DuD-Fachbeiträge

RESEARCH

Alexander Roßnagel
Michael Friedewald *Hrsg.*

Die Zukunft von Privatheit und Selbstbestimmung

Analysen und Empfehlungen zum Schutz der Grundrechte in der digitalen Welt

DuD
Datenschutz und Datensicherheit

OPEN ACCESS

Springer Vieweg

DuD-Fachbeiträge

Die Buchreihe ergänzt die Zeitschrift DuD – Datenschutz und Datensicherheit in einem aktuellen und zukunftsträchtigen Gebiet, das für Wirtschaft, öffentliche Verwaltung und Hochschulen gleichermaßen wichtig ist. Die Thematik verbindet Informatik, Rechts-, Kommunikations- und Wirtschaftswissenschaften. Den Lesern werden nicht nur fachlich ausgewiesene Beiträge der eigenen Disziplin geboten, sondern sie erhalten auch immer wieder Gelegenheit, Blicke über den fachlichen Zaun zu werfen. So steht die Buchreihe im Dienst eines interdisziplinären Dialogs, der die Kompetenz hinsichtlich eines sicheren und verantwortungsvollen Umgangs mit der Informationstechnik fördern möge.

Alexander Roßnagel · Michael Friedewald
(Hrsg.)

Die Zukunft von Privatheit und Selbstbestimmung

Analysen und Empfehlungen zum Schutz der Grundrechte in der digitalen Welt

Springer Vieweg

Hrsg.
Alexander Roßnagel
Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG)
Universität Kassel
Kassel, Deutschland

Michael Friedewald
Fraunhofer ISI
Karlsruhe, Deutschland

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

ISSN 2512-6997 ISSN 2512-7004 (electronic)
DuD-Fachbeiträge
ISBN 978-3-658-35262-2 ISBN 978-3-658-35263-9 (eBook)
https://doi.org/10.1007/978-3-658-35263-9

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Planung/Lektorat: Stefanie Eggert
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Einleitung: Die Zukunft von Privatheit und Selbstbestimmung

Privatheit und Selbstbestimmung im Zeitalter der Digitalisierung

Privatheit und Selbstbestimmung sind Grundbedingungen freier und demokratischer Gesellschaften. Sie wurden als normative Ziele zu einer Zeit konzipiert und ausgestaltet, als es noch keine automatisierte Datenverarbeitung und kein Internet gab. Sie brachten als normatives Konzept das Ideal freier Bürger zum Ausdruck, die aus einem geschützten Rückzugsort heraus selbst darüber bestimmen konnten, wie sie sich in das gesellschaftliche Leben einbringen. Privatheit und Selbstbestimmung waren zusammen mit Meinungs- und Informationsfreiheit, Vereinigungs- und Versammlungsfreiheit Grundlagen demokratischen Ringens um das Allgemeinwohl. Sie schützten die freie Entfaltung von Individuen, gewährleisteten einen vor staatlichem Zugriff geschützten Rückzugsort, bildeten die Grundlage freier Entscheidungsfindung und ermöglichten freie Beiträge zur öffentlichen deliberativen Suche nach dem allgemeinen Interesse.

Unabhängig davon, inwieweit diese normativen Grundbedingungen für Freiheit und Demokratie jemals gesellschaftliche Realität beschrieben, mussten sie sich jedenfalls in dem Maß verändern, wie automatisierte Datenverarbeitung in die Gesellschaft eindrang. Insbesondere neue Gefährdungen von Grundrechten und Demokratie durch die Datenverarbeitung durch staatliche Instanzen forderten in den 1980er Jahren, Privatheit und Selbstbestimmung neu zu konzipieren. Diese neuen Risiken sah das Bundesverfassungsgericht in seinem Volkszählungsurteil vom 15. Dezember 1983 vor allem darin, dass personenbezogene Daten *„unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus – vor allem beim Aufbau integrierter Informationssysteme – mit anderen Datensammlungen zu*

einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsicht- und Anteilnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen"[1]. *„Unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung"* bedurfte der Schutz der Persönlichkeit einer neuen Absicherung durch das Grundrecht auf informationelle Selbstbestimmung. Diese setzt *„voraus, dass dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden"*[2].

Um vor diesen Gefährdungen zu schützen, gewährleistete das neue Grundrecht auf informationelle Selbstbestimmung *„die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen"*[3]. Dieses Grundrecht gewährleistet allerdings kein *„Recht im Sinne einer absoluten, uneingeschränkten Herrschaft über ‚seine' Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit"*[4]. Als Abbildung sozialer Zusammenhänge müssen personenbezogene Daten geregelte Datenverarbeitungen im Interesse des Allgemeinwohls im verhältnismäßigen Umfang zur Verfügung stehen. Die Regelungen zum Schutz der personenbezogenen Daten müssen aber *„eine Gesellschaftsordnung und eine Rechtsordnung verhindern, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. … Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und*

[1] BVerfGE 65, 1.

[2] BVerfGE 65, 1.

[3] Ebd.

[4] Ebd.

Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens ist"[5].

Mit der gegenwärtigen Digitalisierung aller Lebensbereiche, der Globalisierung von Datenaustausch und Kommunikation, der weltweiten Verbreitung digitaler Endgeräte und eingebetteter Systeme, der zunehmenden Bedeutung der Datenökonomie sowie dem Entstehen einer eigenen digitalen Kultur verändern sich die Verwirklichungsbedingungen von Privatheit und Selbstbestimmung erneut. Digitalisierung bietet neue Chancen, sich zu entfalten, sich mit anderen zu vernetzen, sich zu integrieren, sich wirtschaftlich zu betätigen und sich politisch zu engagieren. Zugleich entstehen aber auch neue Gefährdungen und neue Herausforderungen für Freiheit und Demokratie. Diese neuen Chancen und Risiken erfordern ein neues, den veränderten Bedingungen angemessenes Verständnis von Privatheit und Selbstbestimmung.

Die Digitalisierung bietet viele Chancen, um den Schutz und die Wahrnehmung von Privatheit und Selbstbestimmung zu verbessern. Sie bietet viele neue individualisierte Möglichkeiten, sich im privaten Umfeld zu entfalten, sich zu informieren, auf das Wissen der Welt zuzugreifen, Routineentscheidungen zu delegieren, sich in der Alltagsarbeit zu entlasten. Sie bietet vielfältige Chancen, die eigenen Sinne zu erweitern, ohne körperliche Anwesenheit Situationen zu erfassen und zu beeinflussen. Sie erleichtert, sich eine Meinung zu bilden und sie kund zu tun – unmittelbar und ohne Mediatoren. Sie ermöglicht, mit vielen anderen Personen in Kontakt zu treten, sich ihnen gegenüber darzustellen, sich auszutauschen und sich zusammen zu tun. Die Digitalisierung bietet neue berufliche ökonomische Chancen, sie bietet angepasste Unterstützung und indivi dualisierte Assistenz. Die Auswertung der vielen anfallenden Daten stärkt die Wissenschaft, ermöglicht vielfältige neue Erkenntnisse und die Entwicklung neuer Geschäftsmodelle. Sie verstärkt auch die politische Handlungsfähigkeit und vermag demokratische Prozesse zu unterstützen und zu stärken. Schließlich hat sie auch das Potenzial, zukünftige Entwicklungen früher und leichter zu erkennen, politische Kompromisse zu finden und Allgemeininteressen besser zu verfolgen.

Neue Herausforderungen ergeben sich vor allem aus technologischen Entwicklungen. Zum einen führen neue Datenquellen durch Ubiquitous Computing und das Internet der Dinge zu einer enormen Zunahme personenbezogener Daten – vor allem aus der persönlichen Umgebung der betroffenen Personen. Die

[5] Ebd.

Systeme, die diese Daten erheben, verarbeiten und übermitteln, passen sich auf der Grundlage dieser Daten und daraus erstellter Profile sowie ihrer Lernfähigkeit ihren Nutzerinnen und Nutzern an und erleichtern ihnen das Alltags- oder das Berufsleben. Voraussetzung dafür ist aber, dass sie nahezu den gesamten Lebensvollzug protokollieren. Neue Risiken entstehen auch durch neue virtuelle globale Infrastrukturen, wie Such- und Speicherdienste, Social Media sowie Austauschplattformen, deren Nutzung in der digitalen Welt weitgehend unabdingbar ist. Für sie gilt quasi ein sozialer „Anschluss- und Benutzungszwang". Wer sie nutzt, zahlt zwar kein Geld, dafür aber mit personenbezogenen Daten, die für personalisierte Werbung und Dienstleistungen genutzt werden. Schließlich entstehen neue Auswertungsmöglichkeiten für die riesigen Datenmengen durch Big Data und Künstliche Intelligenz. Ihre Ergebnisse erleichtern es, das Verhalten von Menschen und Gruppen zu prognostizieren und zu beeinflussen, und ermöglichen auch die Bewertung von Menschen an algorithmenbasierte Entscheidungssysteme zu delegieren. Zusammengenommen führen diese Entwicklungen dazu, dass die betroffenen Personen für die Datenverarbeiter immer durchsichtiger, die Datenverarbeitungen für die aber immer undurchsichtiger werden. Sie verschieben soziale Macht immer stärker zugunsten der Datenverarbeiter.

Staatliche Stellen nutzen alle diese neuen technischen Möglichkeiten auch zur Erfüllung ihrer Aufgaben. Die zusätzlichen Kenntnisse über Bürger und Bürgerinnen verstärken ihre Macht, nicht aber das Vertrauen, das sie benötigen. Zugleich sind sie neuen Öffentlichkeiten ausgeliefert, die nicht mehr nach alten Mechanismen funktionieren, sondern nach neuen Kulturen zersplitterte virtueller Öffentlichkeiten darstellen (digitaler Tribalismus).

Noch stärker konzentriert sich Daten- und Wissensmacht bei den privaten Internet-Konzernen. Sie üben ihre ökonomische Stärke weltweit auf allen Märkten aus, beeinflussen durch ihre Infrastrukturen Meinungen und Werthaltungen ebenso wie politische Entscheidungsmechanismen. Sie entziehen sich weitgehend staatlichen Vorgaben und bewirken die stärksten Herausforderungen für individuelle und demokratische Selbstbestimmung.

Alle diese Risiken und Herausforderungen sind global und erfordern eigentlich auf die globale Ebene ausgerichtete Schutzkonzepte und weltweit wirksame Schutzmechanismen. Diese Anforderungen überfordern daher einzelne Staaten und übersteigen den Wirkungskreis einzelner Demokratien. Es fehlt jedoch an einer weltweit einheitlichen Sicht auf Privatheit und Selbstbestimmung. Vielmehr konkurrieren unterschiedliche Konzepte für die globale Entwicklung in eine digitale Welt und der Bedeutung von Privatheit und Selbstbestimmung in dieser. In diesem Wettbewerb verfolgt die Europäische Union mit der Grundrechtecharta

und der Datenschutz-Grundverordnung ein Entwicklungskonzept, das auf Menschenwürde und Schutz der Persönlichkeit aufbaut. Damit weist sie einen dritten Weg zwischen dem amerikanischen Modell eines an Gewinnmaximierung orientierten Datenkapitalismus und dem chinesischen Modell einer technikgestützten Überwachungsdiktatur. Dem europäischen Entwicklungsmodell versuchen sich vielen andere Staaten anzuschließen. Es sollte auch die Grundlage für ein zeitgemäßes und zukunftweisendes Verständnis von Privatheit und Selbstbestimmung in der digitalen Welt sein.

Interdisziplinäre Suche nach einem zeitgemäßen und zukunftsweisenden Konzept

Privatheit und Selbstbestimmung ist in einer solchen Welt wieder neu zu konzipieren. Dabei wird es darauf ankommen, Erhaltenswertes zu erhalten, aber den neuen Bedingungen anzupassen. Neuen Chancen der Entwicklung und Entfaltung, die in der bisherigen Konzeption noch nicht berücksichtigt werden konnten, ist ausreichend Raum zu geben, zur Bekämpfung und Vermeidung neuer Risiken für Privatheit und Selbstbestimmung sind neue Schutzkonzepte und -instrumente zu entwickeln.

Bei der Analyse ihrer Verwirklichungsbedingungen, bei der Neukonzeption, was in der künftigen digitalen Welt sinnvoll unter Privatheit und Selbstbestimmung verstanden werden soll, und bei den daraus abzuleitenden Schlussfolgerungen für politisches, rechtliches, wirtschaftliches, soziales und kulturelles Handeln sind unter anderen folgende wichtige Aspekte zu berücksichtigen:

Zunächst ist der *rechtliche Rahmen* zu beachten, der Privatheit und Selbstbestimmung schützt, aber auch konzeptionell festlegt. Sie sind als Grundrechte in der Grundrechtecharta, im Grundgesetz und manchen Landesverfassungen enthalten. Sie lassen durch ihren abstrakten Wortlaut genug Raum für angepasste, zeitgemäße und zukunftstaugliche Konzeptionen. Dennoch enthalten Interpretationen durch die Rechtsprechung und durch die konkretisierende Gesetzgebung in der Datenschutz-Grundverordnung und in den Datenschutzgesetzen des Bundes und der Länder Grenzen für Neukonzeptionen, die es zu beachten gilt. Soweit die rechtsnormativen Konzeptionen von Privatheit und Selbstbestimmung in Gesetzgebung und Rechtsprechung nicht mehr zeitgemäß und zukunftstauglich sind, sind sie anzupassen und fortzuentwickeln. Hierzu sind Verbesserungspotenziale zu erkennen, Entwicklungsziele zu formulieren und rechtpolitische Entwicklungsstrategien zu erarbeiten.

Zum anderen ist der *politische Rahmen* zu beachten, innerhalb dessen um die politische Zukunft von Digitalisierung und Datenschutz gekämpft wird. Dies gilt für die politischen Machtverhältnisse, die weltweit, in der Europäische Union und in Deutschland über den Einfluss auf das Politikfeld entscheiden. Dies gilt auch für die Möglichkeiten des Agendasettings und der Themenauswahl für den politischen Prozess der Entscheidungsfindung. Und es gilt schließlich für die Governance der Datenschutzpolitik und der Datenschutzadministration, die darüber entscheidet, wie Zielsetzungen, Probleme und Lösungsmöglichkeiten thematisiert, priorisiert und konkretisiert werden. Das geeignetste normative Konzept nutzt nichts, wenn es nicht von ausreichend starken Kräften aufgegriffen, in politische Strategien eingebunden und mit der notwendigen Macht durchgesetzt wird.

Digitalisierung erzeugt neue Möglichkeiten zur Befriedigung von Bedürfnissen und der Wertschöpfung in einer *Datenökonomie.* Diese Möglichkeiten zu nutzen setzt aber vielfach Vertrauensbildung und Risikobereitschaft von Kunden voraus, für die Datenschutz eine wichtige Rolle spielt. Wichtige Aspekte des Verständnisses von Privatheit und Selbstbestimmungen betreffen mögliche Geschäftsmodelle, die für Unternehmen attraktiv sind, die den Bedarf auf Verbraucherseite befriedigen und die Anforderungen des Datenschutzes erfüllen. Sie müssen zudem von volkswirtschaftlichen Nutzen sein und sich in der weltweiten Konkurrenz bewähren.

Wie die Datenökonomie ausgestaltet wird, hängt auch von dem *Konsumverhalten* auf Verbraucherseite ab. Ob und inwieweit deren Entscheidungen von Überlegungen oder Routinen zum Schutz ihrer Privatheit beeinflusst werden, ist weitgehend unbekannt. Solche Entscheidungen sind immer in soziotechnische Netzwerke eingebettet und somit auch Resultat der Einflussnahme dieser Netzwerke. Ein neues Konzept von Privatheit und Selbstbestimmung muss berücksichtigen, wie in den neuen Wertschöpfungsprozessen und die auf ihnen fußenden Tauschverhältnisse Bewusstseinsund Handlungsweisen hervorgebracht oder überspielt werden, die Einfluss auf Privatheit und Selbstbestimmung haben.

Aus psychologischer und soziologischer Sicht stellen sich neue Fragen dadurch, dass die Digitalisierung *individuelle und gesellschaftliche Privatheitspraktiken* verändern. Auf der einen Seite steigt das Bedürfnis, privat zu sein und Privatheit zu schützen, und auf der anderen Seite geben Nutzende von Social Media gezielt viele persönliche Information von sich preis. Für ein zukunftsweisendes Konzept von Privatheit und Selbstbestimmung ist es wichtig zu verstehen, in welchen dynamischen Prozessen, unter welchen Bedingungen, aus welchen Motiven und mit welchen Mitteln Individuen und Gruppen den Zutritt zu persönlichen Informationen

kontrollieren. Wichtig ist vor allem auch zu klären, welche Wirkungen die neuen Angebote der Digitalisierung auf soziales Verhalten haben und wie dieses Verhalten die sozialen Verhaltensmöglichkeiten verändert und dazu führt, dass Individuen oder Gruppen aus dem sozialen Zusammenhang ausgeschlossen oder in diesen aufgenommen werden.

Neue Formen der Datenerhebung und -auswertung durch Künstliche Intelligenz und Big Data haben nicht nur Auswirkungen auf betroffene Personen, sondern zunehmend auch auf Dritte und ganze soziale Gruppen. Daher löst sich *philosophische Forschung* zunehmend von stark am Individuum orientierten Privatheitskonzeptionen und thematisieren stärker die sozialen Dimensionen der Privatheit. So stellt sich zum Beispiel die Frage, inwieweit ein Recht auf informationelle Selbstbestimmung praktisch noch individuell ausgeübt und konzeptionell an das Individuum gebunden werden kann. Soweit die Leistungsfähigkeit des Rechts auf informationelle Selbstbestimmung faktisch eingeschränkt ist, sind flankierende und alternative Schutzmaßnahmen zu erörtern sowie kollektive Verantwortlichkeiten aus individuellen Schutzvorstellungen abzuleiten. Zeitgemäße und zukunftsfähige Konzeptionen von Privatheit und Selbstbestimmung müssen daher die soziale Einbettung von Privatheitspraktiken, -problemen und -lösungen in die politisch-normativen, technoökonomischen, soziotechnischen Gefüge berücksichtigen, um bestimmen zu können, wo und auf welche Weise welcher Schutz möglich ist. Erst diese Untersuchung kann auch Grundlage sein, um neue Erkenntnisse über eine normative Bewertung und soziale Gestaltung dieser Gefüge zu gewinnen.

Digitalisierung als politisches, soziales, ökonomisches, rechtliches und kulturelles Phänomen wird vor allem durch die *technische Entwicklung* getrieben und gesteuert. Dies ist für eine neue Konzeption von Privatheit und Selbstbestimmung in zweierlei Weise von besonderer Bedeutung. Erstens ist für ihre Erarbeitung festzustellen, auf welche Weise technologische Veränderungen auf die genannten gesellschaftlichen Bereiche einwirken und diese zu Transformationen anregen. Erkenntnisse über Wirkungen der Digitalisierung ermöglichen, über hilfreiche politische und rechtliche Rahmensetzungen, ökonomische Anreize, soziale Einbettungen und kulturelle Anpassungen zu diskutieren. Zum anderen ist zu untersuchen, wie technische Systeme gestaltet werden können und müssen, um Privatheit und Selbstbestimmung zu unterstützen und zu schützen. Wenn die technische Entwicklung der stärkste Treiber der Digitalisierung und ihrer Auswirkungen ist, dann sollte dieser auch für eine Beeinflussung der gesellschaftlichen Entwicklung und der Gewährleistung ihrer Entwicklungsziele genutzt werden.

Diese ausschnittsweisen Überlegungen zu den Zusammenhängen zwischen der Digitalisierung und den von ihre beeinflussten und sie beeinflussenden gesellschaftlichen Bereichen zeigen, dass eine Suche nach einer zeitgemäßen und zukunftsweisenden Konzeption von Privatheit und Selbstbestimmung nur interdisziplinär gelingen kann.

Das Forum Privatheit

Aus dem Austausch zwischen Vorgängerprojekten[6] und dem Bundesministerium für Bildung und Forschung (BMBF) in den Jahren 2011 und 2012 entstand die Erkenntnis, dass ausgehend von technischen, juristischen, ökonomischen sowie geistes- und gesellschaftswissenschaftlichen Ansätzen ein interdisziplinär fundiertes, zeitgemäßes und zukunftsweisendes Verständnis von Privatheit und Selbstbestimmung erforderlich ist. Dieses Forschungsdesiderat wurde im Zuge der Snowden-Enthüllungen 2013 noch deutlicher und brisanter. Hieraus entstand das interdisziplinäre Verbund-Forschungsprojekt *Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt*[7], das mit Unterstützung des Bundesministeriums für Bildung und Forschung von 2013 bis 2021 das Ziel verfolgte, an Konzepten zur Neubestimmung und Gewährleistung informationeller Selbstbestimmung und Privatheit in der digitalen Welt zu arbeiten.

Das *Forum Privatheit* versteht sich über seine Kerndisziplinen hinaus als eine Plattform für den fachlichen Austausch und erarbeitet Orientierungswissen für den öffentlichen Diskurs in Form wissenschaftlicher Publikationen, Policy- und White-Papers[8] sowie durch Tagungen und Workshops. Mitglieder des *Forum Privatheit* sind die Fraunhofer-Institute für System- und Innovationsforschung (ISI) in Karlsruhe und für Sichere Informationstechnologie (SIT) in Darmstadt, das Fachgebiet Soziologische Theorie und die Projektgruppe verfassungsverträgliche Technikgestaltung (provet), beide Mitglieder des Wissenschaftlichen Zentrums für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel, das Fachgebiet Sozialpsychologie: Medien und Kommunikation an der Universität Duisburg-Essen, das Internationale Zentrum für Ethik in den

[6] Buchmann 2012.

[7] https://www.forum-privatheit.de.

[8] Vgl. die Liste ausgesuchter Veröffentlichungen des *Forum Privatheit* im Anhang dieses Buchs.

Wissenschaften (IZEW) an der Universität Tübingen, das Institut für Wirtschaftsinformatik und neue Medien der Ludwig-Maximilians-Universität München und das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein in Kiel. Von 2013 bis 2017 war auch der Lehrstuhl für Medienpsychologie an der Universität Hohenheim in Stuttgart Mitglied des *Forum Privatheit.*

Übergeordnetes Ziel des Projekts war es, eine interdisziplinäre Sicht auf Probleme der Privatheit und des Datenschutzes zu werfen und aktuelle Forschungsfragen vor dem oben skizzierten Hintergrund zu beantworten. Diese wurden in vier thematische Schwerpunkten gebündelt, nach denen auch die Beiträge in diesem Band gegliedert sind:

Im Schwerpunkt „Privacy-Governance: Privatheit im Kontext von Regulierung der digitalen Welt" wurde untersucht, wie der Einfluss der digitalen Welt auf die sie regulierenden Normen erfolgt und eine Beeinflussung der digitalen Welt durch normative Gestaltung möglich sein kann, wurden Ansätze für eine privatheitsfördernde normative Gestaltung der digitalen Welt (Technik, Organisation, Wirtschaft, Zusammenleben) entwickelt, Inhalte und Wirkungen der Datenschutz-Grundverordnung analysiert, Handlungsmöglichkeiten zur Ausgestaltung des Datenschutzes im Rahmen der Datenschutz-Grundverordnung und Vorschläge zu ihrer Nutzung erarbeitet sowie der Governance-Bedarf und Governance-Formen für die künftigen Herausforderungen von Privatheit und Selbstbestimmung bestimmt und bewertet.

Im Schwerpunkt „Datenökonomien: Verbraucherverhältnisse und Geschäftsmodelle" wurden die Fragen untersucht, wie zentral und dezentral organisierte Datenökonomien in ökonomischer und sozialer Hinsicht funktionieren, welche Wertschöpfungsprozesse und Tauschverhältnisse entstehen, welche Werte dabei geschaffen und wie diese verteilt werden, in welcher Beziehung die Wertschöpfungslogik der Datenökonomien zu Privatheit und Selbstbestimmung steht, welche Konzepte und Praktiken des Privateigentums hierbei eine Rolle spielen und welche Folgen sich in politischer, regulatorischer, ökonomischer und zivilgesellschaftlicher Hinsicht ergeben.

Im Schwerpunkt „Soziale In/-Exklusion" standen die Fragen im Vordergrund, wie Digitalisierung und Privatheit den Einbezug oder Ausschluss in soziale Zusammenhänge beeinflussen und wie dies durch Gestaltungsmaßnahmen verändert werden kann. Dies wurde vor allem am Beispiel demokratischer Selbstregulierung in der digitalen Gesellschaft und des Schutzes von Privatheit und Selbstbestimmung von Kindern in digital überwachten Umgebungen untersucht.

Schließlich war es Ziel im Schwerpunkt „Technische Gestaltung von Daten- und Privatheitsschutz", Bedrohungen für Privatheit und Selbstbestimmung durch

technikinduzierte Wandlungsdynamiken zu analysieren, (pro)aktive Gestaltungsansätze und methoden für privatheitsfreundliche Systeme zu erarbeiten und zu bewerten, das Privacy-by-Design-Paradigma zu operationalisieren und Ansätze zur Stärkung der „digitalen Souveränität“ und zur Erfüllung von rechtlichen Datenschutzpflichten zu erforschen.

Alle Mitglieder arbeiteten mit unterschiedlichen Arbeitsanteilen an alle Schwerpunkten, die Hauptanteile und Verantwortung für die Koordination lagen jedoch bei den Mitgliedern, die „am nächsten“ an dem jeweiligen Thema waren. Die Jahreskon ferenzen des *Forum Privatheit* und die entsprechenden Tagungsbände[9] waren in den letzten vier Jahren jeweils einem dieser Schwerpunkte gewidmet.

