Gero/von Heckel, Katharina, Datenverarbeitung durch Private nach der europäischen Datenschutzreform, NVwZ 2016, 1585–1591.

Ziegler, Sébastian, Internet of Things Cybersecurity Paradigm Shift, Threat Matrix and Practical Taxonomy, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 1–7.

Ziegler, Sébastian, et al., Privacy and Security Threats on the Internet of Things, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 9–43.

Ziegler, Sébastian/Menon, Mythili/Annichino, Pasquale, IoT Privacy and Security in Smart Cities, in: Ziegler (Hrsg.), Internet of Things Security and Data Protection, 2019, 149–171.

Zimmeck, Sebastian, et al., Automated Analysis of Privacy Requirements for Mobile Apps, Network and Distributed System Security Symposium 2017, 1–15.

Zimmeck, Sebastian, et al., MAPS: Scaling privacy compliance analysis to a million apps, Proceedings on Privacy Enhancing Technologies 2019 (3), 66–86.

Zimmeck, Sebastian/Bellovin, Steven M., Privee: An architecture for automatically analyzing web privacy policies, 23rd USENIX Security Symposium 2014, 1–16.

Zimmermann, Christian/Accorsi, Rafael/Müller, Günter, Privacy dashboards: reconciling data-driven business models and privacy, Ninth International Conference on Availability, Reliability and Security 2014, 152–157.

Zimmermann, Reinhard, Richterliches Moderationsrecht oder Totalnichtigkeit?, Berlin 1979.

–, The Law of Obligations, Capetown u. a. 1990.

Zingales, Nicolo, Between a Rock and Two Hard Places: WhatsApp at the Crossroad of Competition, Data Protection and Consumer Law, 33 Computer Law & Security Review 2017, 553–558.

Žliobaitė, Indrė, Measuring discrimination in algorithmic decision making, 31 Data Mining and Knowledge Discovery 2017, 1060–1089.

Zoll, Patrick, Überwachung mit Gesichtserkennung: Made in China, erprobt in Xinjiang und weltweit exportiert, NZZ (3.12.2019), https://www.nzz.ch/international/china-nutzt-gesichtserkennung-fuer-ueberwachung-und-exportiert-sie-ld.1525690.

Zoller, Michael, Vom Kick-Back-Joker zur versteckten Vertriebsprovision: Die Haftung für Vergütungen der Banken geht weiter, BB 2014, 1805–1805.

Zöllner, Wolfgang, Zivilrechtswissenschaft und Zivilrecht im ausgehenden 20. Jahrhundert, AcP 188 (1988), 85–100.

–, Informationsordnung und Recht, Berlin 1990.

–, Regelungsspielräume im Schuldvertragsrecht: Bemerkungen zur Grundrechtsanwendung im Privatrecht und zu den sogenannten Ungleichgewichtslagen, AcP 196 (1996), 1–36.

Zscherpe, *Kerstin*, Anforderungen an die datenschutzrechtliche Einwilligung im Internet, MMR 2004, 723–727.

Zuboff, *Shoshana*, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, London 2019.

Zuiderveen Borgesius, *Frederik J.*, Improving Privacy Protection in the Area of Behavioural Targeting, Alphen aan den Rijn 2015.

–, Informed consent: We can do better to defend privacy, 13 IEEE Security & Privacy 2015, 103–107.

–, Personal data processing for behavioural targeting: which legal basis?, 5 International Data Privacy Law 2015, 163–176.

–, Behavioural Sciences and the Regulation of Privacy on the Internet, in: Alemanno, Alberto/Sibony, Anne-Lise (Hrsg.), Nudge and the Law: A European Perspective, 2015, 179–207.

–, Singling out People without Knowing Their Names – Behavioural Targeting, Pseudonymous Data, and the New Data Protection Regulation, 32 Computer Law & Security Review 2016, 256–271.

–, Strengthening legal protection against discrimination by algorithms and artificial intelligence, The International Journal of Human Rights 2020, DOI: 10.1080/13642987.2020.1743976.

Zuiderveen Borgesius, *Frederik J.*, *et al.*, Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation, 3 European Data Protection Law Review 2017, 1–16.

Zwanzger, *Michael*, Der mehrseitige Vertrag, Tübingen 2013.

Sachregister