Dieses Buch fasst wesentliche Erkenntnisse und Ergebnisse der Forschungen und Diskussionen im Forum Privatheit aus den Jahren 2013 bis 2021 zusammen und präsentiert sie als interdisziplinäre Bausteine einer zeitgemäßen und zukunftsgerechten Konzeption von Privatheit und Selbstbestimmung in der digitalen Welt.

Über dieses Buch

Die europäische Datenschutz-Grundverordnung: Privatheit im Kontext von Regulierung der digitalen Welt

Die beiden Kapitel im ersten Teil dieses Buchs befassen sich damit, wie gewandelte Vorstellungen zum Umgang mit personenbezogenen Daten Regeln des Datenschutzrechts zu beeinflussen vermögen, und umgekehrt, wie neue gesetzliche Regeln des Datenschutzes veränderte normative Erwartungen an den Umgang mit personenbezogenen Daten und zu veränderten Datenschutzpraktiken bewirken. Beide Beiträge tun dies am Beispiel der europäischen Datenschutz-Grundverordnung, deren Umsetzung das Forum Privatheit von Beginn an kritisch-konstruktiv begleitet hat.[10]

Roßnagel, Bile, Geminn und *Nebel* beleuchten in ihrem Beitrag neue Konzepte für den Grundrechtsschutz in der digitalen Welt. Ausgangspunkt ist

[9] Roßnagel, Friedewald und Hansen (2018); Ochs et al. (2019); Stapf et al. (2021); Friedewald, Kreutzer und Hansen (2021).

[10] Roßnagel und Nebel (2016); Roßnagel, Bile et al. (2018); Roßnagel (2017); Roßnagel, Geminn et al. (2019); Karaboga (2018).

die Feststellung, dass die globale Digitalisierung nahezu aller Lebensbereiche zunehmend die individuelle und demokratische Selbstbestimmung gefährdet und umso stärker ihren normativen Schutz erfordert. Die bekannten und bewährten Konzepte, Institutionen und Instrumente des Datenschutzes, die zu Zeiten der kommunalen Gebietsrechenzentren in den 1970er und 1980er Jahren entwickelt wurden, sind für den Schutz gegenüber unseren heutigen globalen digitalen Infrastrukturen mit neuen Datenquellen, virtuellen Infrastrukturen und Verfahren der Künstlichen Intelligenz zunehmend wirkungslos geworden. Die europäische Datenschutz-Grundverordnung (DSGVO) wollte an dieser Stelle Abhilfe schaffen. Die Autoren kritisieren aber, dass die DSGVO mit ihrem Anspruch gescheitert ist, den neuen Herausforderungen durch Harmonisierung und Modernisierung sowie einen risikobasierten Ansatz gerecht zu werden. Darauf aufbauend betrachten die Autoren Elemente zur Fortentwicklung innerhalb des Governance-Rahmens, stellen aber fest, dass diese (bislang) nicht genutzt wurden. Es werden anschließend konkrete Schutzverbesserungen etwa im Bereich des Datenschutzes bei Kindern oder beim Profiling, in Bezug auf eine risikogerechte Regulierung und in Bezug auf die Fortentwicklung der normativen Innovationen wie Sanktionsregime, Datenschutz-Folgenabschätzung und Zertifizierungen angeregt. Abschließend werden neue Konzepte und Instrumente zum Grundrechtsschutz in der globalen digitalen Transformation vorgestellt.

Karaboga, Martin und *Friedewald* setzen sich in ihrem Beitrag mit zwei Strängen der Kritik an der DSGVO auseinander. Zum einen steht die im vorangegangenen Beitrag ausgeführte Kritik an der unzureichenden Harmonisierung und der falsch verstandene Technikneutralität der DSGVO im Fokus. Zum anderen widmen sich die Autoren der Kritik, wonach die mit der DSGVO eingeführten Regelungen zu einer administrativen Mehrbelastung für Unternehmen führen würden. Konkret wird erstens danach gefragt, weshalb die Einführung datenschutzrechtlicher Innovationen durch eine unzureichende Harmonisierung und eine falsch verstandene Technikneutralität begleitet wurden. Zweitens wird gefragt, wie die Innovationen der DSGVO, insbesondere das Sanktionsregime, wirken und welche Effekte die DSGVO auf die Innovationsfähigkeit von Unternehmen hat – wirkt sie eher innovationsfördernd oder innovationshemmend?

Im Hinblick auf die erste Forschungsfrage stellen die Autoren auf Grundlage der Untersuchung des Entscheidungsprozesses der DSGVO fest, dass die mangelnde Harmonisierung des europäischen Datenschutzrechts und die Verabschiedung einer falsch verstandenen Technikneutralität Ergebnis des Widerstands des Ministerrats sind. Das Aufzeigen der historischen Kontinuität der Ablehnung harmonisierter Datenschutzregeln seitens der Mitgliedstaaten

impliziert zudem, dass es sehr unwahrscheinlich ist, dass die Mitgliedstaaten die sich durch die Öffnungsklauseln ergebenden Freiräume für eine Stärkung des Datenschutzrechts nutzen werden.

Im Hinblick auf die zweite Forschungsfrage zeigen die Ergebnisse, dass die DSGVO einerseits durchaus willkommene Innovationshindernisse gerade für solche Datenverarbeitungen schafft, die zu Risiken für die Rechte und Freiheiten der Betroffenen führen könnten. Andererseits deuten die Ergebnisse daraufhin, dass die DSGVO seitens der Mehrzahl deutscher Firmen eher als Wettbewerbsvorteil, denn als -nachteil bewertet wird. Anhand der Diskussion bestehender Studien und der Erhebung eigener Empirie wird aber auch klar, dass die Innovationswirkung der DSGVO weiterer Untersuchungen bedarf.

Datenökonomien: Verbraucherverhältnisse und Geschäftsmodelle

Der zweite Teil dieses Buchs befasst sich damit, wie durch die Digitalisierung neue Wertschöpfungsprozesse und Tauschverhältnisse in zentral und dezentral organisierten Datenökonomien entstehen, die Geschäftsmodelle und Verbraucherverhältnisse so verändern, dass sie massive Auswirkungen auf Privatheit und Selbstbestimmung haben. Die Beiträge zeigen auf, welche Folgen sich hieraus für Privatheit und Selbstbestimmung in politischer, regulatorischer, ökonomischer und zivilgesellschaftlicher Hinsicht ergeben.

Das Kapitel von *Hess, Matt, Thürmel* und *Teebken* untersucht das Zusammenspiel zwischen Unternehmen und Verbrauchern in der Datenökonomie, die dadurch charakterisiert ist, dass Daten in bislang ungekanntem Maß (teil-)automatisch erhoben, gespeichert und verarbeitet werden. Dabei stellen die Verbraucher z. T. selbst – explizit oder implizit durch ihr Verhalten – Daten über sich selbst zur Verfügung. Solche Daten und die darauf basierenden Dienste können wiederum das Entscheidungsverhalten von Unternehmen und Verbrauchern verändern. In einer solchen Datenökonomie entstehen für Unternehmen neue Betätigungsfelder, insbesondere für datengetriebene Dienstleistungen, die auf der verstärkten Verwertung „personenbezogener Daten“ beruhen. Für die Konsumenten können dadurch sowohl Vor- als auch Nachteile entstehen, die individuell abgewogen werden. Anhand von Beispielen aus unterschiedlichen Kontexten erweitert das Autorenteam das Verständnis von Privatheit als komplexes Wechselspiel zwischen Anbietern und Nachfragern.

Zunächst wird die Rolle personenbezogener Daten als unternehmerische Ressource analysiert. Dazu werden detaillierte Charakteristika der involvierten Akteure und Wertschöpfungsstrukturen präsentiert und die Logik zur Nutzung von Daten für unternehmensinterne und -externe Zwecke erläutert. So haben sich mittlerweile differenzierte Märkte für personenbezogene Daten für unterschiedliche Nutzungen entwickelt, die ein erhebliches Wertschöpfungspotenzial aufweisen. Schließlich wird gezeigt, welche Voraussetzungen auf Management- und Datenebene erfüllt sein müssen, damit Daten intern für Synergien und Produktivitätssteigerungen genutzt werden können.

Aus Verbrauchersicht werden die Faktoren analysiert, die im Umgang mit den eigenen und fremden personenbezogenen Daten eine Rolle spielen. Dazu gehören die Zahlungsbereitschaft für einen stärkeren Schutz von Daten, die individuelle Bereitschaft zur Offenlegung von Daten sowie das Bewusstsein, dass das eigene Verhalten (z. B. in Sozialen Medien) auch die Privatheit Dritter tangieren kann. Dabei wird deutlich, wie komplex das Verhalten auf Konsumentenseite letztlich ist und von wie vielen individuellen, strukturellen und kommunikativen Umständen dieses letztlich beeinflusst wird.

Das Kapitel von *Lamla, Büttner, Ochs, Pittroff* und *Uhlmann* wendet sich dem ambivalenten Zusammenspiel von Privatheit und Digitalität zu, indem es deren Relevanz für Diskurse und Praktiken der Selbstbestimmung ausleuchtet und auf die soziotechnischen Transformationen dieses Zusammenspiels bezieht. Privatheit und Digitalität werden dabei als gesellschaftlich mitkonstituierte Sozialformen, Assemblagen oder Kommunikationsverhältnisse perspektiviert, die von historisch sich wandelnden soziokulturellen Einflussgrößen durchzogen sind. Um die skizzierte Perspektive einzunehmen werden zunächst die einschlägigen soziologischen Wissensbestände zu einer kursorischen Darstellung gesellschaftstheoretischer Perspektiven auf Privatheit verdichtet. Daraufhin wendet sich der Beitrag den soziologischen Digitalisierungsforschungen zu, die die Konzeptualisierung von Privatheit nicht unberührt lassen. Hierbei wird v.a. herausgearbeitet, dass das soziologische und gesellschaftstheoretische Bild von Privatheit um Aspekte des Technischen und Materiellen erweitert werden muss. Theoretisch entsprechend eingestellt wird sodann eine Analyse von Selbstbestimmung unter soziodigitalen Verhältnissen präsentiert, die sich an vier zentralen Problemfeldern von Privatheit und Digitalität entfaltet: Die soziale Prämierung von Sichtbarkeit; soziale Konsequenzen digitaler Verhaltensformung; die soziale Dynamik datenökonomischer Erlösmodelle; sowie die Auswirkungen, die sich aus alldem für die Entscheidungsfreiheiten von Nutzenden ergeben. Im Fazit des Beitrags werden Konsequenzen für eine demokratische

und an Selbstbestimmung orientierte Gestaltung von Privatheit benannt. Hierbei zeigt sich ein erheblicher Bedarf an einer Politik der Gestaltung und Regulierung von soziodigitalen Infrastrukturen, die eine Datenökonomie befördert, welche sich der demokratischen Kontrolle, Mitbestimmung und v. a. der Kritik öffnet. Zentrale Kompetenz individueller, wie kollektiver Selbstbestimmung wird damit die Fähigkeit zur Kritik der normierenden Gehalte und Effekte soziodigitaler Infrastrukturen. Diese muss aus den soziodigitalen Verhältnissen und praktischen Situationen selbst erwachsen und die Pluralität von Rechtfertigungsordnungen moderner Gesellschaften einbeziehen, um so die Kontingenz bestehender normativer Ordnungen erfahrbar und alternative Infrastrukturgestaltungspfade begehbar zu machen: Nur, wenn die Infrastrukturen gewährleisten, dass der Faden zur kritischen Praxis nicht reißt, kann Privatheit unter soziodigitalen Bedingungen Ort der Selbstbestimmung bleiben.

Einwirkungen der Digitalisierung auf gesellschaftliche Inklusion und Exklusion

Die beiden Beiträge im dritten Teil des Buchs gehen der Frage nach, wie die Digitalisierung gesellschaftliche In- und Exklusionsprozesse verstärkt oder ihnen entgegenwirkt, indem sie soziale Machtstrukturen und Ungleichheiten verändert, die mit Privatheitspraktiken zusammenhängen. Weitergehend wird thematisiert, wie die Gesellschaft normativ auf diese Prozesse reagieren und wie sie technische und soziale Randbedingungen gestalten sollte.

Meier, Meinert und *Krämer* thematisieren in ihrem Kapitel Schutzbedürfnisse und Schutzverhalten von Internet-Nutzenden aus medienpsychologischer Perspektive. Ausgangspunkt ihrer Argumentation ist die Tatsache, dass die Nutzung des Internets auf der einen Seite zu unzähligen Erleichterungen des täglichen Lebens führt, auf der anderen Seite allerdings auch zu Verletzungen der persönlichen Privatsphäre führen kann, da viele Firmen private Daten der Nutzenden sammeln. Noch sind Nutzende allerdings primär selbst in der Verantwortung, Risiken für ihre Selbstbestimmung zu minimieren, da selbst strenge Datenschutzregelungen wie die europäische DSGVO die Verantwortung für zahlreiche Entscheidungen bei den Nutzenden sehen. Daher ist es von großer Wichtigkeit, die persönlichen Motive für Nutzung bzw. Nicht-Nutzung von Schutzmaßnahmen zu verstehen, um Nutzende gegebenenfalls unterstützen zu können. Vor diesem Hintergrund analysiert der Beitrag sieben empirische Untersuchungen und ordnet deren Hauptergebnisse in den empirischen Kontext bezüglich des Selbstdatenschutzes ein.

Grundsätzlich scheinen Nutzende motiviert zu sein, die eigene Online-Privatsphäre zu schützen, wobei einfach anzuwendende Schutzmaßnahmen häufiger anzutreffen sind als komplexere Strategien. Des Weiteren deuten die Studien darauf hin, dass das individuelle Schutzverhalten bzw. die Schutzmotivation von einer Vielzahl psychologischer Faktoren beeinflusst wird. Einen besonders großen Einfluss hat dabei die Wahrnehmung von Risiken für die Selbstbestimmung, wobei auch weitere Variablen einen positiven Einfluss auf die Umsetzung des Selbstdatenschutzes haben, wie zum Beispiel die empfundene Effizienz der Schutzmaßnahmen, ein Bedürfnis nach höherem Privatheitsschutz oder eine ausgeprägte Privatheitskompetenz. Allerdings gibt es auch Faktoren, die sich negativ auf das Schutzverhalten auswirken können, wie zum Beispiel Resignation, also der Glaube, dass Maßnahmen nicht zu mehr Selbstbestimmung führen können. Schließlich deuten einige Ergebnisse der Untersuchungen darauf hin, dass Transparenz ein probates Mittel für ein bewussteres Verhalten im Netz sein kann. Dabei hat sich als wichtig herausgestellt, dass relevante Informationen möglichst kurz gehalten werden müssen, um die Nutzenden nicht zu überfordern. Besonders förderlich für Schutzverhalten sind außerdem Informationen darüber, welche Privatheitsrisiken bestehen und wie man diese effektiv vermeiden kann. Vor dem Hintergrund der zusammengetragenen Ergebnisse folgern die Autorinnen und Autoren, dass es besonders sinnvoll ist, an die Nutzenden Wissen zu vermitteln, welche negativen Konsequenzen ihre Verhaltensweisen im Netz haben können und wie man sich wirksam vor negativen Folgen schützen kann.

Der Beitrag von *Heesen, Ammicht Quinn, Baur, Hagendorff* und *Stapf* diskutiert anschließend aus ethisch-philosophischer Perspektive die Bedeutung des Konzepts Privatheit für individuelle Freiheit, Selbstverwirklichung und demokratische Teilhabe. Es wird dargestellt, dass in einer datafizierten Gesellschaft das private, individuelle Handeln durch umfassende Datenerhebungen abgebildet und für das politische Handeln fruchtbar gemacht werden kann. Auf diesem Wege können individuelle und private Handlungen durch ihre technische Verdichtung und Auswertung zu überindividuellen und öffentlichen Strukturbedingungen werden. Der Beitrag verdeutlicht, dass – trotz der Schutzwürdigkeit einer privaten Sphäre – private, individuelle Handlungen nicht zum bestimmenden Maßstab politischen Handelns werden dürfen. Dabei werden Argumente aus Demokratietheorie, Technokratiedebatte sowie Probleme der Widersprüche von Wertüberzeugungen und individueller Handlungspraxis (value-action gap) diskutiert. Vor diesem Hintergrund wird der Forschungsstand moderner Privatheitstheorien anhand einer Unterscheidung zwischen ihren individuellen und

überindividuellen Dimensionen systematisiert. Die Beispiele Clouddienste und Medienmündigkeit vertiefen und veranschaulichen die Bedeutung von Privatheit und informationeller Selbstbestimmung für den Schutz der Demokratie.

Gestaltung von technischem und gesellschaftlichem Wandel

Der vierte Teil des Buchs befasst sich schließlich damit, wie dem soziotechnischen Wandel durch die zunehmende Digitalisierung und den dadurch entstehenden Herausforderungen für Datenschutz und Selbstbestimmung begegnet werden kann.

Neue digitale Technologien rufen grundlegende gesellschaftliche und soziale Veränderungen hervor und sind sowohl Auslöser für einen umfassenden sozioökonomischen und institutionellen Wandel als auch Nebenfolge sich ändernder gesellschaftlicher Zusammenhänge, Praktiken und Normen. Der zunehmende Umfang von gesammelten Daten sowie der Grad der Vernetzbarkeit und der Analysemöglichkeiten lassen einen digitale Fußabdruck einer Person entstehen, der im Zentrum des Kapitels von *Conrad, Kreutzer, Mittermeier, Schreiber* und *Simo* steht. Sie skizzieren zunächst die drei miteinander verschränkten technischen Trends, die bei der Entstehung und Nutzung digitaler Fußabdrücke relevant sind, nämlich die Hyperkonvergenz der Informationstechnologie, deren Hyperkonnektivität sowie das Entstehen von immer mehr dynamischen Informations-Ökosystemen. Um gezielt Gestaltungsvorschläge für privatheitsfreundliche Systeme machen zu können, so die weitere Argumentation, müssen zunächst Angriffs- und Bedrohungspotenziale, die aus diesen Trends entstehen, betrachtet werden. Diese werden an Hand von vier Beispielen erläutert: dem Datenschutz 1) im Domain Name System, 2) bei mobilen Diensten wie Dating-Apps und Lern-Apps, 3) bei vernetzten smarten Objekten wie Smart-TVs oder Smart Cars sowie 4) in öffentlichen freien WLANs. Die Beispiele illustrieren das grundsätzliche Spannungsverhältnis zwischen dem Innovationspotential von Digitalisierung und den wirtschaftlichen Interessen von Unternehmen auf der einen sowie den Privatheitsinteressen der Nutzenden auf der anderen Seite. Dieses Spannungsverhältnis spiegelt auch der bestehende rechtliche Rahmen wider. Es wird anschließend argumentiert, dass Innovation und Privatheit durchaus vereinbar sind, beispielsweise, wenn geeignete „Privacy-Enhancing Technologies“ (PETs) entwickelt und genutzt werden. Wie dies aussehen kann, zeigen drei konkrete technische Umsetzungsbeispiele: „Me&MyFriends“ ist ein

Selbstbewertungstool für Nutzende, das es ermöglicht, auf Basis von transparent gemachten Beziehungsgraphen detailliertes Wissen über hinterlassene digitale Spuren bei der Nutzung von Online Social Media zu erlangen. „WallGuard" dient der präventiven Erkennung von Social-Media-Beiträgen, die möglicherweise ein späteres Bereuen nach sich ziehen könnten. „MetaMiner" ist schließlich ein nutzerzentriertes Framework, das eine Verbesserung der Transparenz über die Netzwerkinteraktionen des mobilen Geräts ermöglicht. Gemeinsam ist allen drei Gestaltungsvorschlägen, dass sie verdeutlichen, wie wirkungsvoll Transparenz über den persönlichen digitalen Fußabdruck für den Schutz der informationellen Selbstbestimmung sein kann.

Der abschließende Beitrag von *Hansen, Bieker* und *Bremert* erläutert die Aspekte des Schutzes von Privatheit und Selbstbestimmung durch Systemgestaltung. Ausgangspunkt ist der Risikobegriff als zentraler Bestandteil und wesentliche Neuerung im harmonisierten Datenschutzrecht, der zugleich den Maßstab für die Anforderungen an die Systemgestaltung darstellt. Der sogenannte risikobasierte Ansatz ist dabei nicht nur für eine Betrachtung der Datenschutzrisiken der betroffenen Personen maßgeblich, sondern erfordert eine umfassende Berücksichtigung sämtlicher aus Datenverarbeitungsvorgängen resultierenden Risiken für die Rechte und Freiheiten natürlicher Personen.

Eine solche Beurteilung setzt voraus, dass die Verantwortlichen die spezifischen Grundrechtsrisiken ihrer Datenverarbeitungsvorgänge identifizieren können. Daher stellt der Beitrag einen Ansatz der Risikoerkennung vor, der auf einer systematischen Darstellung der jeweiligen Datenverarbeitung aufbaut und diese mit einer zeitlichen Systematisierung möglicher Grundrechtsausübung verknüpft, die eine solche Risikoerkennung für die Verantwortlichen erleichtern kann. Sodann werden die maßgeblichen Kriterien für die Bewertung der Risiken vorgestellt. Hierbei kommt es auf die Art, den Umfang, die Umstände und die Zwecke der jeweiligen Verarbeitung personenbezogener Daten an. Auf der Grundlage der so erkannten und bewerteten Risiken können Verantwortliche im Vorfeld einer Datenverarbeitung eine datenschutzkonforme Systemgestaltung sicherstellen. Dies umfasst sowohl die Umsetzung der Anforderungen an Datenschutz durch Technikgestaltung, d. h. die Implementierung technischer und organisatorischer Maßnahmen auf Grundlage der erkannten Risiken und Datenschutzgrundsätze, als auch die Berücksichtigung datenschutzfreundlicher Voreinstellungen.

Zuletzt werden Spannungsfelder datenschutzrechtlicher Sachverhalte angesprochen. Die Querverbindungen und Auswirkungen datenschutzfreundlicher Verarbeitungsverfahren auf etwa Aspekte der Informationsfreiheit (im

Kontext öffentlicher Stellen), des Umweltschutzes, des Datenzugangs und des Kartellrechts werden beleuchtet. Mit einer Folgenabschätzung sowie einer frühzeitigen und systematischen datenschutzfreundlichen Systemgestaltung lassen sich in der Regel Lösungen finden, die sämtliche Anforderungen in ausreichendem Maße berücksichtigen.

Alexander Roßnagel
Michael Friedewald

Literatur

Buchmann, J. (Hrsg.). (2012). *Internet Privacy: Eine multidisziplinäre Bestandsaufnahme / A multidisciplinary analysis*. Acatech Studie. Springer.

Bundesverfassungsgericht. (15. Dez. 1983). Urteil des Ersten Senats vom 15. Dezember 1983 – 1 BvR 209/83 – („Volkszählungsurteil"). *BVerfGE 65,* 1–71. http://www.bverfg.de/e/rs19831215_1bvr020983.html.

Friedewald, M., Kreutzer, M., & Hansen, M. (Hrsg.). (2021). *Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg*. DuD-Fachbeiträge. Springer Vieweg. https://doi.org/10.1007/978-3-658-33306-5.

Karaboga, M. (2018). „The emergence and analysis of european data protection politics". In: J. Schwanholz, T. S. Graham, & P.-T. Stoll (Hrsg.), *Managing democracy in the digital age. Internet regulation, social media use, and online civic engagement*. Springer International.

Ochs, C., et al. (Hrsg.). (2019). *Die Zukunft der Datenökonomie. Digitales Leben zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz*. Medienkulturen im digitalen Zeitalter. Springer VS. https://doi.org/10.1007/978-3-658-27511-2.

Roßnagel, A. (Hrsg.). (2017). *Europäische Datenschutz-Grundverordnung: Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts*. Nomos.

Roßnagel, A., Bile, T., et al., (Jan. 2018). *Nationale Implementierung der Datenschutz-Grundverordnung: Herausforderungen – Ansätze – Strategien*. Policy Paper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. https://www.forum-privatheit.de/forum-privatheit-de/publikationen-nd-downloads/veroeffentlichungen-des-forums/positionspapiere-policy-paper/Policy-Paper-Nationale-Implementierung-der-DSGVO_DE.pdf - Implementierung-der-DSGVO_DE.pdf.

Roßnagel, A., & Nebel, M. (Mai 2016). *Die neue Datenschutz-Grundverordnung: Ist das Datenschutzrecht nun für heutige Herausforderungen gerüstet?* Policy Paper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. https://www.forum-privatheit.de/download/die-neue-dsgvo-2016/.

Roßnagel, A., Friedewald, M., & Hansen, M. (Hrsg.). (2018). *Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung*. DuD-Fachbeiträge. Springer Vieweg.

Roßnagel, A., & Geminn, C., et al. (Nov. 2019). *Evaluation der Datenschutz-Grundverordnung*. Policy Paper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt.

Stapf, I., et al. (Hrsg.). (2021). *Aufwachsen in überwachten Umgebungen: Interdisziplinäre Positionen zur Privatheit und Datenschutz in Kindheit und Jugend*. Bd. 14. Kommunikations- und Medienethik. Nomos.

Inhaltsverzeichnis

Gestaltung von technischem und gesellschaftlichem Wandel

Herausgeber- und Autor:innenverzeichnis

Über die Herausgeber

Alexander Roßnagel ist Seniorprofessor für öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel und Sprecher des Forums Privatheit und selbstbestimmtes Leben in der digitalen Welt. Seit dem 01.03.2021 ist er Hessischer Beauftragter für Datenschutz und Informationsfreiheit.

Michael Friedewald leitet das Geschäftsfeld „Inofmations- und Kommunikationstechnik“ am Fraunhofer-Institut für System- und Innovationsforschung ISI in Karlsruhe. Er ist Koordinator des „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt“.

Autorenverzeichnis

Regina Ammicht Quinn Internationales Zentrum für Ethik in den Wissenschaften, Eberhard Karls Universität Tübingen, Tübingen, Deutschland

Andreas Baur Internationales Zentrum für Ethik in den Wissenschaften, Eberhard Karls Universität Tübingen, Tübingen, Deutschland

Felix Bieker Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Deutschland

Tamer Bile Projektgruppe verfassungsverträgliche Technikgestaltung, Universität Kassel, Kassel, Deutschland

Benjamin Bremert Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Deutschland
DZ HYP AG, Hamburg, Deutschland

Barbara Büttner Universität Kassel, Kassel, Deutschland

Bernd Conrad Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt, Deutschland

Michael Friedewald Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe, Deutschland

Christian L. Geminn Projektgruppe verfassungsverträgliche Technikgestaltung, Universität Kassel, Kassel, Deutschland

Thilo Hagendorff Internationales Zentrum für Ethik in den Wissenschaften, Eberhard Karls Universität Tübingen, Tübingen, Deutschland

Marit Hansen Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Deutschland

Jessica Heesen Internationales Zentrum für Ethik in den Wissenschaften, Eberhard Karls Universität Tübingen, Tübingen, Deutschland

Thomas Hess Institut für Digitales Management und Neue Medien, Ludwig-Maximilians-Universität München, München, Deutschland

Murat Karaboga Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe, Deutschland

Michael Kreutzer Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt, Deutschland

Nicole C. Krämer Universität Duisburg-Essen, Duisburg, Deutschland

Jörn Lamla Universität Kassel, Kassel, Deutschland

Nicholas Martin Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe, Deutschland

Christian Matt Institut für Wirtschaftsinformatik, Universität Bern, Bern, Schweiz

Yannic Meier Universität Duisburg-Essen, Duisburg, Deutschland

Judith Meinert Universität Duisburg-Essen, Duisburg, Deutschland

Johanna Mittermeier Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt, Deutschland; TU Darmstadt, Darmstadt, Deutschland

Maxi Nebel Projektgruppe verfassungsverträgliche Technikgestaltung, Universität Kassel, Kassel, Deutschland

Carsten Ochs Universität Kassel, Kassel, Deutschland

Fabian Pittroff Universität Kassel, Kassel, Deutschland

Alexander Roßnagel Hessischer Beauftragter für Datenschutz und Informationsfreiheit; Projektgruppe verfassungsverträgliche Technikgestaltung, Universität Kassel, Kassel, Deutschland

Linda Schreiber Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt, Deutschland

Hervais Simo Fhom Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt, Deutschland

Ingrid Stapf Internationales Zentrum für Ethik in den Wissenschaften, Eberhard Karls Universität Tübingen, Tübingen, Deutschland

Mena Teebken Institut für Digitales Management und Neue Medien, Ludwig-Maximilians-Universität München, München, Deutschland

Verena Thürmel Institut für Digitales Management und Neue Medien, Ludwig-Maximilians-Universität München, München, Deutschland

Markus Uhlmann Universität Kassel, Kassel, Deutschland

Die europäische Datenschutz-Grundverordnung: Privatheit im Kontext von Regulierung der digitalen Welt

Neue Konzepte für den Grundrechtsschutz in der digitalen Welt

Alexander Roßnagel, Tamer Bile, Christian L. Geminn und Maxi Nebel

Die globale Digitalisierung nahezu aller Lebensbereiche gefährdet zunehmend die individuelle und demokratische Selbstbestimmung und erfordert umso stärker ihren normativen Schutz. Doch die Bedingungen für diesen Schutz haben sich radikal geändert. Konzepte, Institutionen und Instrumente, die für diesen Schutz in den 1970er Jahren für die Gefährdung durch kommunale Gebietsrechenzentren entworfen wurden, genügen nicht mehr für den Schutz gegenüber globalen digitalen Infrastrukturen, die das alltägliche Leben bestimmen. Der Beitrag analysiert die Herausforderungen für das Grundrecht auf Datenschutz und informationelle Selbstbestimmung (1), untersucht das aktuelle Schutzkonzept der Datenschutz-Grundverordnung und seine Governance-Struktur (2), diskutiert

A. Roßnagel
Hessischer Beauftragter für Datenschutz und Informationsfreiheit;
Projektgruppe verfassungsverträgliche Technikgestaltung,
Universität Kassel, Kassel, Deutschland
E-Mail: a.rossnagel@uni-kassel.de

T. Bile · C. L. Geminn (✉) · M. Nebel
Projektgruppe verfassungsverträgliche Technikgestaltung,
Universität Kassel, Kassel, Deutschland
E-Mail: c.geminn@uni-kassel.de

T. Bile
E-Mail: t.bile@uni-kassel.de

M. Nebel
E-Mail: m.nebel@uni-kassel.de

A. Roßnagel und M. Friedewald (Hrsg.), *Die Zukunft von Privatheit und Selbstbestimmung,* DuD-Fachbeiträge,
https://doi.org/10.1007/978-3-658-35263-9_1

Schutzverbesserungen in dem neugeschaffenen Regelungsumfeld (3) und erörtert mögliche neue Konzepte und Instrumente zum Grundrechtsschutz in der globalen digitalen Transformation (4).

1 Herausforderungen für die Grundrechte auf Datenschutz und Selbstbestimmung

Seit der Erkenntnis der Grundrechtsrelevanz von Datenverarbeitung[1] und der Verabschiedung der ersten Datenschutzgesetze in den 70er Jahren[2] haben sich die Grundrechtsrisiken radikal verändert und ausgeweitet. Dennoch ist das grundlegende Konzept zur Gewährleistung von Datenschutz weitgehend unverändert.

1.1 Datenschutz und Selbstbestimmung

1983 konkretisierte das Bundesverfassungsgericht die Grundrechte auf Persönlichkeitsschutz nach Art. 2 Abs. 1 GG und auf Menschenwürde nach Art. 1 Abs. 1 GG angesichts der elektronischen Datenverarbeitung zum Grundrecht auf informationelle Selbstbestimmung.[3] Dieses gewährt jeder Person die Befugnis, selbst darüber zu bestimmen, wer welche sie betreffenden Daten zu welchem Zweck verarbeiten darf. In dieses Grundrecht darf ein Datenverarbeiter nur mit informierter Einwilligung der betroffenen Person oder aufgrund einer gesetzlichen Regelung eingreifen, die die Datenverarbeitung eindeutig, bereichsspezifisch und mit ausreichenden Schutzvorkehrungen erlaubt.

Dieses Grundrechtsverständnis wurde von der 2009 in Kraft getretenen Grundrechtecharta der Europäischen Union übernommen und präziser ausgestaltet.[4] Art. 7 GRCh enthält vier Gewährleistungen, nämlich des Privatlebens, des Familienlebens, der Wohnung und der Kommunikation. Die Gewährleistungen des Privatlebens und der Kommunikation schützen wesent-

[1] Z. B. Steinmüller, Lutterbeck u. a (1971).

[2] Das erste Datenschutzgesetz der Welt trat am 13.10.1970 in Hessen in Kraft – s. GVBl. (1970, S. 625). Das Bundesdatenschutzgesetz – BGBl. I (1977, S. 201) – gilt seit dem 01.01.1978.

[3] BVerfGE 65, 1 (42 ff.) – ständige Rechtsprechung.

[4] S. zum Folgenden näher Roßnagel (2019a, S. 1 f).

lichen Aspekte der Selbstbestimmung über das eigene Verhalten und dessen Beobachtung durch Dritte.[5]

Art. 8 GRCh schützt speziell die Entscheidungsbefugnis des Betroffenen über seine personenbezogenen Daten.[6] Nach Abs. 1 hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Soweit private Daten verarbeitet werden, erstreckt sich auch die Achtung des Privatlebens nach Art. 7 GRCh auf diesen Schutz. Da der Datenschutz allerdings weiter reicht als die Achtung des Privatlebens,[7] wurde dafür ein eigenständiges Grundrecht begründet. Abs. 2 Satz 2 fordert die Zweckbindung der Datenverarbeitung und gewährt einen Auskunfts- und Berichtigungsanspruch. Abs. 3 bestimmt, dass eine unabhängige Stelle den Datenschutz zu überwachen hat.

Der grundrechtliche Datenschutz in Art. 7 und 8 GRCh und der grundrechtliche Datenschutz nach Art. 2 Abs. 1 und Art.1 Abs. 1 GG haben im Wesentlichen den gleichen Schutzgehalt, nämlich die freie Selbstbestimmung der jeweils betroffenen Person über den Umgang mit den sie betreffenden Daten zu schützen.[8] Jede Datenverarbeitung, die diese Selbstbestimmung ignoriert, greift in die genannten Grundrechte ein.[9] Für die Bestimmung des Eingriffs kommt es nicht auf die Person an, die den Eingriff vornimmt – auch nicht auf deren Charakterisierung als privat oder staatlich.[10]

Um diese Grundrechte umzusetzen, verfolgt das Datenschutzrecht seit Beginn ein Schutzprogramm, das im Wesentlichen auf folgenden Grundsätzen beruht: Die Datenverarbeitung muss der betroffenen Person transparent sein, weil sie nur dann überprüfen kann, ob die Datenverarbeitung rechtmäßig ist, und ihre Rechte

---

[5] S. z. B. Bernsdorff, in: Meyer und Hölscheidt (2019), Art. 7 Rn. 15 und 20 und Art. 8 Rn. 13; Johannes, in Roßnagel (2018b), § 2 Rn. 60.

[6] EuGH, C-291/12 – ECLI:EU:C:2013:670, Rn. 24 ff., 55 – Schwarz; EuGH, C-293/12 und 594/12 – ECLI.EU:C:2014:238, Rn. 34 ff., 47, 55 – Digital Rights Ireland; EuGH, C-362/14 – ECLI.EU:C:2015:650, Rn. 38 ff., 47, 55 – Schrems; s. Kingreen, in Calliess und Ruffert (2016), Art. 8 GRCh Rn. 1, 9.

[7] S. hierzu Geminn und Roßnagel (2015, S. 703 ff.).

[8] S. z. B. Kingreen, in Calliess und Ruffert (2016), Art. 7 GRCh Rn. 4 und 10, Art. 8 GRCh Rn. 9; Bernsdorff, in: Meyer und Hölscheidt (2019), Art. 8 Rn. 13 f. mwN; Johannes, in Roßnagel (2018b), § 2 Rn. 68 ff.

[9] S. näher Roßnagel (2019a, S. 2 f.).

[10] EuGH, C-101/01, ECLI:EU:C:2003:596, Rn. 86 – Lindquist; EuGH, C 131/12, ECLI:EU:C:2014:317, Rn. 68 – Google Spain; EuGH, C-362/14, ECLI:EU:C:2015:650, Rn. 93 – Schrems; BVerfGE 84, 192 (195); 117, 202 (229); Roßnagel, Pfitzmann u. a. (2001, S. 48 ff.).

wahrnehmen kann. Die Verarbeitung personenbezogener Daten darf nur zu einem bestimmten Zweck erfolgen und ist auf diesen Zweck begrenzt. Sie muss erforderlich sein, um diesen Zweck zu erreichen, und die Verwendung personenbezogener Daten möglichst vermeiden. Informationelle Selbstbestimmung ist nur möglich, wenn die betroffene Person Mitwirkungsmöglichkeiten hat und Einfluss auf die Datenverarbeitung nehmen kann. Daher stehen ihr Rechte auf Auskunft, Korrektur und Widerspruch zu. Außerdem erfordert sie die flankierende Aufsicht unabhängiger Datenschutzkontrolleinrichtungen.[11] Dieses grundlegende Konzept zur Gewährleistung der Grundrechte wurde seit seiner Einführung kaum verändert. Jedoch hat sich die Datenverarbeitung, gegen deren Risiken es schützen soll, radikal gewandelt und ausgeweitet.

1.2 Neue Herausforderungen durch die Digitalisierung

Als solche Herausforderungen stellen sich vor allem die Zunahme personenbezogener Daten durch vielfältige neue Datenquellen, das Entstehen neuer Infrastrukturen, die diese Datenquellen vernetzen und die personenbezogenen Daten zusammenführen, und schließlich neue Verfahren, die diese riesigen Datenmengen aus unterschiedlichsten Quellen auswerten können.

Neue Datenquellen führen zu einer explosionsartigen Zunahme personenbezogener Daten. Viele Alltagsumgebungen und Alltagsgegenstände werden mit „intelligenter“ und vernetzter Informationstechnik ausgestattet. Ubiquitous Computing mit seinen Ausprägungen wie z. B. Smart Cars,[12] Smart Health,[13] Smart Home,[14] Smarten Assistenten,[15] vernetzten Robotern,[16] Smart TV[17] und sonstigen Techniken des Internet der Dinge erfasst die Umgebung der Dinge und der Menschen durch vielfältige Sensoren.[18] Auf der Grundlage dieser Daten und daraus erstellter Profile sowie der Lernfähigkeit der Systeme durch Künstliche

[11] BVerfGE 65, 1 (S. 43 ff.).

[12] S. z. B. Roßnagel und Hornung (2019), Roßnagel, Geminn u. a. (2016, S. 2 ff.).

[13] S. z. B. Jandt (2016, S. 571 ff.), Dochow (2017).

[14] S. z. B. Skistims (2016), Geminn (2016, S. 575 ff.).

[15] S. z. B. Knote u. a. (2020, S. 118 ff.).

[16] S. z. B. Keßler (2017, S. 589 ff.).

[17] S. Forum Privatheit (2016b).

[18] S. z. B. Forum Privatheit (2015), Hornung (2018, S. 315 ff.), Geminn (2017, S. 295 ff.).

Intelligenz passen sich diese Techniksysteme ihren Nutzerinnen und Nutzern an und erleichtern ihnen das Alltags- oder das Berufsleben. Diese Techniken erheben personenbezogene Daten, ohne dass das Individuum sie eingibt – einfach aufgrund schlichten Verhaltens in einer technikgeprägten Umgebung. Auf diese Weise werden unbemerkt viele Lebensregungen in der körperlichen Welt dem digitalen Zugriff zugänglich. Die allgegenwärtige Verarbeitung personenbezogener Daten erfasst potenziell alle Lebensbereiche nahezu vollständig.[19] Die damit verbundenen Risiken gehen die Nutzenden in der Regel freiwillig ein. In der individuellen Abwägung überwiegt meist der erhoffte unmittelbare Vorteil die zeitlich fernliegenden abstrakten Risiken eines Missbrauchs.

In der digitalen Welt ist die Nutzung von *virtuellen Infrastrukturen* wie Such-,[20] Speicher- und Nachrichtendienste, Cloud Computing[21] sowie Social Media[22] und andere Austauschplattformen lebensnotwendig.[23] Da sie für ihr Funktionieren personenbezogene Daten verarbeiten müssen, können sie diese Datenverarbeitung nicht von unterschiedlichen individuellen Einwilligungen abhängig machen. Die individuelle Selbstbestimmung ist letztlich reduziert auf das grundsätzliche „Ja“ oder „Nein“ zum digitalen Leben. Diese Infrastrukturen erzeugen einen eigenen virtuellen Sozialraum, in den nahezu alle Aktivitäten aus der körperlichen Welt übertragen wurden. In diesem hinterlässt jede Handlung Datenspuren, deren Erhebung und – letztlich weltweite – Verbreitung und Verwendung die betroffene Person nicht kontrollieren kann.[24] Den damit verbundenen Risiken zu entgehen, würde voraussetzen, den virtuellen Sozialraum zu meiden – für viele keine realistische Alternative.[25] Es besteht ein virtueller „Anschluss- und Benutzungszwang“.[26] Gegenüber diesem Zwang gibt es kaum Protest. Denn viele Infrastrukturleistungen werden „umsonst“ angeboten. Wer sie nutzt, zahlt zwar kein Geld, dafür aber werden die personenbezogenen Daten zu umfassenden Profilen verarbeitet, die für personalisierte Werbung und Dienstleistungen genutzt

[19] S. hierzu näher bereits Roßnagel (2007).

[20] S. z. B. Eifert (2017, S. 1450 ff.).

[21] S. z. B. Hofmann (2018, S. 293 ff.).

[22] S. z. B. Nebel (2020), Nocun (2018, S. 39), Rothmann (2018, S. 59).

[23] S. z. B. Forum Privatheit (2017c), Schnabel (2009).

[24] S. z. B. Forum Privatheit (2018a).

[25] Für viele sind auch Praktiken des Selbstdatenschutzes keine praktikable und durchgängig funktionierende Alternative, s. Forum Privatheit (2014).

[26] S. Roßnagel (2018a, S. 364 f.).

werden.[27] Die personalisierten Dienstleistungen der Infrastrukturen werden über den gesamten Tagesablauf hinweg in die individuellen Handlungsabläufe integriert und unmerklich Teil des Verhaltens und Handelns.[28]

Die dritte relevante Entwicklungslinie sind neue Auswertungsmöglichkeiten für die riesigen Datenmengen, die u. a. durch die allgegenwärtige Datenverarbeitung und virtuelle Infrastrukturen entstehen: *Big Data*[29] und *Künstliche Intelligenz*[30] durch lernfähige Systeme. Beide Auswertungsformen führen auf unterschiedliche Weise entweder zu sehr präzisen Persönlichkeitsprofilen oder zu Mustern individueller und kollektiver Eigenschaften, die ermöglichen, das Verhalten von Menschen und Gruppen zu prognostizieren und zu steuern.[31] Personenbezogene Auswertungen sind die Grundlage einer gezielten Verhaltensbeeinflussung durch Microtargeting. Abstrakte Muster können dazu dienen, Lagen und Situationen besser zu beurteilen oder deren Entwicklung zu prognostizieren. Auch wer keine Daten preisgegeben hat, ist im Algorithmus der Statistik gefangen. Sie führt zu einer anonymen Vergemeinschaftung, der niemand entgehen kann. Diese Muster wirken durch die Normativität der Normalität, die sie beschreiben, verhaltensbestimmend, selbst wenn sie keine personenbezogenen Daten enthalten, und beschränken damit die individuelle und kollektive Selbstbestimmung.[32]

1.3 Aushöhlung des Schutzkonzepts

Die beschriebenen Entwicklungen höhlen das Schutzkonzept des Datenschutzes und der Selbstbestimmung aus, weil sie nur dann umsetzbar sind, wenn sie dessen Vorgaben ignorieren.

Soweit die betroffene Person digitale Infrastrukturen nutzen muss, um am gesellschaftlichen oder wirtschaftlichen Leben teilzunehmen, sieht sie sich durch

[27] S. hierzu Kugelmann (2016, S. 566 ff.).

[28] S. näher Roßnagel (2014, S. 78 ff.).

[29] Richter (2015), Richter, in Jandt und Steidle (2018, 308 ff.), Hoffmann-Riem (2018).

[30] Forum Privatheit 2020b.

[31] S. z. B. Richter (2016, S. 581), Roßnagel und Nebel (2015, S. 458), Roßnagel, Geminn u. a. (2016, S. 21 ff.).

[32] S. Weichert (2013, S. 258), Roßnagel (2013, S. 566).

die Techniknutzung einem faktischen Zwang zur Datenpreisgabe ausgesetzt.[33] Soweit keine wirklichen Alternativen bestehen, ist die individuelle *Einwilligung* ein inhaltsleerer Formalismus.[34] Auch die Fülle und Vielfalt der Verarbeitungsvorgänge mit zahllosen impliziten (Mini-)Interaktionen und die Vielzahl von Verantwortlichen, die Daten unter sich austauschen, schließen gehaltvolle Entscheidungen der betroffenen Person aus.[35] Für Big Data-Analysen und das Trainieren lernfähiger Systeme ist es ausgeschlossen, dass die vielen – oft Millionen – betroffenen Personen vorher um ihre Einwilligung gebeten werden.

Der Gewährleistung von *Transparenz* stößt in der digitalen Welt aufgrund der Vielfalt und Komplexität allgegenwärtiger Datenverarbeitung an subjektive und objektive Grenzen. Zudem soll „smarte" Informationstechnik gerade im Hintergrund und damit unmerklich den Menschen bei vielen Alltagshandlungen unterstützen. Die betroffenen Personen wissen daher nie, ob und wenn ja welche Handlungen von ihnen beobachtet und registriert und welche Datensammlungen zusammengeführt werden, müssen damit aber ständig rechnen.[36]

Der Grundsatz der *Zweckbindung* widerspricht sowohl der Idee einer unbemerkten, komplexen und spontanen technischen Unterstützung der betroffenen Person als auch dem Ziel, durch das Zusammenführen und Auswerten möglichst vieler Daten aus vielfältigen Quellen neue Erkenntnisse zu gewinnen.[37] Je vielfältiger und umfassender die zu erfassenden Alltagshandlungen und je unterschiedlicher die Datenquellen sind, umso schwieriger wird es, den Zweck einzelner Datenverarbeitungen vorab festzulegen und die Datenverarbeitung auf diesen zu begrenzen.[38] Sollen „smarte" Informationstechniken die Nutzenden in allen Situationen unterstützen, können sie nicht auf einen bestimmten Zweck begrenzt werden.[39] Sollen durch Big Data-Auswertungen neue Korrelationen erkannt und aus diesen neue Erkenntnisse gewonnen werden, widerspricht dies diametral jeder Zweckbindung.[40]

---

[33] S. auch Roßnagel, in Simitis, Hornung u. a. (2019), Art. 5 DSGVO Rn. 40 ff.

[34] Zur Kritik am Konzept der Einwilligung s. z. B. Forum Privatheit (2020a), Kamp und Rost (2013, S. 80), Roßnagel (2016, S. 563).

[35] S. hierzu Roßnagel, Geminn u. a. (2016, S. 102 f.).

[36] S. hierzu Roßnagel, in Simitis, Hornung u. a. (2019), Art. 5 DSGVO Rn. 61 f.

[37] S. zum Folgenden Roßnagel, in Simitis, Hornung u. a. (2019), Art. 5 DSGVO Rn. 112 ff.

[38] S. hierzu Forum Privatheit (2019a, S. 10), Martini (2014, S. 1481), Roßnagel, Geminn u. a. (2016, S. 102 f.), Geminn (2017, S. 295).

[39] S. z. B. Roßnagel (2016, S. 564).

[40] S. Richter (2016, S. 583).

Die Grundsätze der *Datenminimierung,* der Speicherbegrenzung und der Datensparsamkeit sind an den jeweils begrenzten Zweck gebunden.[41] Ebenso wie der Grundsatz der Zweckbindung werden auch diese Grundsätze ihre Steuerungskraft verlieren.[42] Wenn der Zweck der Datenverarbeitung ohne wirkliche Grenzen ist, führt auch die Frage, welche Datenverarbeitung für diesen Zweck erforderlich ist oder wie der Zweck mit möglichst wenig personenbezogenen Daten erreicht werden kann, nicht mehr zu einer überschaubaren Eingrenzung erlaubter Datenverarbeitung. Alle Systeme, die kontextsensitiv die betroffene Person entlasten oder unterstützen sollen, die Präferenzen der Nutzenden erkennen und ihnen gerecht werden sollen oder allgemein alle Assistenzsysteme, die sich selbstlernend verbessern und an ihre Nutzenden und ihre Umgebung anpassen sollen, können ihre Funktionen nur richtig erfüllen, wenn sie diese Grundsätze ignorieren.[43]

Die betroffene Person hat zwar eine Reihe von *Auskunfts- und Mitwirkungsrechten.* Ihr wird es jedoch aufgrund der umfangreichen, vielfältigen, unmerklichen, komplexen und zersplitterten Verarbeitung ihrer Daten faktisch kaum möglich sein, diese Rechte als Individuum gezielt und effektiv zu nutzen. Vielfach wird sie nicht einmal in der Lage sein, die vielen Verantwortlichen zu identifizieren.[44]

Im Ergebnis werden die Grundrechte auf Datenschutz und informationelle Selbstbestimmung aufgrund zunehmender Machtasymmetrien aufgrund gesteigerter Wissensmacht immer wichtiger, zugleich verliert das überkommene Konzept des Datenschutzes aber an Umsetzungspotenzial. Es bietet kaum noch ausreichende und wirksame Schutzmechanismen gegen die spezifischen Herausforderungen der neuen Technikentwicklungen. Dieser Prozess führt nicht nur zu einem weiteren Datenschutzproblem, sondern zur Infragestellung des gesamten Konzepts des bisherigen Datenschutzes.

[41] S. Forum Privatheit (2017b).

[42] S. hierzu auch Roßnagel, in Simitis, Hornung u. a. (2019), Art. 5 DSGVO Rn. 134 ff. und 165 ff.

[43] S. Pallas (2018, S. 17 ff.), Roßnagel und Nebel (2015, S. 458).

[44] S. hierzu auch Geminn (2020, S. 307).

2 Neue Governance-Strukturen: Ko-Regulierung in der Europäischen Union

Neben den Herausforderungen für Datenschutz und Selbstbestimmung hat sich auch der normative Rahmen für das Konzept zum Schutz dieser Grundrechte durch die Einführung der Datenschutz-Grundverordnung geändert. Um erkennen zu können, ob die neuen Unionsregelungen diesen Herausforderungen gerecht werden, untersucht dieser Abschnitt die Zielsetzungen, die inhaltlichen Regelungen und die Governance-Struktur dieser Verordnung.

2.1 Datenschutz-Grundverordnung

Seit dem 25. Mai 2018 gilt die Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO) unmittelbar in der gesamten Europäischen Union und im Europäischen Wirtschaftsraum. Sie ist in allen Mitgliedstaaten anwendbar und Teil ihrer jeweiligen Rechtsordnung. Gegenüber dem nationalen Datenschutzrecht genießt sie Anwendungsvorrang.[45]

Die Datenschutz-Grundverordnung löst die Datenschutz-Richtlinie 95/46/EG aus dem Jahr 1995 ab, deren Datenschutzkonzept auf das deutsche Datenschutzrecht der 1980er Jahre zurückgeht[46] Als Richtlinie galt sie nicht unmittelbar, sondern forderte von den Mitgliedstaaten, nationale Datenschutzgesetze im Einklang mit ihren Zielen zu erlassen. Diese Datenschutzgesetze enthielten viele unterschiedliche Detailregelungen und führten zu uneinheitlichen Datenschutzniveaus in den Mitgliedstaaten. Nach langen Vorbereitungen wurde die Datenschutz-Grundverordnung nach einem mehr als vierjährigen kontroversen Gesetzgebungsprozess am 27. April 2016 erlassen.[47] Sie ist das Ergebnis vielfältiger Kompromisse zwischen den Gesetzgebungsorganen der Europäischen Union, der Kommission, dem Parlament und dem Rat, und einem bis dahin nicht bekannten Lobbyeinfluss.

Die Datenschutz-Grundverordnung orientiert sich in weiten Teilen an den alten Zielen und Grundsätzen der Datenschutz-Richtlinie. Sie übernimmt unter anderem in Art. 2 und 3 DSGVO die Regelungen zum sachlichen und räum-

[45] S. hierzu ausführlich Roßnagel, in ders. (2018b, S. 31 ff. und 41 ff.).

[46] Ausführlich Roßnagel, in ders. (2018b), § 1 Rn. 9.

[47] Ausführlich Roßnagel, in ders. (2018b), § 1 Rn. 15 ff.

lichen Anwendungsbereich, in Art. 5 DSGVO die Grundsätze der Datenverarbeitung, in Art. 6 Abs. 1 DSGVO die Voraussetzungen für die Zulässigkeit der Datenverarbeitung und in Art. 9 DSGVO die Regelungen zu besonderen Kategorien personenbezogener Daten. Hinsichtlich der Rechte der betroffenen Person orientiert sie sich in den Art. 12 bis 23 DSGVO ebenfalls stark an der Richtlinie. In Art. 28 und 29 DSGVO greift die Datenschutz-Grundverordnung grundsätzlich auf die Vorgaben der Richtlinie zur Auftragsverarbeitung zurück. In Art. 32 DSGVO übernimmt sie die Anforderungen an die Datensicherheit, in Art. 44 bis 50 DSGVO die Grundsätze zur Datenübermittlung in Drittländer und in Art. 51 bis 59 DSGVO die Konzeption der Stellung und Aufgaben der Aufsichtsbehörden. In allen Fällen sind die Regelungen der Verordnung nahezu oder wortwörtlich an den Konzeptionen der Datenschutz-Richtlinie ausgerichtet. Die Regelungen werden in der Verordnung zwar teils präzisiert, neugestaltet oder erweitert, aber konzeptionell nicht weiterentwickelt.[48]

2.2 Harmonisierung

Mit den Regelungen der Verordnung verfolgt der Unionsgesetzgeber gemäß der Erwägungsgründe 7 und 13 DSGVO das Ziel, einen „kohärenten und klar durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union“ herzustellen, „ein gleichmäßiges Datenschutzniveau“ zu gewährleisten und „Unterschiede, die den freien Verkehr personenbezogener Daten im Binnenmarkt behindern könnten“, zu beseitigen.[49] Für diese Harmonisierung verfolgte die Kommission mit ihrem Entwurf ein sehr ehrgeiziges Regelungskonzept. Durch die Wahl einer Verordnung statt einer Richtlinie wollte sie den Mitgliedstaaten die für alle Bereiche der digitalen Gesellschaft höchst relevante Regelungsmaterie des Datenschutzes nehmen. An die Stelle der unterschiedlichen nationalen Gesetze sollte ein unionsweit einheitliches Datenschutzgesetz treten. Trotz der hohen Komplexität des Datenschutzes in allen Lebensbereichen in den damals 28 Mitgliedstaaten sah sie nur ca. 50 Artikel mit materiellen Vorschriften vor. Im Gegensatz dazu versuchte z. B. das Datenschutzrecht in Deutschland bis dahin den Regelungsanforderungen des Datenschutzes in Verwaltung, Wirtschaft, Kultur, Wissenschaft und vielen weiteren Gesellschaftsbereichen dadurch

[48] S. Forum Privatheit (2016a).

[49] Zu den Zielen der DSGVO s. z. B. Forum Privatheit (2016a).

gerecht zu werden, dass es tausende bereichsspezifische Regelungen enthielt, die risikogerecht Datenschutz gewährleisten sollten. Dementsprechend sind die Regelungen der Datenschutz-Grundverordnung hochabstrakt und unterkomplex.

Diesem Mangel wollte die Kommission dadurch abhelfen, dass sie sich selbst die Kompetenz vorbehielt, die vielen unbestimmten Regelungen auszufüllen und fortzuentwickeln. Zu diesem Zweck sah ihr Entwurf 26 Ermächtigungen vor, die Verordnung durch delegierte Rechtsakte nachträglich zu konkretisieren, und 23 Ermächtigungen, sie durch Durchführungsrechtsakte auszugestalten. Dem widersprach jedoch der Rat und setzte durch, dass fast alle Ermächtigungen in Öffnungsklauseln für die Mitgliedstaaten umgewandelt wurden.[50] Im Ergebnis ermöglichen 70 Öffnungsklauseln den Mitgliedstaaten, an vielen Stellen von den Regelungen der Verordnung abzuweichen oder sie zu konkretisieren. Öffnungsklauseln können Regelungsaufträge enthalten, die die Mitgliedstaaten verpflichten, bestimmte Regelungen zu erlassen. Sie können aber auch Regelungsoptionen bieten, die den Mitgliedstaaten die Möglichkeit eröffnen, eigene Regelungen zu schaffen oder bereits bestehende Regelungen beizubehalten, sofern diese den abstrakten Vorgaben der Verordnung nicht widersprechen.[51] Eine vollständige Ersetzung des nationalen Datenschutzrechts ist in der Verordnung also nicht nur nicht angelegt, sondern im Gegenteil durch die lückenhaften und ausfüllungsbedürftigen Regelungen auch gar nicht möglich. Den Mitgliedstaaten bleibt ein vergleichsweise breiter Handlungsspielraum, unbestimmte Begriffe der Verordnung zu präzisieren, ausfüllungsbedürftige Vorgaben zu konkretisieren, unvollständige Regelungen zu ergänzen oder Regelungslücken zu schließen, solange dabei das Regelungsziel der Verordnung nicht verletzt wird. Bestehende nationale Regelungen können damit durchaus anwendbar bleiben und neue Regelungen erlassen werden.[52]

Die Datenschutz-Grundverordnung bewirkt nicht nur vielfältige unterschiedliche Abweichungen der Mitgliedstaaten, sondern überlässt ihnen im Ergebnis auch große Regelungsbereiche vollständig. Der wichtigste Bereich ist der komplette öffentliche Sektor mit allen Verwaltungsbereichen, aber auch sonstigen öffentlichen Einrichtungen wie Hochschulen und Kulturstätten. Weitere Bereiche sind alle Arbeitsverhältnisse, die Medien und die Forschung. In Deutschland wurden zwar aufgrund der Datenschutz-Grundverordnung das Bundesdaten-

[50] S. näher Roßnagel, in ders. (2018b), § 1 Rn. 15 ff.

[51] Forum Privatheit (2018c, S. 6).

[52] Forum Privatheit (2018c, S. 4).

schutzgesetz novelliert und allein im Bund Anpassungen in ca. 200 Gesetzen mit Datenschutzregelungen durch drei umfangreiche Artikelgesetze vorgenommen.[53] Doch wurden dadurch kein einziges Datenschutzgesetz und kein einziger Abschnitt zum Datenschutzrecht gestrichen. Sie gelten trotz Datenschutz-Grundverordnung weiter.

Die Datenschutz-Grundverordnung hat daher das Datenschutzrecht in Europa nicht vereinheitlicht, sondern in vielen wichtigen Bereichen die Vielfalt an unterschiedlichen Regelungen beibehalten. Aufgrund ihrer eigenen Regelungen hat sie das Ziel der Harmonisierung von Anfang an weitgehend verfehlt. In der Europäischen Union besteht kein einheitliches Datenschutzrecht, sondern eine Ko-Regulierung des Datenschutzes durch die Gesetzgeber der Union und der Mitgliedstaaten.

Die Verordnung regelt Zielsetzungen und Grundsätze, grundlegende Rechte und Pflichten und fundamentale Strukturen der Durchsetzung von Datenschutzrecht. Die Präzisierung und Ausfüllung ihrer abstrakten Regelungen und den Datenschutz in wichtigen Gesellschaftsbereichen aber bestimmen vielfach die Mitgliedstaaten. Durch diese Ko-Regulierung entsteht für den Rechtsanwender eine nur schwer zu durchschauende Gemengelage, die nicht nur zu einer erheblichen Rechtsunsicherheit führt, sondern auch eine effektive Umsetzung des Datenschutzrechts erschwert.

2.3 Modernisierung

Das zweite zentrale Ziel der Verordnung ist es, das Datenschutzrecht zu modernisieren und den Schutz der Grundrechte zu verbessern. „Rasche technologische Entwicklungen und die Globalisierung haben“ laut Erwägungsgrund 6 „den Datenschutz vor neue Herausforderungen gestellt. Das Ausmaß der Erhebung und des Austauschs personenbezogener Daten hat eindrucksvoll zugenommen. Die Technik macht es möglich, dass private Unternehmen und Behörden im Rahmen ihrer Tätigkeiten in einem noch nie dagewesenen Umfang auf personenbezogene Daten zurückgreifen. … Die Technik hat das wirtschaft-

[53] Datenschutz-Anpassungs- und -Umsetzungsgesetz EU vom 30.06.2017 (DSAnpUG-EU), BGBl. I, 2097; Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU (2. DSAnpUG-EU) vom 20.11.2019, BGBl. I, 1626; Gesetz zur Umsetzung der Richtlinie (EU) 2016/680 im Strafverfahren sowie zur Anpassung datenschutzrechtlicher Bestimmungen an die Verordnung (EU) 2016/679 vom 20.11.2019, BGBl. I, 1724.

liche und gesellschaftliche Leben verändert.“ Diese Entwicklungen erfordern nach Erwägungsgrund 7 einen „soliden, kohärenteren und durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union, um eine Vertrauensbasis zu schaffen, die die digitale Wirtschaft dringend benötigt, um im Binnenmarkt weiter wachsen zu können. Jede Person sollte die Kontrolle über ihre eigenen Daten besitzen, und private Nutzer, Wirtschaft und Staat sollten in rechtlicher und praktischer Hinsicht über mehr Sicherheit verfügen.“[54]

Überwiegend will die Datenschutz-Grundverordnung diesen neuen Herausforderungen mit den alten, schon in der Datenschutz-Richtlinie bekannten Grundsätzen und Konzepten begegnen, die bereits vor über 20 Jahren teilweise als überholt oder unzureichend galten. Sie enthält aber auch einige normative Innovationen.[55] Neu ist beispielsweise die Bestimmung des räumlichen Anwendungsbereichs der Verordnung nach dem Betroffenenprinzip in Art. 3 Abs. 2 DSGVO. Sie ist anwendbar, wenn ein Datenverarbeiter personenbezogene Daten von Personen verarbeitet, die sich in der Union aufhalten, nämlich wenn er entweder der betroffenen Person Waren oder Dienstleistungen anbietet (Marktort) oder die Datenverarbeitung der Beobachtung ihres Verhaltens dient (Beobachtungsort).[56] Dadurch will die Datenschutz-Grundverordnung auf dem europäischen Markt für Wettbewerbsgleichheit zwischen Anbietern in der Union und Anbietern außerhalb der Union sorgen und die Wahrnehmung von Betroffenenrechten erleichtern. Neu ist auch die grundsätzliche Altersgrenze von Kindern in Art. 8 DSGVO, um in die Verarbeitung ihrer Daten für Dienste der Informationsgesellschaft einzuwilligen.[57] Auch das Recht auf Datenübertragbarkeit in Art. 20 DSGVO zählt zu den Innovationen. Es gibt betroffenen Personen das Recht, ihre Daten, die sie einem Verantwortlichen bereitgestellt haben, auf einen anderen Datenverarbeiter zu übertragen.[58] Neu sind auch die expliziten Anforderungen an den Datenschutz durch Systemgestaltung und Voreinstellungen in Art. 5 Abs. 1 lit. f und 25 DSGVO,[59] die Möglichkeit einer Datenschutzzerti-

[54] S. hierzu auch Erwägungsgründe 1, 2 und 4 DSGVO.

[55] S. ausführlich Roßnagel (2019b, S. 467 ff.).

[56] Die übliche Bezeichnung Marktortprinzip trifft nur für Art. 3 Abs. 2 lit. a DSGVO zu, nicht aber für lit. b.

[57] Hiervon können jedoch die Mitgliedstaaten abweichen, s. dazu Nebel und Dräger (2019).

[58] Zur Kritik an dieser s. Forum Privatheit (2019a, S. 8).

[59] S. z. B. Bieker und Hansen (2017, S. 165 ff.).

fizierung in Art. 42 und 43 DSGVO[60] sowie die Datenschutz-Folgenabschätzung in Art. 35 DSGVO.[61] Verbesserungen hat die Verordnung schließlich im Bereich der Aufsichtsbehörden erfahren: Ihre Befugnisse wurden in Art. 58 DSGVO gestärkt und die Zusammenarbeit der Aufsichtsbehörden in der Union in Art. 60 bis 76 DSGVO geregelt.[62] Die medienwirksamste Neuerung brachte wohl Art. 83 Abs. 5 DSGVO, nach dem bei den dort aufgelisteten Verstößen Geldbußen von bis zu 20 Mio. Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden können.[63]

Diese Neuerungen unterstützen die Durchsetzung des Datenschutzrechts und stärken das Bewusstsein für Datenschutz. Sie führen aber nicht dazu, dass die grundlegenden Vorgaben zu den Grundsätzen des Datenschutzes, zur Zulässigkeit der Datenverarbeitung und zu den Rechten der betroffenen Personen den neuen Herausforderungen entsprechen. Sie sind zwar in ihrer Abstraktheit auch auf neue Sachverhalte anwendbar, enthalten aber keine spezifischen Anforderungen. Im ersten Zugriff hat immer der Verantwortliche die Möglichkeit, die abstrakten Regelungen in seiner Datenverarbeitung zur Anwendung zu bringen. Dies führt zur Verstärkung von Machtungleichgewichten, weil überall da, wo das Recht normative Spielräume eröffnet, letztlich soziale, politische und wirtschaftliche Macht eindringt und einseitige Ergebnisse durchsetzt.[64]

Außerdem berücksichtigt die Verordnung nicht das veränderte Systemdesign moderner Technologien, in dem nicht mehr nur linear der Verantwortliche auf der einen Seite die personenbezogenen Daten der betroffenen Person auf der anderen Seite verarbeitet, sondern in denen Privatpersonen arbeitsteilig Verarbeitungsvorgänge als Teil einer Infrastruktur vornehmen können (z. B. Blockchain, Mix-Netze, Crowd-Sensing, Peer-to-Peer-Kommunikation, Social Networks). Die Grenzen der individuellen Verantwortlichkeit verschwimmen zunehmend, werden aber von den Regelungen der Verordnung nicht ausreichend berücksichtigt und können damit natürliche Personen unangemessen benachteiligen

[60] S. z. B. Maier, Lins u. a. (2019, S. 225 ff.), Maier und Bile (2019, S. 468 ff.), Maier, Pawlowska u. a. (2020, S. 445 ff.).

[61] S. ausführlich Forum Privatheit (2017a).

[62] S. näher Roßnagel (2017).

[63] S. Forum Privatheit (2019b).

[64] S. hierzu Roßnagel (2020c, S. 222 ff.).

und Machtasymmetrien verstärken.[65] Damit wird die Verordnung den künftigen Herausforderungen technisch-ökonomischer Entwicklungen nicht gerecht. Das Festhalten an überholten und unzureichenden Lösungen wirkt jedoch besonders schwer, da die Mitgliedstaaten von diesen grundlegenden Richtungsentscheidungen der Verordnung nicht abweichen dürfen.[66]

Schließlich versäumt es die Verordnung, Maßnahmen zu ergreifen, die nicht nur Verantwortliche, sondern auch Hersteller in die Pflicht nehmen würden, um Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen in technologische Anwendungen zu implementieren. Bisher trifft diese Pflicht den Verantwortlichen allein und es obliegt ihm, die Umsetzung bei Herstellern einzufordern. Deutlich bessere Effekte ließen sich mit der Verpflichtung der Hersteller erzielen. Dies muss nicht allein durch Ge- und Verbote erfolgen. In Kombination mit einem System von Anreizen und alternativen Regelungsformen könnte ein weitaus besserer Datenschutz durch Systemgestaltung und damit der Schutz der betroffenen Personen erreicht werden.[67]

2.4 Risikoneutralität

Dem Modernisierungsziel entgegen steht letztlich auch das spezifische Verständnis der Verordnung von Technikneutralität.[68] Richtig verstandene Technikneutralität soll verhindern, dass rechtliche Vorschriften aufgrund ihrer Formulierung technische Weiterentwicklungen ausschließen oder umgekehrt nicht mehr anwendbar sind. Dies schließt aus, Regelungen für einzelne *Ausprägungen* einer spezifischen IT-Anwendung zu treffen. Dies darf aber nicht verhindern, Vorgaben für bestimmte technische *Funktionen* vorzusehen – insbesondere, wenn sie besondere Risiken für Grundrechte verursachen.[69] Denn in einer technikgeprägten Welt kann Grundrechtsschutz nicht erfolgen, wenn nicht auch Risiken durch Technik aufgegriffen und durch die Regulierung technischer Funktionen gesteuert werden.

---

[65] S. Forum Privatheit (2019a, S. 10 f.).

[66] S. Forum Privatheit (2018c, S. 5).

[67] S. ausführlich Bile, Geminn u. a. (2018).

[68] S. Erwägungsgrund 15 DSGVO; die damalige Justizkommissarin Reding (2012, S. 198).

[69] S. grundsätzlich Roßnagel, in Eifert und Hoffmann-Riem (2009, S. 323 ff.).

Die Verordnung regelt jedoch überhaupt keine technischen Risiken. In keiner ihrer Regelungen geht die Verordnung die spezifischen grundrechtlichen Risiken moderner Informationstechnik an, wie sie in Abschn. 1.1 dargestellt wurden. Auch wo die Technik unterschiedliche Grundrechtsrisiken verursacht, finden die gleichen „technikneutralen" Regelungen Anwendung.[70] Zum Beispiel gelten die gleichen Zulässigkeitsregeln, Zweckbegrenzungen, Schutzvorkehrungen oder Rechte der betroffenen Person für alle Datenverarbeiter gleichermaßen, von der wenig riskanten Kundenliste eines Kleinstunternehmens bis hin zu globalen Konzernen wie Google oder Facebook, die mit risikoreichen Techniksystemen massenhaft personenbezogene Daten verarbeiten. Soweit es den Schutz der betroffenen Personen angeht, ist die Datenschutz-Grundverordnung risikoneutral.

Dagegen berücksichtigt sie die (geringeren) Risiken der Datenverarbeitung, wenn es um die Belastungen der Verantwortlichen geht.[71] Diese werden „entsprechend der Risiken von Datenverarbeitungsprozessen" reduziert oder beschränkt.[72] Dies bewirkt, dass nur ein Bruchteil der Verantwortlichen und Auftragsverarbeiter die in der Verordnung vorgesehenen Pflichten erfüllen muss.[73]

Datenverarbeitungen zu verhindern, die unzumutbare Risiken verursachen, ist nicht das Ziel der Verordnung. Sie knüpft an keiner Stelle die Zulässigkeit besonders riskanter Funktionen der Datenverarbeitung an das Fehlen bestimmter Grundrechtsrisiken oder macht sie von der Bewältigung dieser Risiken abhängig. Doch nur durch die Berücksichtigung typischer Risiken bestimmter Datenverarbeitungsformen im Verordnungstext hätte die notwendige Rechtssicherheit und Interessengerechtigkeit erreicht werden können.[74]

Zusammenfassend ist festzuhalten, dass die Datenschutz-Grundverordnung ihr Ziel der notwendigen Modernisierung des Datenschutzrechts weitgehend verfehlt.

---

[70] Eine Ausnahme besteht für automatisierte Entscheidungen in Art. 22 DSGVO, der jedoch in Abs. 2 auf die Regelungen in den Mitgliedstaaten verweist.

[71] S. zum datenschutzrechtlichen Risiko Bieker, Bremert u. a. (2018, S. 492).

[72] Zum risikobasierten Ansatz s. Roßnagel (2018a, S. 375 f.).

[73] S. kritisch Roßnagel (2016, S. 565).

[74] Dass im Unionsdatenschutzrecht risikoadäquate Regelungen möglich sind, zeigen z. B. Art. 6 der eCall-Verordnung (EU) 2015/758 oder Art. 8, 10 und 16 des Entwurfs einer ePrivacy-Verordnung der Kommission – s. Forum Privatheit (2018c, S. 5 f.).

3 Fortentwicklung des Governance-Rahmens

Die Herausforderungen des Grundrechtsschutzes durch die Digitalisierung sind somit durch die Datenschutz-Grundverordnung nicht bewältigt. Vielmehr setzt das Erreichen dieses Ziels weiterhin eine risikogerechte Modernisierung des Datenschutzrechts in der Europäischen Union voraus. Wie diese Voraussetzung hergestellt werden kann, bleibt daher eine dringend zu lösende Aufgabe. Daher untersucht der folgende Abschnitt Möglichkeiten, das Datenschutzrecht innerhalb des Regelungsrahmens der Datenschutz-Grundverordnung fortzuentwickeln.

3.1 Fortentwicklung durch Behörden und Gerichte

Im Governance-Rahmen der Datenschutz-Grundverordnung kommt eine wichtige Rolle für die Fortentwicklung des Datenschutzrechts den nationalen Aufsichtsbehörden und dem Europäischen Datenschutzausschuss zu. Sie treffen Entscheidungen im Einzelfall und geben Stellungnahmen und Empfehlungen ab. Auch die nationalen Gerichte und der Europäische Gerichtshof tragen zum besseren Verständnis der Verordnung bei. Sie alle konkretisieren die abstrakten Vorgaben der Verordnung und passen sie – soweit der Text der Verordnung dies ermöglicht – immer wieder an die neuen Herausforderungen an. Sie können dadurch viele Defizite der Verordnung ausgleichen, ihre Vorgaben zu praktikablen Anforderungen fortentwickeln und dadurch für mehr Rechtssicherheit sorgen.

Der Datenschutzausschuss oder einzelne Aufsichtsbehörden sind allerdings durch ihre spezifischen Aufgaben und Befugnisse beschränkt und können keine Korrektur des Normtextes bewirken. Zwar kommt ihren Aussagen grundsätzlich eine hohe praktische Bedeutung zu. Dennoch bleibt der erste Zugriff auf die Auslegung der Verordnung bei den Verantwortlichen. Vor allem ihre Praxis der Datenverarbeitung prägt in der Breite das Verständnis des gebotenen Datenschutzes. Sie nutzen jede Unklarheit des Textes für ihre Verarbeitungsinteressen.[75] Die Tatsache, dass die Verantwortlichen Bußgelder der Aufsichtsbehörden und selbst deren Verwarnungen auf breiter Front vor Gericht angreifen, zeigt, dass die Rolle der Aufsichtsbehörden wie auch des Ausschusses nicht so stark ist, wie es für eine effektive Governance notwendig wäre. Ihre Interpretation der Verordnung

[75] S. Roßnagel (2020c, S. 222 ff.)

gilt immer nur vorbehaltlich einer Klärung durch die nationalen Gerichte und letztlich den Europäischen Gerichtshof.

Der Europäische Gerichtshof bestimmt zwar als höchste Instanz ultimativ die Auslegung der Datenschutz-Grundverordnung. Ihm sind für die systematische Klärung von Streitfragen rund um die Datenschutz-Grundverordnung jedoch faktische Grenzen gesetzt. Er kann immer nur im Rahmen des jeweiligen Einzelfalls und nur in den Fällen entscheiden, die ihm vorgelegt werden. Er kann zwar anlässlich einer konkreten Streitfrage durch ein seltenes „obiter dictum" auch eine Aussage zu einer grundsätzlichen Fragestellung treffen. Doch werfen solche Aussagen meist mehr Fragen auf, als sie beantworten. Zudem sind die Kapazitäten des Gerichts begrenzt. Eine zeitnahe Klärung der Streitfragen zum Datenschutzrecht ist angesichts der Masse der Verfahren nicht nur zum Datenschutzrecht ausgeschlossen. Ein Äquivalent zur Verfassungsbeschwerde im deutschen Recht existiert nicht. Dies sowie die Überlastung des Gerichts könnte zukünftig für Deutschland durch das Bundesverfassungsgericht etwas abgemildert werden. Es hat in zwei jüngeren Entscheidungen zum „Recht auf Vergessen"[76] erklärt, künftig auch die Einhaltung der Grundrechtecharta und damit des Grundrechts auf Datenschutz zu prüfen. Für die Fortentwicklung des Datenschutzrechts durch Gerichte gilt jedoch immer: Bis letztlich ein höchstinstanzliches Gericht in Einzelfällen Defizite der Verordnung beseitigt und für Rechtssicherheit und Interessenausgleich sorgt, vergeht geraume Zeit. Vielfach hat die Dynamik der technischen Entwicklung das Problem dann bereits überholt.

Eine strukturelle Fortentwicklung sowohl durch die Aufsichtsbehörden und den Datenschutzausschuss wie auch durch die Gerichte findet außerdem ihre Grenze im Wortlaut des Gesetzestextes. Sie kann nur vom Unionsgesetzgeber oder – innerhalb des von der Datenschutz-Grundverordnung gewährten Spielraums – vom nationalen Gesetzgeber umgesetzt werden.

3.2 Evaluation der Datenschutz-Grundverordnung als Chance ihrer Fortentwicklung

Notwendig ist eine Fortentwicklung des Textes der Datenschutz-Grundverordnung aus vier Gründen. Erstens kann die Datenschutz-Grundverordnung

[76] BVerfG, NJW (2020, S. 300 ff. und 314 ff.).

schon infolge der ständig fortschreitenden Digitalisierung[77] kein statisches Regelungswerk sein. Vielmehr muss der Schutz der Werte, die in diesem Wandel unverändert bleiben sollen, sich immer wieder den Herausforderungen anpassen. Zweitens ist die Datenschutz-Grundverordnung nur eine erste Fassung einer unionsweiten Datenschutzregelung, eine Sammlung von unterschiedlichen, nur mühsam systematisierten Kompromissergebnissen, die bei den vieldimensionalen Interessengegensätzen und den 2015 gegebenen Machtverhältnissen durchsetzbar waren.[78] Sie ist ein legislativer Versuch, der angesichts neuer Herausforderungen für Persönlichkeitsrechte und Demokratie immer wieder neu zu konzipieren und zu verhandeln ist. Drittens konnten die Autoren der Verordnung die vielen und vielfältigen Praxisprobleme in allen von ihr erfassten Wirtschafts-, Verwaltungs- und Gesellschaftsbereichen gar nicht kennen. Daher ist wenig verwunderlich, dass sich in der Praxis sehr viele Probleme zeigen, den Vorgaben der Verordnung in den verschiedenen Anwendungsbereichen eine nachvollziehbare und lebenspraktische Form zu geben. Schließlich enthält die Verordnung strukturelle Defizite – wie ihre Risikoneutralität und fehlende Vorgaben für Hersteller – die den gebotenen Grundrechtsschutz auch gegenüber den neuen und künftigen Herausforderungen verhindern.

Mit Art. 97 DSGVO ist in der Verordnung deshalb ein Mechanismus zu ihrer regelmäßigen Evaluation und Weiterentwicklung vorgesehen, der als Chance der Modernisierung der Verordnung gesehen werden muss.[79] Nach Abs. 1 hat die Kommission bereits zwei Jahre nach Geltungsbeginn der Datenschutz-Grundverordnung bis zum 25. Mai 2020 über ihre Bewertung und Überprüfung zu berichten und den Bericht zu veröffentlichen. Danach sollen Evaluationen alle vier Jahre erfolgen. Nach Abs. 2 soll die Kommission „insbesondere" die Anwendung und die Wirkungsweise des Kap. V über die Übermittlung personenbezogener Daten an Drittländer insbesondere im Hinblick auf Angemessenheitsfeststellungen und des Kap. VII über Zusammenarbeit und Kohärenz überprüfen. Sie kann nach Abs. 3 für die Evaluation „Informationen von den Mitgliedstaaten und den Aufsichtsbehörden anfordern". Nach Abs. 4 hat sie die „Standpunkte und Feststellungen des Parlaments, des Rates und anderer einschlägiger Stellen oder Quellen" zu berücksichtigen. Nach Abs. 5 legt die Kommission in ihrem Bericht

[77] S. Erwägungsgrund 6 und 7 DSGVO.

[78] S. hierzu Roßnagel, in ders. (2018b), § 1 Rn. 15 ff.

[79] S. zum Folgenden Roßnagel (2020b, S. 287 ff.) und den gesamten Schwerpunkt von DuD 5/2020.

„erforderlichenfalls geeignete Vorschläge zur Änderung“ der Datenschutz-Grundverordnung vor und „berücksichtigt dabei insbesondere die Entwicklungen in der Informationstechnologie und die Fortschritte in der Informationsgesellschaft“.

Wie sich aus Art. 97 Abs. 2 und 5 DSGVO ergibt, soll die Kommission in ihren Evaluationen nicht nur die Umsetzung der Kap. V und VII untersuchen, sondern die jeweilige Ausgestaltung der gesamten Verordnung daraufhin überprüfen, welche Defizite bei ihrer Anwendung zu erkennen sind, und auch Änderungen der Datenschutz-Grundverordnung vorschlagen, die diese Defizite beseitigen. Dabei sind nicht nur die jeweils gegenwärtigen Datenschutzpraktiken zu berücksichtigen, sondern – wie Abs. 5 deutlich macht – auch die absehbaren Herausforderungen.[80] Daher beschränken sich die allermeisten Stellungnahmen von Mitgliedstaaten und Verbänden zur Evaluation der Verordnung nicht nur auf Probleme der Umsetzung, sondern erstrecken sich auch auf Vorschläge zur Verbesserung des Verordnungstextes.[81]

Im Gegensatz dazu zeigte die Kommission in ihrem Evaluationsbericht vom 24. Juni 2020[82] kein Interesse,[83] bereits nach so kurzer Zeit den mühsam ausgehandelten Kompromiss, den die Datenschutz-Grundverordnung darstellt, auch nur in Kleinigkeiten in Frage zu stellen und beschränkte sich auf die Untersuchung von einzelnen Umsetzungsproblemen.[84] Da sie nach Art. 17 Abs. 2 EUV allein das Recht hat, Gesetzesinitiativen in den Prozess der Unionsgesetzgebung einzubringen, kann letztlich sie bestimmen, ob und wenn ja welche Änderungsvorschläge sie aufgreift oder ignoriert. Daher muss ihr gegenüber immer wieder deutlich gemacht werden, dass sie zur ständigen Fortentwicklung des Grundrechtsschutzes verpflichtet ist.

Wie umfassend der Evaluationsauftrag auch verstanden wird, ein selbstreflexiver, kontinuierlicher Prozess der Anpassung ist möglich, gewollt und auch notwendig, um mit technischen Innovationen Schritt zu halten oder Mängel im

[80] S. zum Umfang der Berichtspflicht Schiedermair, in Simitis, Hornung u. a. (2019), Art. 97 DSGVO Rn. 6 ff.

[81] S. zu diesen Stellungnahmen ausführlich Roßnagel (2020b), S. 287 ff.

[82] S. Europäische Kommission, Communication from the Commission to the European Parliament and the Council, COM (2020) 264 final (SWD (2020) 115 final) vom 24.06.2020. S. auch Commission Staff Working Document vom 24.06.2020.

[83] So auch bereits Europäische Kommission, COM (2019) 374 final, wo sich die Kommission primär mit der Umsetzung der Verordnung, nicht mit der Verordnung selbst beschäftigt.

[84] S. hierzu affirmativ Heberlein (2020, S. 487), kritisch Roßnagel (2020a, S. 657 ff.).

Regelwerk zu beseitigen. Gerade bei letzterem ist es aufgrund der Eigenschaften der digitalen Welt ein unhaltbarer Zustand, wenn erkannte Mängel persistieren. Aber auch die mangelhafte Adressierung oder Nicht-Adressierung aufkommender Techniken über einen längeren Zeitraum ist angesichts der Schäden, die drohen, wenn personenbezogene Daten erst einmal in der Welt sind, inakzeptabel. Die Union kann ihrem Schutzauftrag für die Rechte und Freiheiten des Einzelnen nur gerecht werden, wenn sie dafür sorgt, dass das Datenschutzrecht mit den realen Möglichkeiten der Datenverarbeitung Schritt hält. Eine regelmäßige Überprüfung und gegebenenfalls Anpassung des Datenschutzrechts ist mithin auch verfassungsrechtlich geboten.

3.3 Notwendige praktische Verbesserungen der Datenschutz-Grundverordnung

Dabei zeigt sich, dass bereits kleine textliche Änderungen in der Datenschutz-Grundverordnung eine große Wirkung bezogen auf die Gewährleistung von Rechtssicherheit, die Erhöhung der Praxistauglichkeit der Regelungen und den Ausgleich des Machtungleichgewichts zwischen Verantwortlichem und betroffener Person entfalten können.[85] Einige Beispiele:

Das Verhältnis der Erlaubnistatbestände in Art. 6 Abs. 1 DSGVO zueinander ist im Text der Verordnung ungeklärt. So besteht Streit darüber, ob ein Verantwortlicher, der von der betroffenen Person eine Einwilligung eingefordert hat, seine Datenverarbeitung nachträglich auf überwiegende berechtigte Interessen stützen kann, wenn die betroffene Person die Einwilligung widerrufen hat. Er hat die betroffene Person nicht über den neuen Erlaubnistatbestand informiert und nimmt ihr damit außerdem das Recht zur Datenübertragung nach Art. 20 DSGVO. Daher sollte Art. 6 Abs. 1 DSGVO klarstellen, dass ein Verantwortlicher sich neben einer Einwilligung nicht zusätzlich auf einen gesetzlichen Erlaubnistatbestand berufen kann. Wenn er von der betroffenen Person eine Einwilligung einfordert, muss er sich auch auf die Regeln zu einer Einwilligung einlassen. Er muss dann vor allem einen Widerruf der Einwilligung gegen sich gelten lassen und kann nicht trotz des Widerrufs die Datenverarbeitung unter Berufung auf

[85] S. Roßnagel und Geminn (2020), mit 33 konkreten Änderungsvorschlägen für den Text der Verordnung.

einen anderen gesetzlichen Erlaubnistatbestand fortsetzen; zudem muss er der betroffenen Person eine Übertragung ihrer Daten ermöglichen.[86]

Ein anderes Beispiel ist das Gebot der Datenvermeidung, das in § 3a BDSG-alt noch enthalten war. Es fehlt in der Datenschutz-Grundverordnung. Diese kennt nur das Minimierungsgebot, personenbezogene Daten nur insoweit zu verarbeiten, wie dies zur Erreichung des Zwecks der Verarbeitung erforderlich ist. Den Zweck kann der Verantwortliche aber so wählen, dass die Verarbeitung vieler Daten erforderlich wird. Das Gebot der Datenvermeidung würde den Verantwortlichen aber verpflichten, seine Zwecke so auszuwählen, dass möglichst wenige personenbezogene Daten verarbeitet werden. Es sollte deshalb in Art. 5 DSGVO aufgenommen werden.[87]

Die besondere Schutzbedürftigkeit von Kindern[88] berücksichtigt die Datenschutz-Grundverordnung in sechs Regelungen – allerdings nicht vollständig und nicht systematisch. Daher sollte der Wortlaut der Verordnung diesen besonderen Aspekt zusätzlich und ausdrücklich berücksichtigen – z. B. bei der Veränderung des Verarbeitungszwecks in Art. 6 Abs. 4 DSGVO, bei der Einwilligung in die Verarbeitung besonderer Kategorien von personenbezogenen Daten in Art. 9 Abs. 2 lit. a DSGVO, beim Widerspruch nach Art. 21 DSGVO, bei der Einwilligung in automatisierte Entscheidungen nach Art. 22 Abs. 2 lit. c DSGVO und bei der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO.[89]

Werden Daten bei der betroffenen Person erhoben, so ist diese nach Art. 13 Abs. 1 und 2 DSGVO unmittelbar zum Zeitpunkt der Erhebung über Einzelheiten zur Datenverarbeitung zu informieren. Dies wird in der Praxis häufig so verstanden, dass bei Vertragsschluss oder beim ersten Kontakt mit der betroffenen Person in umfangreichen Datenschutzerklärungen oder Allgemeinen Geschäftsbedingungen alle denkbaren Eventualitäten künftiger Datenverarbeitungen beschrieben werden müssen. Dies geschieht oft schon lange Zeit vor der tatsächlichen Erhebung der Daten und vor der Entscheidung der betroffenen Person, ob sie mit der Datenverarbeitung einverstanden ist. Dies hat zur Folge, dass sie sich an die umfassenden Inhalte der – unter Umständen Jahre zuvor erfolgten – Information nicht mehr erinnern wird, wenn ihre Daten (dann irgendwann) tat-

[86] S. z. B. Forum Privatheit (2019a, S. 4 f.), Roßnagel und Geminn, Datenschutz-Grundverordnung verbessern, (2020, S. 49 ff., S. 116 f.).

[87] S. Forum Privatheit (2019a, S. 5 f.), Roßnagel und Geminn (2020, S. 47 f., S. 116).

[88] S. hierzu Roßnagel, in Stapf, Ammicht Quinn u. a. (2021, 165 ff.).

[89] S. hierzu ausführlich Roßnagel (2020d, S. 90 ff.)

sächlich erhoben werden. Die Praxis entspricht damit nicht der Zielsetzung der Datenschutz-Grundverordnung, die betroffene Person so zu informieren, dass sie ihre informationelle Selbstbestimmung optimal ausüben kann. Damit der Zweck der Informationspflicht nicht ausgehöhlt wird, sind Ergänzungen am Wortlaut von Art. 13 Abs. 1 und 2 DSGVO geboten, die klarstellen, dass die Information situationsadäquat erfolgt, nämlich unmittelbar vor der konkreten Datenerhebung und der potentiellen Entscheidung der betroffenen Person.[90]

Das Recht auf Datenübertragbarkeit nach Art. 20 DSGVO bezieht sich nur auf personenbezogene Daten, die die betroffene Person dem Verantwortlichen „bereitgestellt" hat. Sonstige Daten werden nicht erfasst. Beim Wechsel von einer Bank zur anderen oder von einem E-Mail-Provider zum anderen hieße das, dass zwar die selbst getätigten Überweisungen und die selbst versendeten E-Mails (Ausgangspostfach) mit umziehen können, Überweisungen und E-Mails von Dritten aber nicht (Eingangspostfach). Diese widersinnige Folge des Wortlauts von Art. 20 DSGVO kann durch die Ersetzung des Begriffs „bereitgestellt" durch „verursacht" geklärt werden.[91]

Art. 22 Abs. 1 DSGVO normiert das „Recht" der betroffenen Person, „nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie ähnlicher Weise erheblich beeinträchtigt". Dies ist grundsätzlich als Verbot von automatisierten Entscheidungen im Einzelfall zu interpretieren. Problematisch ist, dass dieses Verbot sehr eng formuliert ist und damit leicht zum Nachteil der betroffenen Person angewendet werden kann. Zum einen erfasst Art. 22 Abs. 1 DSGVO lediglich die Entscheidung selbst, nicht aber die vorhergehende automatisierte Verarbeitung und auch nicht die auf einer automatisierten Verarbeitung beruhende Entscheidung. Um diesem Defizit zu begegnen, sollte das Wort „ausschließlich" in Art. 22 Abs. 1 DSGVO gestrichen werden. So würden auch solche automatisierten Entscheidungen unter das Verbot fallen, in denen ein Mensch die Letztentscheidung fällt, ohne diese inhaltlich beeinflussen zu können. Zum anderen soll das Verbot nur gelten, wenn die Entscheidung eine Rechtswirkung entfaltet oder die betroffenen Personen auf ähnliche Weise erheblich beeinträchtigt. Um auch andere Einschränkungen zu erfassen, sollte für

[90] S. Forum Privatheit (2019a, S. 8), Roßnagel und Geminn (2020, S. 64 f., S. 121, S. 162).

[91] S. Forum Privatheit (2019a, S. 8 f.), Roßnagel und Geminn (2020, S. 77 ff., S. 172 f.), Geminn (2020, S. 309 f.).

das Verbot genügen, wenn die Entscheidung geeignet ist, die betroffene Person in erheblicher Weise zu beeinträchtigen.[92]

Ein großer Mangel der Verordnung besteht darin, dass sie zwar das Profiling punktuell erwähnt, seine besonderen Risiken aber nicht ausreichend regelt. Um diesen zu begegnen, sind risikoadäquate Regelungen notwendig. Die Datenschutz-Grundverordnung könnte gesetzlich festlegen, für welche Zwecke Profiling zulässig ist und für welche nicht. Vergleichbar mit der Regelung in Art. 9 DSGVO für besondere Kategorien personenbezogener Daten könnte die Regelung festlegen, dass Profiling grundsätzlich nicht erlaubt ist und nur in den ausdrücklich vorgesehenen Fällen zugelassen ist.[93]

Ein prominentes Beispiel ist auch der Datenschutz durch Technikgestaltung. Die zugrundeliegende Vorschrift des Art. 25 Abs. 1 DSGVO etabliert zwar eine Pflicht des Verantwortlichen, nicht aber des Herstellers von Datenverarbeitungssystemen. Ohne eine Pflicht des Herstellers, kann aber in den meisten Fällen der Verantwortliche dieser Pflicht nicht genügen. Daher sind in der Verordnung auch entsprechende Pflichten der Hersteller vorzusehen.[94]

Probleme, wie die hier beispielhaft vorgestellten, können durch eine Änderung des Normtextes einzelner Vorschriften gelöst werden und hätten leicht im Prozess der Evaluation der Datenschutz-Grundverordnung aufgegriffen und umgesetzt werden können. Dass die Kommission dies nicht getan hat, ist bedauerlich. Sie warten aber weiterhin auf ihre Erörterung und Umsetzung.

3.4 Strukturelle Modernisierung der Datenschutz-Grundverordnung

Soweit Änderungen in der grundlegenden Konzeption der Datenschutz-Grundverordnung in Frage stehen, um die Effektivität des Grundrechtsschutzes zu verbessern, oder Fortentwicklungen des europäischen Datenschutzrechts bedacht werden müssen, um dieses gegenüber den künftigen Herausforderungen der Digitalisierung zu wappnen, bedürfen sie im Rahmen der Ko-Regulierung des europäischen Datenschutzrechts umfassenderer und längerfristiger Unter-

[92] S. Forum Privatheit (2019a, S. 6 f.); Roßnagel und Geminn (2020, S. 82 ff., S. 129 ff.), Weichert (2020, S. 295), Glatzner (2020, S. 312 ff.).

[93] S. Forum Privatheit (2019a, S. 7 f.); Roßnagel und Geminn (2020, S. 88 ff.); Glatzner (2020, S. 312 ff.).

[94] S. z. B. Roßnagel und Geminn (2020, S. 91 ff. und 132 ff.).

suchungen und Diskussionen in den Mitgliedstaaten und der Union. Diese sollten folgende Aspekte berücksichtigen:[95]

Das wohl bedeutsamste strukturelle Defizit der Datenschutz-Grundverordnung ist ihre Risikoneutralität gegenüber Herausforderungen für die Grundrechte der betroffenen Personen.[96] Eine Fortentwicklung des Datenschutzrechts muss die Form einer risikogerechten Regulierung annehmen, die techniknah und bereichsspezifisch ist. Sie muss Vorgaben zur Systemgestaltung enthalten, die zwar keine technischen Merkmale vorgeben, aber technische Funktionen einzelner Technikliniен regeln.

Die Regelungen zu den Voraussetzungen der Zulässigkeit der Datenverarbeitung, zur Zulässigkeit von Zweckänderungen, zu konkreten Rechten der betroffenen Personen und zu den Pflichten der Verantwortlichen müssen spezifisch für bestimmte Technikfunktionen oder bereichsspezifisch für bestimmte Anwendungsprobleme konkretisiert werden. Grundsätzlich sind zwei unterschiedliche Ansatzpunkte für im richtigen Sinn technikneutrale, aber risikospezifische Datenschutzregelungen möglich:

- Entweder regelt das Datenschutzrecht Funktionen von Techniken, die in vielen Wirtschafts-, Gesellschafts- und Verwaltungsbereichen zum Einsatz kommen – wie etwa Videoüberwachung, Cloud Computing oder algorithmenbasierte Entscheidungsverfahren – und fordert für diese bereichsübergreifend die Ausgestaltung einzelner wichtiger Funktionen – wie z. B. die Nachvollziehbarkeit und Begründbarkeit von algorithmenbasierten Entscheidungen.[97]
- Oder es regelt Ausprägungen von Datenschutzvorgaben in spezifischen Anwendungsbereichen – wie z. B. für Smart Cars, Smart Buildings oder Social Networks. In diesen Regelungen fordert es bereichsspezifische Ausgestaltungen von Technikfunktionen – wie etwa im Smart Car bestimmte Anzeigen vor der Verarbeitung von bestimmten personenbezogenen Daten, Möglichkeiten der Intervention von Fahrern oder die Zulässigkeit von Speicherungen oder Weitergaben von Daten an Dritte – und berücksichtigt dabei die spezifischen Bedingungen und Ausprägungen ihrer Anwendung.[98]

[95] S. ausführlich Roßnagel und Geminn (2020, S. 149 ff.).

[96] S. Abschn. 1.2.4.

[97] S. Forum Privatheit (2020b, S. 11 f.)

[98] S. Abschn. 1.4.1; s. z. B. auch Roßnagel und Hornung, in: dies. (2019, S. 469 ff.)

Notwendig ist immer, die geeigneten Anforderungen an die Verantwortlichen, aber auch an die Hersteller und Anbieter von Techniksystemen zu stellen, mit deren Hilfe die Verantwortlichen die Anforderungen erfüllen sollen.[99]

3.5 Fortentwicklung der normativen Innovationen

Die Datenschutz-Grundverordnung enthält einige echte regulative Innovationen für den Datenschutz.[100] Sie sind mit hohen Erwartungen und vielen Hoffnungen verbunden: Sie sollen nicht nur zu mehr Datenschutzschutz, sondern auch zu einem gerechteren, passgenaueren und praktikableren Datenschutz führen. Obwohl die Datenschutz-Grundverordnung vor über vier Jahren in Kraft getreten ist und seit mehr als zwei Jahren in den Mitgliedstaaten gilt, sind diese Innovationen noch nicht umgesetzt, können noch nicht genutzt werden oder stoßen auf Schwierigkeiten. Die Datenschutz-Grundverordnung hat sie zwar eingeführt, oft aber nur benannt, angekündigt oder angedeutet. Sie regelt diese Innovationen nur in Ansätzen und lässt viele wichtige Details offen. Alle diese Innovationen sind über die bestehenden Regelungen hinaus von weiteren Kriterien, Verfahrensregelungen, Initiativen, Konzepten, Erprobungen und materiellen Vorbedingungen abhängig. Da sie fehlen, können die Innovationen nicht unmittelbar angewendet, umgesetzt oder in Anspruch genommen werden. Bei allen Innovationen behindert die Datenschutz-Grundverordnung selbst ihre Effektivität.[101]

Der Erfolg des Datenschutzrechts ruht vornehmlich auf zwei Säulen: effektive Abschreckung vor Rechtsverstößen[102] und greifbarer Nutzen für die beteiligten Akteure. Datenschutzrecht wird häufig als eine Last wahrgenommen – sowohl bezogen auf Innovation als auch auf wirtschaftlichen Erfolg. Dies führt zu Versuchen, strenge datenschutzrechtliche Vorgaben zu umgehen. Es ist deshalb wichtig, auf regulatorischer Basis Marktanreize zu schaffen, die Datenschutz als Wettbewerbsvorteil etablieren, anstatt ihn zum Nachteil werden zu lassen. Das Recht muss daher Anreize setzen, die eigenen Interessen zu mobilisieren, um Datenschutz zu verbessern. Für Hersteller, Entwickler und Anwender von

[99] Roßnagel und Geminn (2020, S. 156 f.)

[100] S. Abschn. 1.2.3.

[101] S. näher Roßnagel (2019b, S. 467 ff.)

[102] S. näher Forum Privatheit (2019b).

Datenverarbeitungssystemen muss sich Datenschutz lohnen. Dies kann dadurch erreicht werden, dass Datenschutz eine positive Marktinformation – wie etwa ein Zertifikat – sein kann, die einen Wettbewerbsvorteil bewirkt.[103] Ein weiterer Anreiz lässt sich dadurch setzen, dass nachgewiesene datenschutzfreundliche Systemgestaltungen bei der öffentlichen Auftragsvergabe berücksichtigt werden. Direkte wirtschaftliche Vorteile für die betreffenden Unternehmen können auch steuerliche Regelungen bieten, die datenschutzgerechtes Verhalten belohnen. Andere Anreize setzen beim Verhalten der Nutzenden an und versuchen, diese dazu anzuhalten, ihre eigenen personenbezogenen Daten besser zu schützen. Das gilt für die Förderung von Maßnahmen zum Selbstdatenschutz[104] und für das Nudging.[105] Solche Anreize hat die Datenschutz-Grundverordnung unzureichend geregelt. Sie sind durch Ergänzungen in der Verordnung weiterzuentwickeln.

Anreize, die dabei herausstechen, sind Audits und Zertifizierungen.[106] Die Datenschutz-Grundverordnung regelt jedoch weder eine Produktbestätigung noch ein Verfahren einer kontinuierlichen Verbesserung eines Datenschutzmanagementsystems.[107] Sie sieht vielmehr eine Überprüfung und Bestätigung von „Datenverarbeitungsvorgängen" allein am Maßstab der Einhaltung der Vorgaben der Datenschutz-Grundverordnung vor – also ein drittes Konzept der freiwilligen Überprüfung eines datenschutzrelevanten Objekts.[108] Dabei zielt sie auf das Kunststück einer statischen Überprüfung eines dynamischen Systems, das mit einer auf einen bestimmten Zeitpunkt bezogenen Feststellung seiner Rechtskonformität abgeschlossen wird. Es „prämiert" die Einhaltung der ohnehin geltenden rechtlichen Vorgaben, ohne näher zu regeln, wie diese Feststellung als Marktinformation verwendet werden darf. Ob diese Form der Überprüfung und Bestätigung auf praktisches Interesse stößt, bleibt abzuwarten. Gleichwohl gibt es keine rechtliche Pflicht, die bestimmt, dass eine Zertifizierung auf die Vorgaben der Datenschutz-Grundverordnung beschränkt sein muss. Daher ist es möglich, Standards zu setzen und zu prüfen, die über das rechtlich geforderte Mindestmaß hinausgehen. Allerdings wären die Ergebnisse dieser Prüfung keine Zertifikate

[103] S. Bile, Geminn u. a. (2018, S. 111 ff.).

[104] S. Forum Privatheit, Selbstdatenschutz, (2014).

[105] Bile, Geminn u. a. (2018, S. 104 ff.).

[106] S. hierzu umfassend Bile, Geminn u. a. (2018, S. 93 ff.).

[107] S. hierzu Roßnagel (2000), Bittner (2021).

[108] S. Maier, Lins u. a. (2019, S. 225), Maier und Bile (2018, S. 468), Maier, Pawlowska u. a. (2020, S. 445 ff.).

nach Art. 42 DSGVO. Somit verhindert die Verordnung nicht eine Steigerung und Weiterentwicklung des Datenschutzes, unterstützt diese aber auch nicht. Dabei wäre für die zertifizierten Unternehmen die Werbung mit datenschutzkonformen Produkten und Systemen der beste Anreiz, freiwillig den Datenschutz ihrer Verarbeitungsvorgänge zu verbessern. Selbst für die Konformitätsbestätigung nach Art. 42 DSGVO fehlt eine Regelung, ob und wie ein erworbenes Zertifikat durch Werbung kommuniziert werden kann.[109]

3.6 Wege zur Modernisierung der Datenschutz-Grundverordnung

Da die Informationstechnik und ihre Anwendungen immer wieder Herausforderungen für den Grundrechtsschutz bewirken, ist die risikoadäquate Anpassung des Datenschutzrechts eine permanente und dynamische Aufgabe. Für diese hat die Datenschutz-Grundverordnung statt einer Monopolisierung und Zentralisierung in der Weiterentwicklung des Datenschutzrechts[110] eine sinnvolle Arbeitsteilung zwischen Union und Mitgliedstaaten eingerichtet. Nur so ist die notwendige Komplexität der Datenschutzregelungen angesichts einer sich ständig wandelnden, gesellschaftsweiten Verarbeitung personenbezogener Daten auch zu erreichen.[111]

Die von der Verordnung angeordnete Ko-Regulierung kann auch für die Suche nach einem modernen Datenschutzrecht eingesetzt werden: Diese sollte einem in sich stimmigen, demokratischen und pluralistischen Modell der Evolution des Datenschutzrechts folgen. Rechtsevolution sollte sich an der natürlichen Evolution orientieren, deren Elemente aber gezielt organisieren. Sie muss wie diese auf den Prinzipien der Variation und der Selektion aufbauen. Dieses könnte unter anderem wie folgt aussehen:[112]

Die notwendige *Variation* von Lösungsansätzen könnte dadurch erreicht werden, dass die Mitgliedstaaten – im weiten Rahmen der Datenschutz-Grundverordnung – vielfältige neue Datenschutzkonzepte erproben, die auf jeweils neue Herausforderungen moderner Informationstechnik reagieren oder diese

[109] S. Geminn (2018, S. 1593).

[110] S. hierzu Roßnagel, in ders. (2018b), § 1 Rn. 15 ff.

[111] S. Abschn. 1.2.2.

[112] S. hierzu Roßnagel (2018a, S. 383 f.).

sogar steuern. Angesichts der Vielfalt und Dynamik der zukünftigen, heute noch unbekannten Herausforderungen der Digitalisierung für die Grundrechte kann auf der Ebene der Mitgliedstaaten mit unterschiedlichen Regelungskonzepten experimentiert werden. Dadurch können vielfältige Quellen dazu beitragen, dass sich in der Union ein lebendiger Datenschutz entwickelt. Statt einer – ohnehin nicht zu erreichenden – Vereinheitlichung der Datenschutzpraxis ermöglichen unbestimmte Rechtsbegriffe und ihre situationsgerechte Konkretisierung, dass in den einzelnen Mitgliedstaaten Datenschutz den lokalen Bedingungen angepasst werden kann. Schließlich bieten die vielen Regelungsmöglichkeiten der Mitgliedstaaten Chancen für eine Modernisierung des Datenschutzrechts, indem dort versucht wird, durch risikoadäquate Regelungen einen ausreichenden Schutz der Grundrechte gegen künftige Herausforderungen zu gewährleisten.

Die Kommission sollte diese Variationen nicht als Verstoß gegen die Datenschutz-Grundverordnung ansehen, sondern deren Anwendung in einem oder mehreren Mitgliedstaaten als geeignetes Mittel verstehen, um eine Erprobung verschiedener Datenschutzkonzepte in der Praxis durchzuführen. Solange derartige mitgliedsstaatliche Variationen nicht gegen grundlegende Festlegungen der Datenschutz-Grundverordnung verstoßen, helfen sie, diese grundlegenden Festlegungen durch Erfahrung mit neuen und angepassten Datenschutzkonzepten zu verbessern.

In den regelmäßigen Evaluationen der Kommission der Datenschutz-Grundverordnung findet eine Bewertung und *Selektion* der verschiedenen Datenschutzkonzepte statt. In den Diskussionen über den Evaluationsbericht haben alle Interessierte die Möglichkeit, ihre individuellen Bewertungen in die Evaluation einzubringen. Hier werden die Erfolge für den Grundrechtsschutz der betroffenen Personen und für den Ausgleich mit den Grundrechtspositionen und den öffentlichen Interessen der Datenverarbeiter bewertet.

Schließlich finden in regelmäßigen Novellen zur Datenschutz-Grundverordnung Festlegungen durch den Unionsgesetzgeber statt, in denen er das in einzelnen Mitgliedstaaten Bewährte unionsweit übernimmt. Nicht alles muss er in der Datenschutz-Grundverordnung regeln. Er sollte keine „One Size Fits All"-Regelungen anstreben, sondern bereichsspezifische Regelungen, die den besonderen Risiken eines Anwendungsbereichs gerecht werden. Nur so kann er der Unterkomplexität der gegenwärtigen Datenschutz-Grundverordnung abhelfen.

4 Konzepte und Instrumente zur Bewältigung der technisch-ökonomischen Herausforderungen

Damit Recht die Grundrechte in einer digitalen Welt schützen und fördern kann, muss es die Entwicklung der Informationstechnik nach rechtlichen Kriterien steuern und technische Systeme grundrechtsverträglich gestalten.[113] Dieser Anspruch einer rechtliche Steuerung ist jedoch mit folgenden Grundproblemen konfrontiert:

- Die technisch-ökonomischen Herausforderungen für den Grundrechtsschutz sind globaler Natur. Die riskanten Techniken werden weltweit von sehr vielen Datenverarbeitern eingesetzt. Vor allem global agierende Großkonzerne mit übergroßer Wirtschaftsmacht bieten besonders datenorientierte Dienste an und beuten Profile von Milliarden Personen aus.[114] Hier stellt sich das Problem, wie nationale Demokratien – in dieser Hinsicht gilt auch die Europäische Union als nationale Demokratie – diese weltweite Gefährdung der Grundrechte begrenzen können.
- Viele soziale Ziele der Machtsteigerung, der Gewinnmaximierung, der Kontrolle und Verhaltenssteuerung erscheinen durch ihre Inkorporation in technische Systeme den betroffenen Personen und den politischen Akteuren als technische Sachzwänge.[115] Die technischen Systeme hätten immer auch anders gestaltet werden können. Sie wurden jedoch meist gezielt so gestaltet, um mit dem technischen Sachzwang jeweils (auch) das gewünschte soziale Ziel zu erreichen. Werden sie z. B. individualisiert angeboten, erzwingen sie die Bildung von Profilen über die Nutzenden und ermöglichen deren Kontrolle. Arbeitet z. B. ein Techniksystem mit bestimmten Statistikmustern, erfordert es die Anwendung von Big Data-Analysen und ermöglicht kollektive Verhaltenssteuerungen. Hier stellt sich das Problem einer grundrechtsförderlichen und machtbegrenzenden Technikgestaltung.
- Soweit Techniksysteme den Charakter von Infrastrukturen der digitalen Gesellschaft annehmen, wie dies etwa bei bestimmten Plattformen und Suchsystemen der Fall ist, entwickeln sie einen besonderen Zwangscharakter. Technische Infrastrukturen sind Techniksysteme, die ständig und flächen-

[113] S. näher Roßnagel (2020c, S. 226).

[114] S. z. B. Zuboff (2018).

[115] S. näher Roßnagel (2020c, S. 222 f.).

deckend Dienstleistungen gleicher Qualität erbringen (sollen). Für ihre Nutzung gelten Bedingungen und Regeln, die alle beachten müssen, die sie nutzen. Wer diese Bedingungen und Regeln bestimmen kann, schafft den idealen Sachzwang. Für die meisten Nutzenden ist die Nutzung der Infrastruktur nicht freiwillig, weil sie auf diese aus sozialen oder beruflichen Gründen angewiesen sind. Sie haben keine Auswahl auf einem Markt verschiedener Möglichkeiten, sondern sind gezwungen, diese Infrastrukturen zu den geforderten Bedingungen zu nutzen.[116] Hier stellt sich das Problem, die gesellschaftliche Verantwortung digitaler Infrastrukturen für die Grundrechte ihrer Nutzenden einzufordern.

- Zu vielen datenhungrigen Technikanwendungen wird aber niemand gezwungen. Vielmehr werden sie freiwillig genutzt, weil sie den Nutzenden die Erfüllung ihrer Träume versprechen. Vor allem die Datenverarbeitung im Alltag (IoT) verspricht eine schöne neue Welt, in der die Informationstechnik zu weniger lästiger Arbeit, zu einem lückenlosen Gedächtnis, zu einer Erweiterung der Sinne, zu mehr Kreativität, zu besserer Gesundheit oder zu alltäglicher Sicherheit verhilft. Diese Wunschträume verführen zur Nutzung dieser Technikanwendungen und zur Inkaufnahme der scheinbar notwendig mit ihnen verbundenen Verarbeitung personenbezogener Daten.[117] Hier stellt sich das Problem, wie Grundrechtsschutz gegen die Risiken der Technik von der individuellen Zustimmung gelöst und objektiviert werden kann.

Trotzt dieser Schwierigkeiten und Widerstände ist grundsätzlich am Ziel von Datenschutz und Selbstbestimmung sowie dem Schutz weiterer Grundrechte festzuhalten. Es ist in der digitalisierten Welt – mithilfe der einschlägigen Schutzregelungen – auch gegen widerständige Umstände und Interessen weiterhin durchzusetzen.

4.1 Rechtliche Gestaltung grundrechtsriskanter Techniksysteme

Informationstechnik verändert die Verwirklichungsbedingungen von Grundrechten. Sie kann ihre Wahrnehmung stärken. Sie kann neue Möglichkeiten der

[116] S. Roßnagel (2020c, S. 222).

[117] S. hierzu Roßnagel (2007, S. 13 ff.).

Selbstbestimmung und Selbstentfaltung bieten oder Leben und Gesundheit besser schützen. Sie kann aber auch – und das ist wahrscheinlicher – Machtpositionen stärken und Verhaltenssteuerung erleichtern. Welche dieser Potentiale verwirklicht werden und wer die Oberhand in der Nutzung der jeweiligen Technik gewinnt, ist letztlich die entscheidende Machtfrage. Wer in einer technikgeprägten Welt Freiheit sichern und Macht begrenzen will, muss Informationstechnik so gestalten, dass sie machtbegrenzend und freiheitsfördernd wirkt. Wenn Technik der stärkste Bestimmungsfaktor ist, um menschliches Verhalten zu steuern, muss Recht Technik gestalten, um diese Ziele zu erreichen.

Notwendig ist hierfür eine rechtliche Gestaltung von Informationstechniksystemen.[118] Diese wird nicht dadurch bewirkt, dass Recht Allgemeinplätze vorgibt wie zum Beispiel „Stand der Technik". Denn dies überlässt Technikern, die Kriterien und ihre Umsetzung zu bestimmen. Ziel der Technikentwicklung ist sehr oft eine Machtsteigerung für den Investor. Er stellt die Anforderungen an die Technik oft so, dass das Techniksystem vor allem diese Wirkung erzielt. Die Datenverarbeitung für eine fertig entwickelte Technik erscheint dann oft als Sachzwang. Das Techniksystem hätte aber auch anders gestaltet werden können – mit anderen Folgen für die Grundrechte. Wenn Recht die Technikentwicklung beeinflussen soll, um seine Ziele zu erreichen, ist es besonders wichtig, alternative Gestaltungsmöglichkeiten aufzugreifen und Gestaltungen vorzuschreiben, die machtbegrenzend und freiheitsfördernd sind.

Hierfür sind bereichsspezifische Vorgaben für hilfreiche oder zu verhindernde Technikfunktionen notwendig – z. B. für Smart Cars, für Smart Home oder für selbstlernende KI-Systeme in einem bestimmten Anwendungsbereich. Beispielsweise bedarf der Datenschutz bei vernetzten Automobilen einer bereichsspezifischen Regelung, weil nur so die besonderen Risiken durch die Verarbeitung von personenbezogenen Daten aus dem vernetzten und künftig selbständig fahrenden Automobil adäquat erfasst und allen Beteiligten entsprechende Rechts- und Innovationssicherheit geboten werden können. Unter anderen sollten folgende rechtliche Vorgaben bestehen:[119]

- Nach dem Prinzip des „Privacy by Design" und des „Privacy by Default" sollten die Datenverarbeitung im Auto für den Halter oder den Fahrer so

[118] S. hierzu ausführlich Roßnagel, Hornung u. a. (2018).

[119] S. z. B. Roßnagel und Hornung (2019, S. 473 ff.) unter Rückgriff auf Empfehlungen des Arbeitskreises VII des 52. Deutschen Verkehrsgerichtstags (2014).

konfiguriert, die Architektur der Datenverarbeitungssysteme so datenschutzfreundlich (z. B. Datenhaltung im Auto statt auf einem Server) und die Prozesse so an den Anforderungen des Datenschutzrechts (z. B. implementierte Löschkonzepte) orientiert sein, dass sie die Datenschutzgrundsätze umsetzen.

- Zur Transparenz für betroffene Personen sollte jeweils eine umfassende und verständliche Information erfolgen, bei welchem Dienst welche Daten generiert und verarbeitet werden sowie welche Daten auf welchen Wegen und zu welchen Zwecken übermittelt werden.
- Bei der freiwilligen oder vertraglich vereinbarten Datenübermittlung an Dritte sind Fahrzeughalter und Fahrer technisch in die Lage zu versetzen, diese zu kontrollieren und zu unterbinden.
- Personenbezogene Daten sollten prinzipiell im Auto selbst verbleiben und nur anonymisierte oder pseudonymisierte Daten im Backend der Hersteller oder Diensteanbieter verarbeitet werden.
- Außerdem ist festzulegen, welche Datenkategorien nur flüchtig und welche für einen gewissen Zeitraum, welche anonym, pseudonym und personenbezogen gespeichert werden dürfen.
- Zulässige Zweckänderungen sind spezifisch und bestimmt zu regeln – etwa für die Aufklärung von Verkehrsunfällen ab einer bestimmten Schwere.
- Für Unfalldatenspeicher sind die Daten festzulegen, die erhoben, gespeichert oder übermittelt werden sollen, und verfahrensrechtliche und technische Schutzvorkehrungen zu bestimmen.
- Die Anforderungen an den Datenschutz gegenüber Herstellern sollten bei der Zulassung der Automobile geprüft werden. Die Umsetzung der Anforderungen gegenüber Diensteanbietern sollten diese durch ein Audit oder eine Zertifizierung nachweisen.

Um zu verhindern, dass rechtliche Regelungen schnell ihre Wirksamkeit verlieren, sollten sie – entsprechend einer richtig verstandenen Technikneutralität – keine konkreten technischen Merkmale regeln, die von einer Weiterentwicklung der Technik bald überholt werden. Richtig und notwendig ist es jedoch, risikoreiche *Funktionen* einer Techniklinie zu regeln. Nur so lassen sich die spezifischen Risiken adressieren – und die Regelungen mit dem nächsten Update weiterhin anwenden.[120]

[120] Roßnagel (2018a, S. 377 f.).

Dagegen verkennt die überzogene Ideologie der Technikneutralität, wie sie in der Datenschutz-Grundverordnung Anwendung findet,[121] dass Macht in jede Ritze dringt, die rechtliche Regelungen aufweisen, und jede Leerstelle besetzt, die Recht bestehen lässt. Diese „Technikneutralität" ist ein technokratisches, vermeintlich wertfreies Ordnungskonzept, das aber den Machtfaktor ignoriert. Ebenso schädlich ist aber auch die machtvergessene Naivität, die meint, die vielen Leerstellen der Datenschutz-Grundverordnung ließen Raum für datenschutzgerechte Lösungen nach den jeweils eigenen Vorstellungen. Dies wäre allenfalls dann der Fall, wenn man die Macht hätte, die eigenen Lösungen gegen Widerstand durchzusetzen. Was nicht explizit geregelt ist, entwickelt sich so immer zum Nachteil des Schwächeren. Statt abstrakt zu sein, müssen rechtliche Regelungen Technikfunktionen so regulieren, dass unerwünschte Macht das gewünschte Ziel der Machtbegrenzung nicht konterkarieren kann.[122]

Das Umweltrecht ist hier einen deutlichen Schritt weiter. Hier ist anerkannt, dass Industrieunternehmen letztlich klare und für Ingenieure eindeutige Vorgaben benötigen, um tatsächliche Änderungen zu bewirken. Zwar gibt es auch hier abstrakte Vorgaben wie die Vermeidung schädlicher Umwelteinwirkungen, die Vorsorge für eine nachhaltige Entwicklung oder die Beachtung des Stands der Technik. Doch werden diese abstrakten Vorgaben durch Grenzwerte oder Beschaffenheitsanforderungen konkretisiert, die mess- und nachprüfbar sind.[123]

4.2 Objektiver Grundrechtsschutz

Bisher ist das Datenschutzrecht stark individualistisch ausgerichtet und unterstellt vielfach, dass die Grundrechte auf Datenschutz und informationelle Selbstbestimmung gewahrt werden können, indem gleichberechtigte Partner die Zwecke und Bedingungen der Datenverarbeitung aushandeln.[124] Dementsprechend sieht Art. 6 Abs. 1 UAbs. 1 lit. a und b DSGVO die Einwilligung der betroffenen Person oder einen Vertrag mit ihr als ausreichende Grundlage der Verarbeitung auch sehr umfangreicher und sehr persönlichkeitsbezogener Daten

[121] S. Abschn. 1.2.4.

[122] S. Roßnagel (2020c, S. 227).

[123] S. z. B. Schultze-Fielitz, Technik und Umweltrecht, in Schulte und Schröder (2011, S. 464 ff.), Roßnagel und Hentschel, in Führ (2019), § 5 Rn. 41 ff., 432 ff. und § 7 Rn. 10 ff., 72 ff., 149 ff.

[124] S. Forum Privatheit (2020a).

an. Das Datenschutzrecht vertraut hier darauf, dass Transparenz und Eigenverantwortung für den Schutz der Grundrechte ausreichend sind: Der Datenverarbeiter muss die betroffene Person über die Datenverarbeitung informieren und diese kann dann entscheiden, ob sie in die Datenverarbeitung einwilligt oder mit dem Datenverarbeiter einen entsprechenden Vertrag schließt.

Dieses Konzept ignoriert jedoch die faktischen Machtverhältnisse. Dies nutzen z. B. Internetkonzerne aus. Sie lassen sich durch Einwilligungen von jeglichen Rechtsverpflichtungen befreien und etablieren in Form von Allgemeinen Geschäftsbedingungen ein eigenes Regelungsregime.[125] Dieses erlaubt ihnen, die Daten ihrer Nutzer zu vielfältigen Zwecken auszubeuten, deren Rechte einzuschränken und ihre eigenen Handlungsspielräume extrem auszuweiten. Diese Einwilligungslösung ist auch nach Geltung der Datenschutz-Grundverordnung weiterhin die rechtliche Grundlage für die Macht der Konzerne. Insofern lässt die Verordnung das Individuum, das beruflich oder sozial zur Nutzung der digitalen Plattform gezwungen ist, im Stich.

Dieses Beispiel zeigt, dass die Fragen des Grundrechtsschutzes nicht allein der Vereinbarung ungleicher Vertragspartner überlassen werden darf. Unter den beschriebenen Umständen asymmetrischer Machtverteilung und struktureller Grundrechtsrisiken ist das Modell der wohlinformierten Techniknutzenden, die nach individuellen Verhandlungen freiwillig ihre Daten preisgeben, für den Grundrechtsschutz nicht adäquat. Vielmehr müssen die Schutzregelungen die objektive Funktion des Rechts stärker betonen.

Recht muss in solchen Fällen einseitiger Machtausübung die Möglichkeit der Einwilligung beschränken und die Vertragsgestaltung der Datenverarbeitung auf objektive Funktionen der Leistungserbringung beschränken.[126] Art. 7 Abs. 4 DSGVO enthält hierzu einen viel zu schwachen Ansatz. Nach dieser Vorschrift muss bei der Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, dem Umstand einer Kopplung von Vertragsabschluss und Einwilligung nur „in größtmöglichem Umfang Rechnung getragen werden“. Sie enthält nur eine „Berücksichtigungspflicht“ und soll im Ergebnis nicht bei den Social Networks greifen, wenn die Einwilligung wirtschaftlich die Gegenleistung für die geldfreien Leistungen der Plattform ist.[127] Bis zum Geltungsbeginn der Daten-

[125] S. z. B. Schantz, in Schantz und Wolff (2017), Rn. 504 f., 509.

[126] Roßnagel und Geminn (2020, S. 53 ff., S. 117).

[127] S. z. B. Klement, in Simitis, Hornung u. a. (2019), Art. 7 Rn. 58 ff.; Buchner und Kühling, in Kühling und Buchner (2018), Art. 7 Rn. 48.

schutz-Grundverordnung waren die Rechte der betroffenen Person im deutschen Datenschutzrecht nicht abdingbar. Diese Regelung ist mit der Datenschutz-Grundverordnung entfallen. Sie hätte im Rahmen der Evaluation der Datenschutz-Grundverordnung wieder eingeführt und ausgeweitet werden können. Dies sollte möglichst bald nachgeholt werden.[128]

Außerdem sind unterschiedliche rechtliche Ansatzpunkte zur Steuerung der Technikentwicklung enger zusammenzuführen und abzustimmen, wie dies etwa bei der Bewertung von Allgemeinen Geschäftsbedingungen erforderlich ist, um tatsächlich Gestaltungsmacht des Rechts gegenüber der Technik zu erreichen. Wenn z. B. Datenschutzrecht, Verbraucherschutzrecht, Wettbewerbsrecht und Steuerrecht hinsichtlich des Grundrechtsschutzes der strukturell wirtschaftlich Schwächeren zusammenarbeiten, können die Grundrechte des Datenschutzes und der informationellen Selbstbestimmung auch in extremen Machtasymmetrien objektiv gewährleistet werden.

4.3 Infrastrukturverantwortung

Auch die Betreiber von digitalen Infrastrukturen nehmen Aufgaben der Daseinsvorsorge in der digitalen Gesellschaft wahr. Sie sind daher mit den Betreibern der Straßen, des Bahnverkehrs, des Briefverkehrs, der Wasserver- und -entsorgung, der Abfallentsorgung oder der Energieversorgung in der analogen Welt vergleichbar. Ohne ihre Infrastrukturleistungen wäre das gesellschaftliche Zusammenleben infrage gestellt und die Ausübung von Grundrechten gefährdet. Infrastrukturbetreiber haben daher, unabhängig ob sie privatrechtlich oder öffentlich-rechtlich verfasst sind, eine gesteigerte gesellschaftliche Verantwortung und unterliegen in besonderem Maß staatlicher Aufsicht. Sie haben auch die Grundrechte der von ihnen Abhängigen in besonderer Weise zu achten und zu schützen.

Dies gilt in verstärkter Weise, wenn die Infrastrukturbetreiber durch autoritative Setzung eine eigene Rechtsordnung in Form von Gemeinschaftsregeln erstellen, die staatlichen Rechtsregeln, die durch demokratische Prozesse zustande kommen, Konkurrenz machen. Im Zweifelsfall müssen das staatliche Recht und erst recht die Grundrechte der Grundrechtecharta und des Grundgesetzes diesen Gemeinschaftsstandards vorgehen. Soweit Grundrechte betroffen

[128] Roßnagel und Geminn (2020, S. 87 f., S. 131 f.).

sind, muss die Ausgestaltung und der Betrieb der Infrastrukturen stärker an diesen als an ökonomischen Konzernzielen ausgerichtet sein.

Daher sind mit der Rechtsprechung des Bundesverfassungsgerichts die öffentliche Verantwortung von Infrastrukturbetreibern und ihre verstärkte Grundrechtsbindung zu betonen. Wenn Grundrechte Freiheit schützen, indem sie Macht begrenzen, und wenn Macht stärker von Infrastrukturbetreibern ausgeübt wird als vom Staat, können sich die Grundrechte nicht nur gegen den Staat richten. Sie müssen auch diejenigen verpflichten, die durch ihre technischen Infrastrukturen diese Macht ausüben. Als privatwirtschaftliche Konglomerate können sie sich zwar grundsätzlich auf Berufs- und Eigentumsfreiheit berufen. Wie das Bundesverfassungsgericht z. B. 2016 in seinem Urteil zum Atomausstieg festgestellt hat, wird dieser Grundrechtsschutz jedoch immer schwächer, je weiter er sich vom Zweck dieser Grundrechte entfernt, den Erwerb der Lebensgrundlagen und die persönliche Freiheit zu sichern.[129] Wenn die Ausübung dieser Grundrechte zur Akkumulation von enormer gesellschaftlicher Macht führt, die die Freiheit anderer Menschen gefährdet, dann muss diese Macht – nach den Entscheidungen des Bundesverfassungsgerichts zu Fraport,[130] zum Bierdosen-Flashmob,[131] zum Fußballstadionverbot[132] und zu Social Networks[133] – durch die Grundrechte anderer begrenzt werden. „Je nach Gewährleistungsinhalt und Fallgestaltung kann … die mittelbare Grundrechtsbindung Privater einer Grundrechtsbindung des Staates … nahe oder auch gleich kommen".[134] Dies kommt für den „Schutz der Kommunikation" insbesondere dann in Betracht, „wenn private Unternehmen die Bereitstellung schon der Rahmenbedingungen öffentlicher Kommunikation selbst übernehmen und damit in Funktionen eintreten, die – wie die Sicherstellung der Post- und Telekommunikationsdienstleistungen – früher dem Staat als Aufgabe der Daseinsvorsorge zugewiesen waren".[135] Diese Überlegung dürfte vor allem für private Anbieter relevant werden, die Infrastrukturen der digitalen Gesellschaft betreiben: Je abhängiger die Gesellschaft von ihren Infrastrukturleistungen ist und je tiefgreifender ihre Leistungserbringung die Verwirklichung

[129] BVerfGE 143, 246, Rn. 218 f.

[130] BVerfGE 128, 226 (253).

[131] BVerfG, NJW (2015; S. 2485).

[132] BVerfGE 148, 267 (S. 283 f.).

[133] BVerfG (2. Kammer), NVwZ (2019), S. 959 (Rn. 15).

[134] BVerfGE 128, 226 (S. 248).

[135] BVerfGE 128, 226 (S. 249 f.); verstärkt durch BVerfG, NJW (2015), 2485 (S. 2486).

von Grundrechten, insbesondere der informationellen Selbstbestimmung und der gesellschaftlichen Kommunikation, beeinflusst, desto eher unterliegen sie einer staatsgleichen Grundrechtsbindung.

Für die Adressaten von Grundrechten gilt somit: Je größer die gesellschaftliche Macht, desto stärker muss die Bindung an Grundrechte sein.[136] Diese ist dogmatisch weiterzuentwickeln und auf die Machtzentren anzuwenden. Für die Freiheit spielt es keine Rolle, wer sie gefährdet. Angesichts der zunehmenden Machtkonzentration erwächst für Demokratie und Rechtsstaat daher im Schutz der Freiheit die wohl wichtigste Aufgabe der Zukunft.

4.4 Globalisierung des Grundrechtsschutzes

Wie aber soll Deutschland oder die Europäische Union ihre Regeln zu Beachtung der Grundrechte und zur grundrechtsverträglichen Gestaltung der Informationstechnik gegenüber global agierenden Internetkonzernen durchsetzen, von denen besondere Grundrechtsrisiken ausgehen? Das globale Internet und die Globalisierung der Herausforderungen für die Grundrechte erfordern eigentlich globale Regelungen. Die Vergangenheit zeigt jedoch, dass auf internationaler Ebene – wenn diese überhaupt gegen den Widerstand der USA und Chinas vereinbart werden könnten – als globale Datenschutzregeln allenfalls nichtssagende Allgemeinfloskeln zu erreichen sind – wie etwa die OECD-Regeln zum Datenschutz.[137]

Hilfreiche Regulierungen zum Schutz der Grundrechte sind allenfalls auf Ebene der Europäischen Union möglich. Diese haben weltweit ein großes Gewicht, auch wenn die Europäische Union hinter USA und China nur die drittgrößte Volkswirtschaft der Welt repräsentiert. Immerhin steht sie für einen Markt mit weitgehend einheitlichen oder vergleichbaren Datenschutzregeln mit über 450 Mio. Einwohnern. Mit der Datenschutz-Grundverordnung hat die Europäische Union Datenschutzregelungen geschaffen, die auch für global agierende Konzerne gelten. Hierfür ist vor allen das Betroffenenprinzip des Art. 3 Abs. 2 DSGVO relevant, das die Datenschutz-Grundverordnung weitgehend dann für anwendbar erklärt, wenn Daten von Personen in der Europäischen Union

[136] S. hierzu auch BVerfG (2. Kammer), NVwZ (2019), S. 959 (Rn. 15).

[137] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, revised 2013.

verarbeitet werden. Und ihre Regelungen sind auch gegenüber Unternehmen außerhalb der Union durchsetzbar, solange diese Geschäfte auf dem europäischen Markt tätigen wollen – wie die Sanktionen nach Art. 83 DSGVO gegenüber Apple und Google zeigen.

Die Datenschutz-Grundverordnung will außerdem ihr Datenschutzniveau, das – bei aller Verbesserungsbedürftigkeit und -fähigkeit im Einzelnen – im Vergleich zu allen anderen Datenschutzgesetzen weltweit führend ist, global exportieren. Sie lässt nämlich die Übermittlung von Daten von Personen aus der Europäischen Union in andere Ländern nach Art. 45 DSGVO vor allem dann zu, wenn die Kommission festgestellt hat, dass das Drittland ein „angemessenes Schutzniveau bietet". Um als angemessen zu gelten, müssen die Datenschutzregelungen und die Datenschutzpraxis in dem Drittland nicht dem Vorbild in der Europäischen Union exakt gleichen, aber diesem adäquat sein. Solche Angemessenheitsentscheidungen sind bisher für 13 Staaten getroffen worden. Der jüngste Anerkennungsbeschluss betrifft den nicht-öffentlichen Sektor in Japan.[138] Um diese Anerkennung zu erreichen,[139] hatte sich Japan neue Datenschutzregelungen gegeben.[140] Auch viele weitere Staaten weltweit haben – wie etwa Brasilien,[141] Chile, Süd-Korea, Kenia, Indien, Indonesien und sogar Kalifornien – haben neue Datenschutzregelungen getroffen oder bereiten solche vor, um auf der Grundlage eines Anerkennungsbeschlusses mit der Europäischen Union personenbezogene Daten ohne Beschränkung austauschen zu können.

Die Datenschutz-Grundverordnung ist weltweit ein Vorbild. Sie regelt erstmals für die gesamte Europäische Union einheitlich und unmittelbar die Grundsätze einer zentralen Gestaltungsaufgabe aller Bereiche der digitalen Gesellschaft, nämlich der Verarbeitung personenbezogener Daten. Die Verordnung hat globale Dimensionen und dient vielen Staaten als Vorbild für einen dritten Weg der Entwicklung in die digitale Welt: Zwischen dem amerikanischen Modell des rücksichtslosen Datenkapitalismus und dem chinesischen Modell der umfassenden Überwachungsdiktatur zeigt die Datenschutz-Grundverordnung einen nachahmenswerten Entwicklungspfad. Sie gibt die Richtung an, wie die Nutzung personenbezogener Daten für gesellschaftliche, ökonomische und staatliche

[138] S. näher Fujiwara, Geminn u. a. (2019, S. 204).

[139] S. Tatsumi (2019, S. 424).

[140] S. zur Reform Geminn und Fujiwara (2016, S. 363). Zur parallel erfolgten Reform des Datenschutzrechts im öffentlichen Bereich s. Fujiwara und Geminn (2016, S. 522).

[141] Brazilian-General-Data-Protection-Law, Law No. 13,709, of August 14, 2018; s. auch Hoeren und Pinelli (2020, S. 351 ff.), Gabel und Berg (2020, S. 157 ff.).

Zwecke mit der Achtung und dem Schutz von Grundrechten und Freiheiten vereinbart werden kann.

Literatur

Bieker, F., Bremert, B., & Hansen, M. (2018). Die Risikobeurteilung nach der DSGVO. *DuD – Datenschutz und Datensicherheit*, *8,* 492–496.

Bieker, F., & Hansen, M. (2017). Datenschutz „by Design" und „by Default" nach der neuen europäischen Datenschutz-Grundverordnung. *RDV – Recht der Datenverarbeitung, 4,* 165–170.

Bile, T., Geminn, C., Grigorjew, O., Husemann, C., Nebel, M., & Roßnagel, A. (2018). Fördern und Fordern: Regelungsformen zur Anreizgestaltung für einen wirksamen Schutz von Privatheit und informationeller Selbstbestimmung. In M. Friedewald (Hrsg.), *Privatheit und selbstbestimmtes Leben in der digitalen Welt. Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes* (S. 83–126). Springer Vieweg.

Bittner, T. (2021). *Geeignete Rahmenbedingungen für ein Datenschutzaudit bei Auftragsverarbeitern – Eine Untersuchung von Ausgestaltung, Nutzen und Aussagekraft.* Nomos.

Calliess, C., & Ruffert, M. (Hrsg.). (2016). *EUV/AEUV* (5. Aufl.). Beck.

Dochow, C. (2017). *Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen*. Nomos.

Eifert, M. (2017). Rechenschaftspflichten für soziale Netzwerke und Suchmaschinen. *NJW – Neue Juristische Wochenschrift, 20,* 1450–1454.

Eifert, M., & Hoffmann-Riem, W. (Hrsg.). (2009). *Innovationsfördernde Regulierung*. Duncker & Humblot.

Forum Privatheit (Ammicht Quinn, R., Baur, A., Bile, T., u. a.). (2018a). *Tracking – Beschreibung und Bewertung neuer Methoden*. White Paper, Karlsruhe.

Forum Privatheit (Eisele, D., Grigorjew, O., Karaboga, M., u. a.). (2017c). *Privatheit in öffentlichen WLANs – Spannungsverhältnisse zwischen gesellschaftlicher Verantwortung, ökonomischen Interessen und rechtlichen Anforderungen.* White Paper, Karlsruhe.

Forum Privatheit (Friedewald, M., Bieker, F., Obersteller, H., u. a.). (2017a). *Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz* (3. Aufl.). White Paper, Karlsruhe.

Forum Privatheit (Karaboga, M., Matzner, T., Morlok, T., u. a.). (2015). *Das versteckte Internet, zu Hause – Im Auto – Am Körper*. White Paper, Karlsruhe.

Forum Privatheit (Geminn, C., Hagendorff, T., Karaboga, M., u. a.). (2020b). *Risiken Künstlicher Intelligenz für die menschliche Selbstbestimmung*. Policy Paper, Karlsruhe.

Forum Privatheit (Ghiglieri, M., Hansen, M., Nebel, M., u. a.). (2016b). *Smart-TV und Privatheit, Bedrohungspotentiale und Handlungsmöglichkeiten.* Forschungsbericht, Karlsruhe.

Forum Privatheit (Martin, N., Bile T., Nebel, M., u. a.). (2019b). *Das Sanktionsregime der Datenschutz-Grundverordnung – Auswirkungen auf Unternehmen und Datenschutzaufsichtsbehörden*. Forschungsbericht, Karlsruhe.

Forum Privatheit (Roßnagel, A., Bile T., Friedewald, M., u. a.). (2018c). *Nationale Implementierung der Datenschutz-Grundverordnung, Herausforderungen – Ansätze – Strategien*. Policy Paper, Karlsruhe.

Forum Privatheit (Roßnagel, A., Bile T., Geminn, C., u. a.). (2018b). *Datenschutz stärken, Innovationen ermöglichen. Wie man den Koalitionsvertrag ausgestalten sollte*. Policy Paper, Karlsruhe.

Forum Privatheit (Roßnagel, A., Bile, T., Nebel, M., Geminn, C.). (2020a). *Die Einwilligung – Möglichkeiten und Fallstricke*, Policy Paper, Karlsruhe.

Forum Privatheit (Roßnagel, A., Friedewald, M., Geminn, C. u. a.) (2017b). *Datensparsamkeit oder Datenreichtum? Zur neuen politischen Diskussion über den datenschutzrechtlichen Grundsatz der Datensparsamkeit.* Policy Paper, Karlsruhe.

Forum Privatheit (Roßnagel, A., Geminn, C., Nebel, M., Bile, T.). (2019a). *Evaluation der Datenschutz-Grundverordnung*. Policy Paper, Karlsruhe.

Forum Privatheit (Roßnagel, A., & Nebel, M.). (2016a). *Die neue Datenschutz-Grundverordnung – Ist das Datenschutzrecht nun für heutige Herausforderungen gerüstet*. Policy Paper, Karlsruhe.

Forum Privatheit (Karaboga, M., Masur, P., Matzner, T., u. a.). (2014). *Selbstdatenschutz.* White Paper, Karlsruhe.

Friedewald, M. (Hrsg.). (2018). *Privatheit und selbstbestimmtes Leben in der digitalen Welt*. Springer Vieweg.

Führ, M. (Hrsg.). (2019). *Gemeinschaftskommentar zum Bundes-Immissionsschutzgesetz* (2. Aufl.). Heymanns.

Fujiwara, S., & Geminn, C. (2016). Reform des japanischen Datenschutzrechts im öffentlichen Bereich. Entwicklung des Rechts- und Gesetzessystems für den Datenschutz. *ZD – Zeitschrift Datenschutz, 11,* 522–528.

Fujiwara, S., Geminn, C., & Roßnagel, A. (2019). Angemessenes Datenschutzniveau in Japan. Der Angemessenheitsbeschluss der Kommission und seine Folgen. *ZD – Zeitschrift Datenschutz, 5,* 204–208.

Gabel, D., & Berg, C. (2020). Das neue brasilianische Datenschutzgesetz – DSGVO unter dem Zuckerhut. In L. Specht-Riemenschneider, B. Buchner, C. Heinze, & O. Thomsen (Hrsg.), *Festschrift für Jürgen Taeger – IT-Recht in Wissenschaft und Praxis* (S. 157). R&W Verlag.

Geminn C. L., & Roßnagel, A. *(*2015). „Privatheit" und „Privatsphäre" aus der Perspektive des Rechts – Ein Überblick. *JZ – Juristische Zeitung, 14,* 703–708.

Geminn, C. L. (2016). Das Smart Home als Herausforderung für das Datenschutzrecht – Enthält die DSGVO risikoadäquate Regelungen? *DuD – Datenschutz und Datensicherheit, 09,* 575–580.

Geminn, C. L. (2017). Risikoadäquate Regelungen für das Internet der Dienste und Dinge? *DuD – Datenschutz und Datensicherheit, 41,* 295–299.

Geminn, C. L. (2020). Betroffenenrechte verbessern – Überarbeitungsbedarf der Datenschutz-Grundverordnung. *DuD – Datenschutz und Datensicherheit, 5,* 307–311.

Geminn, C. L.(2018). Das Europäische Datenschutzrecht – Zwischen Leuchtturmfunktion und Werteexport? *DVBl – Deutsches Verwaltungsblatt, 24,* 1593–1598.

Geminn, C. L., & Fujiwara, S. (2016). Das neue japanische Datenschutzrecht. Reform des Act on the Protection of Personal Information. *ZD – Zeitschrift Datenschutz, 8,* 363–368.

Glatzner, F. (2020). Profilbildung und algorithmenbasierte Entscheidungen. *Datenschutz und Datensicherheit, 5,* 312–315.

Heberlein, H. (2020). Zwei Jahre Anwendung der DS-GVO. Der erste Evaluierungsbericht der EU-Kommission. *ZD – Zeitschrift Datenschutz, 10,* 487–492.

Hill, H. (Hrsg.). (2014). *E-Transformation. Veränderung der Verwaltung durch digitale Medien* (S. 78). Nomos.

Hoeren, T., & Pinelli, S. (2020). Das neue brasilianische Datenschutzrecht. Eine kritische Betrachtung im Vergleich mit der DS-GVO. *ZD – Zeitschrift Datenschutz, 7,* 351–354.

Hoffmann-Riem, W. (Hrsg.). (2018). *Big Data – Regulative Herausforderungen*. Nomos.

Hofmann, J. (2018). Dynamische Zertifizierung – Der Weg zu einem verordnungskonformen Cloud Computing. In A. Roßnagel, M. Friedewald, & M. Hansen (Hrsg.), *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung* (S. 293). Springer Vieweg.

Hornung, G. (2018). Sind neue Technologien datenschutzrechtlich regulierbar? Herausforderungen durch „Smart Everything". In A. Roßnagel, M. Friedewald, & M. Hansen (Hrsg.), *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung* (S. 315). Springer Vieweg.

Jandt, S. (2016). Smart Health – Wird der DSGVO den dynamischen Herausforderungen gerecht? *DuD – Datenschutz und Datensicherheit, 09,* 571–574.

Jandt, S., & Steidle, R. (Hrsg.). (2018). *Datenschutz im Internet – Rechtshandbuch zu DSGVO und BDSG*. Nomos.

Johannes, P. (2018). Grundrechtecharta und Grundgesetz. In A. Roßnagel (Hrsg.), *Das neue Datenschutzrecht. Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetz* (S. 54). Nomos.

Kamp, M., & Rost, M. (2013). Kritik an der Einwilligung. *DuD – Datenschutz und Datensicherheit, 02,* 80–84.

Keßler, O. (2017). Intelligente Roboter – Neue Technologien im Einsatz. Voraussetzungen und Rechtsfolgen des Handelns informationstechnischer Systeme. *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung, 09,* 589–594.

Knote, R., Thies, L. F., Roßnagel, A., Söllner, M., Jandt, S., & Leimeister, J. M. (2020). Rechtsverträgliche und qualitätszentrierte Gestaltung für „KI made in Germany". Ein interdisziplinärer Ansatz am Beispiel smarter persönlicher Assistenten. *Informatik Spektrum, 43*, 118. https://doi.org/10.1007/s00287-020-01252-9

Kugelmann, D. (2016). Datenfinanzierte Internetangebote – Regelungs- und Schutzmechanismen der DSGVO. *DuD – Datenschutz und Datensicherheit, 40,* 566–570.

Kühling, J., & Buchner, B. (Hrsg.). (2018). *DS-GVO – BDSG* (2. Aufl.). Beck.

Maier, N., & Bile, T. (2019). Die Zertifizierung nach der DSGVO. *DuD – Datenschutz und Datensicherheit, 8,* 478–482.

Maier, N., Lins, S., Teigeler, H., Roßnagel, A., & Sunyaev, A. (2019). Die Zertifizierung von Cloud-Diensten nach der DSGVO. *DuD – Datenschutz und Datensicherheit, 4,* 225–229.

Maier, N., Pawlowska, I. M., Lins, S., & Sunyaev, A. (2020). Die Zertifizierung nach der DSGVO. Transparenz und Vertrauen für Nutzer digitaler Dienste? *ZD – Zeitschrift Datenschutz, 9,* 445–449.

Martini, M. (2014). Big Data als Herausforderung für den Persönlichkeitsschutz und das Datenschutzrecht. *DVBl. – Deutsches Verwaltungsblatt, 129,* 1481–1489.

Meyer, J., & Hölscheidt, S. (Hrsg.). (2019). *Charta der Grundrechte der Europäischen Union* (5. Aufl.). Beck.

Nebel, M. (2020). *Persönlichkeitsschutz in Social Networks – Technische Unterstützung eines grundrechtskonformen Angebots von Social Networks*. Springer Vieweg.

Nebel, M., & Dräger, M. (2019). Altersgrenzen für die Einwilligung von Kindern nach Art. 8 DS-GVO in den einzelnen Mitgliedstaaten. *ZD-aktuell – Zeitschrift Datenschutz, 10,* 06645.

Nocun, K. (2018). Datenschutz unter Druck: Fehlender Wettbewerb bei sozialen Netzwerken als Risiko für den Verbraucherschutz. In A. Roßnagel, M. Friedewald, & M.Hansen (Hrsg.), *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung* (S. 39). Springer Vieweg.

OECD. (2013). The OECD privacy framework. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

Pallas, F. (2018). Herausforderungen, Probleme und Paradoxien des Datenschutzes. Datenschutz in Zeiten alles durchdringender Vernetzung: Herausforderungen für das Zusammenspiel von Technik und Regulierung. In A. Roßnagel, M. Friedewald, M. Hansen (Hrsg.), *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung* (S. 17). Springer Vieweg.

Reding, V. (2012). Sieben Grundbausteine der europäischen Datenschutzreform. *ZD – Zeitschrift für Datenschutz, 5,* 195–198.

Richter, P. (2016). Big Data, Statistik und die Datenschutz-Grundverordnung. *DuD – Datenschutz und Datensicherheit, 09,* 581–586.

Richter, P. (Hrsg.) (2015). *Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data.* Nomos.

Roßnagel, A. (2000). *Datenschutzaudit*. Vieweg.

Roßnagel, A. (2007). *Datenschutz in einem informatisierten Alltag*. Friedrich-Ebert-Stiftung.

Roßnagel, A. (2013). Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht. *ZD – Zeitschrift für Datenschutz, 11,* 562–567.

Roßnagel, A. (2014). Regulierung – Was leistet unser Datenschutzrecht (nicht)? In H. Hill (Hrsg.), *E-Transformation. Veränderung der Verwaltung durch digitale Medien* (S. 79). Nomos.

Roßnagel, A. (2016). Wie zukunftsfähig ist die Datenschutz-Grundverordnung? *DuD – Datenschutz und Datensicherheit, 09,* 561–565.

Roßnagel, A. (2017). *Datenschutzaufsicht nach der Datenschutz-Grundverordnung, Neue Aufgaben und Befugnisse der Aufsichtsbehörden*. Springer Vieweg.

Roßnagel, A. (2018a). Notwendige Schritte zu einem modernen Datenschutzrecht. In A. Roßnagel, M. Friedewald, & M. Hansen (Hrsg.), *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung* (S. 361–384). Springer Vieweg.

Roßnagel, A. (Hrsg.) (2018b). *Das neue Datenschutzrecht, Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze*. Nomos.

Roßnagel, A. (2019a). Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht – Zur Dogmatik der Datenverarbeitung als Grundrechtseingriff. *NJW – Neue Juristische Wochenschrift, 1–2,* 1–5.

Roßnagel, A. (2019b). Innovationen der Datenschutz-Grundverordnung – Wer greift die Chancen zu besserem Datenschutz auf? *DuD – Datenschutz und Datensicherheit, 8,* 467–472.

Roßnagel, A. (2020a). Die Evaluation der Datenschutz-Grundverordnung. Eine vertane Chance zur Verbesserung der Verordnung. *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung, 10,* 657–661.

Roßnagel, A. (2020b). Evaluation der Datenschutz-Grundverordnung. Verfahren – Stellungnahmen – Vorschläge. *DuD – Datenschutz und Datensicherheit, 5,* 287–292.

Roßnagel, A. (2020c). Technik, Recht und Macht – Zur Aufgabe des Freiheitsschutzes in Rechtsetzung und Rechtsanwendung im Technikrecht. *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung, 4,* 222–228.

Roßnagel, A. (2020d). Der Datenschutz von Kindern in der Datenschutz-Grundverordnung – Vorschläge für die Evaluierung und Fortentwicklung. *ZD – Zeitschrift für Datenschutz, 2020,* 88–92.

Roßnagel, A. (2021). Privatheit und Selbstbestimmung von Kindern in der digitalisierten Welt: Ein juristischer Blick auf die Datenschutz-Grundverordnung. In I. Stapf, R. Ammicht Quinn, J. Heesen, & N. Krämer (Hrsg.), *Aufwachsen in überwachten Umgebungen: Wie lässt sich Datenschutz in Schule und Kinderzimmer umsetzen?* (S. 165). Nomos.

Roßnagel, A., Friedewald, M., & Hansen, M. (Hrsg.). (2018). *Die Fortentwicklung des Datenschutzes – Zwischen Systemgestaltung und Selbstregulierung*. Springer Vieweg.

Roßnagel, A., & Geminn, C. L. (2020). *Datenschutz-Grundverordnung verbessern, Änderungsvorschläge aus Sicht der Verbraucher*. Nomos.

Roßnagel, A., Geminn, C., Jandt, S., & Richter, P. (2016). *Datenschutzrecht 2016 – „Smart genug für die Zukunft?", Ubiquitous Computing und Big Data als Herausforderung des Datenschutzrechts*. Kassel University Press.

Roßnagel, A., & Hornung, G. (Hrsg.). (2019). *Grundrechtsschutz im Smart Car – Kommunikation, Sicherheit und Datenschutz im vernetzten Fahrzeug*. Springer Vieweg.

Roßnagel, A., Hornung, G., Geminn, C. L., & Johannes, P. C. (Hrsg.). (2018). *Rechtsverträgliche Technikgestaltung und technikadäquate Rechtsentwicklung*. Kassel University Press.

Roßnagel, A., & Nebel, M. (2015). (Verlorene) Selbstbestimmung im Datenmeer – Privatheit im Zeitalter von Big Data. *DuD – Datenschutz und Datensicherheit, 07,* 455–459.

Roßnagel, A., Pfitzmann, A., & Garstka, H. (2001). *Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern*. Möller Druck.

Rothmann, R. (2018). Ungewollte Einwilligung? Die Rechtswirklichkeit der datenschutzrechtlichen Willenserklärung im Fall von Facebook. In A. Roßnagel, M. Friedewald, & M. Hansen (Hrsg.), *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung* (S. 59). Springer Vieweg.

Schantz, P., & Wolff, H. A. (Hrsg.). (2017). *Datenschutzgrundverordnung und Bundesdatenschutzgesetz in der Praxis*. Beck.

Schnabel, C. (2009). *Datenschutz bei profilbasierten Location Based Services – Die datenschutzadäquate Gestaltung von Service-Plattformen für Mobilkommunikation*. Kassel University Press.

Schulte, M., & Schröder, R. (Hrsg.). (2011). *Handbuch des Technikrechts* (2. Aufl.). Springer.

Simitis, S., Hornung, G., & Spiecker, gen. Döhmann, I. (Hrsg.). (2019). *Datenschutzrecht – DSGVO mit BDSG*. Nomos.

Skistims, H. (2016). *Smart Homes – Rechtsprobleme intelligenter Haussysteme unter besonderer Beachtung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*. Nomos.

Stapf, I., Ammicht Quinn, R., Friedewald, M., Heesen, J., & Krämer, N. (Hrsg.). (2020). *Aufwachsen in überwachten Umgebungen*. Nomos.

Steinmüller, W., Lutterbeck, B., Mallmann, C., Harbort, U., Kolb, G., & Schneider, J. (1971). *Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministers des Innern, BT-Drs., VI/3826*, 5.

Tatsumi, T. (2019). „Angemessene" Datenschutzaufsicht in Japan? Kurze Diagnose der ersten Angemessenheitsfeststellung unter DSGVO. *CR – Computer und Recht, 7,* 424–430.

Weichert, T. (2013). Big Data und Datenschutz. Chancen und Risiken einer neuen Form der Datenanalyse. *ZD – Zeitschrift Datenschutz, 6,* 251–259.

Weichert, T. (2020). Die DSGVO, ein – Ganz guter – Anfang. *DuD – Datenschutz und Datensicherheit 5,* 293–296.

Zuboff, S. (2018). *Das Zeitalter des Überwachungskapitalismus*. Campus.

Prof. Dr. Alexander Roßnagel ist Seniorprofessor für öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel und Sprecher des Forums Privatheit und selbstbestimmtes Leben in der digitalen Welt. Seit dem 01.03.2021 ist er Hessischer Beauftragter für Datenschutz und Informationsfreiheit.

Tamer Bile ist wissenschaftlicher Mitarbeiter in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel.

Dr. Christian L. Geminn ist Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel.

Dr. Maxi Nebel ist wissenschaftliche Mitarbeiterin in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) am Wissenschaftlichen Zentrum für Informations-Technikgestaltung (ITeG) an der Universität Kassel.

Governance der EU-Datenschutzpolitik

Harmonisierung und Technikneutralität in und Innovationswirkung der DSGVO

Murat Karaboga, Nicholas Martin und Michael Friedewald

1 Einführung

Die DSGVO stellt das weltweit ambitionierteste Gesetz zum Schutz personenbezogener Daten dar und führte zahlreiche Innovationen in das EU-Datenschutzrecht ein. Zu diesen zählen beispielsweise das Marktortprinzip, das Recht auf Datenübertragbarkeit, die Anforderungen an den Datenschutz durch Systemgestaltung (data protection by design) und durch Voreinstellungen (data protection by default) sowie die Datenschutz-Folgenabschätzung (DSFA). Auf der Ebene der Governance-Strukturen fand das Prinzip der sog. Rechenschaftspflicht Eingang in das EU-Datenschutzrecht. An die Seite gestärkter Betroffenenrechte und Aufsichtsbehörden trat die sogenannte Rechenschaftspflicht, mit der das Ziel verfolgt wurde, den Datenverarbeitern[1] einerseits mehr Verantwortung hinsichtlich der Befolgung der datenschutzrechtlichen Vorgaben zu übertragen und die Intensität dieser Verantwortung andererseits gemäß dem sog. risikobasierten Ansatz vom Risiko der jeweiligen Verarbeitung abhängig zu machen. Als Element dieser Rechenschaftspflicht wurde

[1] Aus Gründen der besseren Lesbarkeit wird im Beitrag der Begriff Datenverarbeiter statt „für die Verarbeitung Verantwortlicher“ verwendet.

M. Karaboga (✉) · N. Martin · M. Friedewald
Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe, Deutschland
E-mail: murat.karaboga@isi.fraunhofer.de

N. Martin
E-mail: nicholas.martin@isi.fraunhofer.de

M. Friedewald
E-mail: michael.friedewald@isi.fraunhofer.de

A. Roßnagel und M. Friedewald (Hrsg.), *Die Zukunft von Privatheit und Selbstbestimmung,* DuD-Fachbeiträge,
https://doi.org/10.1007/978-3-658-35263-9_2

das maximal mögliche Sanktionsmaß auf eine Bußgeldhöhe von 20 Mio. EUR oder im Falle eines Unternehmens auf bis zu 4 % seines weltweiten Jahresumsatzes festgelegt.[2] Somit sieht die DSGVO ein komplexes Schutzsystem vor: Es behält die allgemein verbindlichen Datenschutz-Prinzipien vorausgegangener Datenschutz-Gesetze, sieht eine Stärkung der Betroffenenrechte und zugleich die relative Intensivierung der Pflichten der Verarbeiter vor. Indem Aufsichtsbehörden gestärkt werden und ernstzunehmende Sanktionen verhängen können, soll gewährleistet sein, dass die Vorgaben eingehalten werden.

Die DSGVO war aber auch vielfach Kritik ausgesetzt. Von bürgerrechtlicher Seite werden vor allem die unzureichende Harmonisierung und die falsch verstandene Technikneutralität der Verordnung bemängelt. So beinhaltet die DSGVO trotz der anfänglichen Bestrebung zur Vereinheitlichung des europäischen Datenschutzrechts 70 Öffnungsklauseln. Diese ermöglichen es den Mitgliedstaaten von den Vorgaben der Verordnung abzuweichen oder diese zu konkretisieren. Daher müsse eher von einer Ko-Regulierung des Datenschutzes durch die Gesetzgeber der Union und der Mitgliedstaaten gesprochen werden. Die Harmonisierung des EU-Datenschutzes werde auf diese Weise verfehlt. Technikneutrale gesetzliche Regelungen sind hingegen relevant, damit gesetzliche Vorgaben den technischen Fortschritt nicht verhindern oder aufgrund des Fortschritts nicht mehr im intendierten Sinne anwendbar sind. Bei den DSGVO-Regelungen zur Technikneutralität wird allerdings kritisiert, dass diese nicht neutral gegenüber den Techniken, sondern gegenüber den Risiken verstanden werden. Es bleibe unberücksichtigt, dass die Risiken, die aus der Datenverarbeitung eines mittelständischen Handwerksbetriebs entstehen, üblicherweise in Umfang und Schwere anders sind als diejenigen, die aus der umfassenden und weltweiten Datenverarbeitung von Konzernen wie Google oder Facebook entstehen. Es könne deshalb resümiert werden, dass die Datenschutz-Grundverordnung sich hinsichtlich des Schutzes der Betroffenen risikoneutral verhält.[3]

Von Seiten der datenverarbeitenden Wirtschaft wird an der DSGVO insbesondere kritisiert, dass sie eine Innovationsbremse darstelle. Die European Data Coalition,[4] unter deren Dach beispielsweise Nokia, SAP und Ericsson versammelt sind, prognostizierte Ende 2015, als sich die EU-Organe auf einen Kompromisstext geeinigt hatten, dass das Aufschließen der europäischen Digitalwirtschaft an die internationale Konkurrenz aufgrund der neuen Sanktionsregelungen sowie der Rechtsunsicherheit in weite Ferne rücken werde. Die datenschutzkritische Industry Coalition

[2] Roßnagel et al. (2021).

[3] Roßnagel et al. (2021).

[4] EDC (2015).

for Data Protection[5] prognostizierte neben innovationshemmenden und wirtschaftsschädigenden Effekten, dass insbesondere KMU unter der administrativen Mehrbelastung in Folge der neuen Regelungen leiden und datengetriebene Dienste gar nicht oder nur mit Verspätung auf den europäischen Markt gelangen würden. In einer Bitkom-Umfrage aus dem Jahr 2019 gaben drei von vier Unternehmen an, dass Datenschutzanforderungen die größte Hürde beim Einsatz neuer Technologien darstellten.[6]

Vor dem Hintergrund der geschilderten ambivalenten Einschätzungen des Inhalts und der Wirkung der DSGVO adressiert der Beitrag zwei Fragen:

1. Weshalb wurde die Einführung datenschutzrechtlicher Innovationen durch eine unzureichende Harmonisierung und eine falsch verstandene Technikneutralität begleitet?
2. Welche Effekte hat die DSGVO auf die Innovationsfähigkeit von Unternehmen – wirkt sie eher innovationsfördernd oder innovationshemmend, und wie wirkt das neue Sanktionsregime?

Die erste Forschungsfrage wird mittels einer polit-historischen Analyse der Genealogie der Themen Harmonisierung und Technikneutralität beantwortet. Im Vordergrund steht dabei, mittels einer dokumentenanalytischen Vorgehensweise aufzuzeigen, welche ausschlaggebenden Diskurspositionen die Formierung der jeweiligen Politiken bewirkt haben. Im letzten Schritt wird entlang der Analyse der am politischen Aushandlungsprozess der DSGVO beteiligten Akteure gezeigt, welche Handlungsalternativen bestanden und weshalb sich die o. g. Politik-Ergebnisse durchsetzen konnten.

Die Beantwortung der zweiten Forschungsfrage erfolgt mittels einer Betrachtung der soweit verfügbaren empirischen Daten und Literatur.

2 Der politische Diskurs zur Modernisierung des europäischen Datenschutzrechts

Fragen der Harmonisierung wie der technologiespezifischen Regulierung lassen sich bis in die Anfänge der europäischen Datenschutzpolitik in den 1970er-Jahren zurückverfolgen. Später sollte die Frage der Harmonisierung Ende der 1980er-Jahre zu einer der ausschlaggebenden Gründe für die Erarbeitung der Datenschutz-

[5] ICDP (2015).

[6] Bitkom (2019).

Richtlinie von 1995 werden, die erst mit dem Inkrafttreten der DSGVO abgelöst wurde. Allerdings scheiterte der Versuch der Harmonisierung bereits in dieser Zeit (vgl. Abschn. 2.1).

Die regulatorische Adressierung der Datenschutz-Risiken bestimmter Technologien wurde zur selben Zeit zum Thema. Technische Entwicklungen auf dem Gebiet der Telekommunikation waren nicht nur Anlass für die Erarbeitung der Datenschutz-Richtlinie, sondern auch der ISDN-Richtlinie, die im Jahr 2003 von der ePrivacy-Richtlinie abgelöst und im Rahmen einer weiteren Novelle im Jahr 2009 zur Cookie-Richtlinie weiterentwickelt wurde und deren erneute Reform, diesmal hin zur ePrivacy-Verordnung, seit Anfang 2017 auf EU-Ebene verhandelt wird. Im Laufe der 2000er-Jahre forcierte die EU-Kommission vor dem Eindruck neuer Technologien zudem eine weitere bereichsspezifische Regulierung zur RFID-Technologie. Letztlich führte der Widerstand auf Seiten der Datenverarbeiter und der Mitgliedstaaten dazu, dass in den verabschiedeten Regulierungsinstrumenten vergleichsweise schwache Vorgaben zur Adressierung der technologiespezifischen Datenschutz-Risiken verankert wurden (vgl. Abschn. 2.2).

In der Datenschutzreform, die im Jahr 2009 angestoßen wurde und an deren Ende die Verabschiedung der DSGVO stand, wurde von der Kommission ein weiteres Mal die Forcierung von Harmonisierung und der Adressierung technologiespezifischer Datenschutz-Risiken angestrebt. Obwohl die Harmonisierung seitens der datenverarbeitenden Wirtschaft besonders stark eingefordert wurde, wurden die Vorschläge der Kommission zur Harmonisierung im Aushandlungsprozess der DSGVO sowohl von der Wirtschaft als auch von den Mitgliedstaaten abgelehnt. Das Europäische Parlament, die Datenschutzaufsichtsbehörden und zivilgesellschaftliche Datenschützer zeigten hingegen ein vergleichsweise geringes Interesse an der Harmonisierung. Im Ergebnis wurde im Verordnungstext eine Ko-Regulierung zwischen Unionsgesetzgeber und den Mitgliedstaaten verankert, wodurch das Ziel der Harmonisierung nicht in zufriedenstellendem Maße erreicht wurde. Die Adressierung technologiespezifischer Datenschutz-Risiken scheiterte aus ähnlichen Gründen: So hatte die Kommission in ihrem Verordnungsentwurf angekündigt, technologiespezifische Regelungen mittels delegierter und Durchführungsrechtsakte zu erlassen. Dieser Vorstoß wurde allerdings seitens der datenverarbeitenden Wirtschaft vehement abgelehnt, während die Befürworter strengerer Datenschutzregelungen kein nennenswertes Interesse an Regelungen zeigten, die technologiespezifische Datenschutz-Risiken adressieren (vgl. Abschn. 2.3).

2.1 Harmonisierung des Datenschutzrechts in der EU

Der Diskurs um die Harmonisierung von Datenschutz-Regulierungen wurde entfacht, nachdem im Laufe der 1970er-Jahre angesichts der zunehmenden Globalisierung der europäischen und der weltweiten Wirtschaft klar wurde, dass auch der Verkehr personenbezogener Daten die Grenzen der Nationalstaaten überschreiten würde. Den ersten Versuch einer internationalen Harmonisierung stellen die 1980 bzw. 1981 verabschiedeten Datenschutzrichtlinien der OECD und die Datenschutz-Konvention des Europarats dar. Nachdem mehrere europäische Staaten während der 1970er-Jahre unabhängig voneinander Datenschutz-Gesetze erlassen hatten, befürchtete die OECD die Gefahr der Erschwerung grenzüberschreitender Datenflüsse und daraus resultierender volkswirtschaftlicher Wachstumseinbußen. Die Wirkung der daraufhin ausgearbeiteten und am 23. September 1980 angenommenen OECD-Datenschutzrichtlinien blieb allerdings gering[7] Der Grund dafür lag zum einen im unverbindlichen Charakter der Richtlinien – keiner der OECD-Mitgliedstaaten war verpflichtet, den Vorgaben zu folgen. Zum anderen lag der Grund darin, dass im Hinblick auf die Umsetzung der Vorgaben in nationales Recht Selbstregulierung und gesetzliche Bestimmungen gleichgesetzt wurden, weil die nicht-europäischen OECD-Staaten kein Interesse am Erlass gesetzlicher Bestimmungen zeigten. Im Laufe der 1980er-Jahre stellte sich zunehmend heraus, dass die OECD-Richtlinien eher national divergierenden und inhaltlich unzureichenden Selbstregulierungspraktiken zuträglich waren, statt zur internationalen Harmonisierung eines effektiven Schutzniveaus bzw. -regimes beizutragen.[8]

Die am 28. Januar 1981 unterzeichnete Datenschutz-Konvention 108 des Europarats war im Vergleich zu den OECD-Richtlinien stärker grundrechtlich und weniger wirtschaftspolitisch motiviert. Zudem befürwortete die Konvention staatliche Regulierung anstelle von Selbstregulierung und entfaltete für die Unterzeichnerstaaten bindende Wirkung.[9] Mehrere der in den Folgejahren überarbeiteten nationalen Datenschutzgesetze wie das Bundesdatenschutzgesetz von 1990 und die EG-Datenschutz-Richtlinie von 1995 wurden von der Konvention beeinflusst.[10] Unklare inhaltliche Vorgaben[11] und eine abweichende Implementierung[12] führten allerdings

[7] Schiedermair (2012, S. 152 ff.), OECD (2011, S. 12–15).

[8] Bennett und Raab (2006, S. 87 ff.)

[9] Zerdick (1995, S. 81).

[10] González Fuster (2014, S. 93).

[11] European Commission (1990, S. 2 f.)

[12] Simitis et al. (2019, S. 187 f.), Rn. 110.

dazu, dass auch die Konvention die angestrebte Harmonisierungswirkung letztlich verfehlte.[13]

Ende der 1980er-Jahre wurde zwar zunehmend klar, dass die Versuche der Harmonisierung der Datenschutz-Gesetze mittels dieser Instrumente scheiterten, doch dies allein reichte nicht dafür aus, die EU-Politik zur Aktivität zu bewegen. Erst als ein aus nationalen Datenschutzaufsichtsbehörden bestehendes Akteursnetzwerk die Blockade grenzüberschreitender Datentransfers in Staaten mit unzureichenden Datenschutzgesetzen androhte und vertragsrechtliche Änderungen hin zu einer verstärkten europäischen Integration auch auf politischen Themenfeldern[14] als ermöglichender Faktor wirkten, legte die Europäische Kommission am 18. Juli 1990 ein Bündel an Vorschlägen zum Schutz personenbezogener Daten vor. Das Hauptelement dieser Vorschläge bildete die spätere EG-Datenschutz-Richtlinie, mit der das Datenschutzrecht EG-weit harmonisiert werden sollte.[15]

Bei der Ausarbeitung ihrer Regelungsvorschläge stand die Kommission vor der Herausforderung, Elemente der zwischenzeitlich zunehmend stärker divergierenden nationalen Datenschutzgesetze so zu übernehmen, dass eine möglichst große Unterstützung für ihren Richtlinienvorschlag sichergestellt würde. Den Mitgliedstaaten war generell wenig an der Erarbeitung harmonisierter Datenschutz-Regelungen gelegen. Stattdessen bezweckten sie mittels Ausübung politischen Drucks die Inkorporation ihrer nationalen Regelungen auf europäischer Ebene.[16] Zudem bedeutete die im politischen Prozess der EU angelegte, inhärente Notwendigkeit zur Kompromissfindung, dass die Kommission auch die Positionen jener Staaten – wie etwa Großbritannien – berücksichtigen musste, die beim Datenschutz weitgehend auf Selbstregulierung setzten. Da ein einheitliches Schutzniveau bei Selbstregulierungsmaßnahmen noch schwieriger zu gewährleisten ist, kollidierte dieser Ansatz mit der intendierten Harmonisierungswirkung.[17]

---

[13] Bennett und Raab (2006, S. 87 ff.)

[14] Zu nennen sind hier das 1985 unterzeichnete Schengener Abkommen und die 1986 unterzeichnete Einheitliche Europäische Akte (EEA), der später 1992 in der Unterzeichnung des Maastrichter Vertrags kulminierte (Simitis 1995, S. 453; Newman 2008, S. 115).

[15] European Commission (1990, S. 2), Nr. 1.

[16] Dass selbst die Übernahme vieler Elemente des Datenschutzrechts eines Mitgliedstaates nicht zwangsläufig zu einer größeren Unterstützung führte, verdeutlicht das Beispiel der Bundesrepublik. Obwohl die Kommission sich in ihrem 1990er-Richtlinienvorschlag stark am deutschen Datenschutzrecht orientierte, wurde der Vorschlag seitens der deutschen Ratsdelegation nicht in besonderem Maße unterstützt. Stattdessen übte die Bundesrepublik Druck auf die Kommission aus, damit im Zuge der Überarbeitung des Vorschlags weitere Bestandteile des deutschen Datenschutzrechts, etwa das Konzept des betrieblichen Datenschutzbeauftragten, in die finale Richtlinie aufgenommen werden (Simitis 1995, S. 450).

[17] Simitis (1995, S. 449 ff.)

Wie später in ihrem Legislativvorschlag zur DSGVO sah die Kommission auch in ihrem Richtlinienvorschlag für sich selbst weitgehende Rechtsetzungsbefugnisse im Hinblick auf die „für die Anwendung dieser Richtlinie auf die Besonderheiten bestimmter Bereiche erforderlichen Maßnahmen“ vor (Art. 29 DS-RL-E). Dabei sollte die Kommission von einem beratenden Ausschuss bestehend aus Vertretern der Mitgliedstaaten unterstützt werden (Art. 30 DS-RL-E). Die Empfehlungen des Ausschusses sollten jedoch nicht bindend sein, sondern von der Kommission lediglich „soweit wie möglich“ (ebd.) berücksichtigt werden. Wäre dieser Kommissionsvorschlag erfolgreich gewesen, hätte die Kommission die Befugnis gehabt, zahlreiche Details der Richtlinie unter Verweis auf ihre Anwendungsrelevanz, also etwa die Harmonisierung der Informations- und Meldepflichten usw. – unter weitgehender Übergehung nationaler Standpunkte – im Alleingang zu regulieren.[18] Entsprechend massiv wurde der Kommissionsvorschlag kritisiert: Weder die Mitgliedstaaten noch die Wirtschaft oder das Europäische Parlament begrüßten den Richtlinienentwurf. In den Folgejahren erfuhr der Kommissionsvorschlag große Veränderungen, sodass die finale Datenschutz-Richtlinie kaum mehr dem Entwurf glich.[19,20]

Gemessen an den damals in Kraft befindlichen internationalen Datenschutz-Instrumenten war die DS-RL sicherlich sowohl inhaltlich als auch im Hinblick auf ihre Harmonisierungswirkung innovativ. Denn trotz der im Aushandlungsprozess vorgenommenen zahlreichen Modifikationen des Schutzniveaus stellte sie zum Zeitpunkt ihrer Verabschiedung das strengste überstaatliche Datenschutzinstrument der Welt dar. Schließlich sollte die Richtlinie im Laufe der Jahre auch die Rolle der Datenschutz-Konvention ablösen und zum weltweit einflussreichsten Datenschutzinstrument aufsteigen.[21]

Gemessen am Inhalt der damaligen europäischen Datenschutzgesetze stellten sie dagegen eher eine diffuse Konservierung bestehender Gesetze denn eine ernsthafte Weiterentwicklung und Harmonisierung dar.[22] Dies hatte zwei Gründe. Zum einen war die Kommission darum bemüht, für ihren Richtlinienvorschlag die Zustimmung möglichst vieler Mitgliedstaaten zu gewinnen. Folglich war der bestimmende Faktor der Richtliniengestaltung die Erhöhung der Wahrscheinlichkeit seiner

[18] Bignami (2005, S. 838 f.)

[19] Bainbridge (1996, S. 25 ff.)

[20] Im Laufe des Aushandlungsprozesses wurden fast alle Befugnisse der Europäischen Kommission, die sie für sich im Hinblick auf die Harmonisierung des europäischen Datenschutzrechts vorgesehen hatte, gestrichen. Letztlich war die Kommission nur noch in die Genehmigung von Datentransfers in Drittstaaten eingebunden, verlor aber selbst dort die für sich vorgesehene herausgehobene Stellung (Bignami 2005, S. 839).

[21] Raab (2006); Greenleaf (2012).

[22] Simitis (1995, S. 451), (2001, S. 111).

Verabschiedung durch die bereits erwähnte eklektizistische Inkorporation möglichst vieler mitgliedstaatlicher Rechtselemente und nicht die Erarbeitung eines konsistenten und innovativen Datenschutzgesetzes.[23] Zum anderen führte aber auch die im politischen Prozess der EG angelegte Notwendigkeit der Erzielung von Kompromissen dazu, dass Möglichkeiten zur Weiterentwicklung und Harmonisierung der Richtlinie verspielt wurden. Letztlich versuchte die Kommission, jeden Konflikt zu vermeiden, der aus ihrer Sicht die Verabschiedung der Richtlinie gefährdet hätte. Entsprechend musste die Kommission selbst in kritischen Fällen den mitgliedstaatlichen Forderung nach nationalen Abweichungen von den Richtlinien-Vorgaben nachgeben, um das Projekt der Richtlinie nicht als Ganzes zu gefährden.[24] Die Unklarheit der Regelungen spiegelte somit den schwierigen Gesetzgebungsprozess aufgrund der unterschiedlichen Positionen der mitentscheidenden Instanzen, insbesondere im Rahmen des Ministerrats, wider.[25] Simitis attestierte daher: „Das mühsam zustandegekommene einheitliche Regelwerk droht wieder in seine nationalen Bestandteile zu zerfallen, die angestrebte „Harmonisierung" riskiert vollends zur Fiktion zu geraten.".[26] Angesichts der sich anbahnenden Probleme hinsichtlich der Erreichung der angestrebten Harmonisierung legte die Kommission ihre Hoffnung schließlich in die Implementierung der Richtlinie.[27]

In den Folgejahren bestätigten sich die Vermutungen, dass die Datenschutz-Richtlinie weder im Hinblick auf die erhoffte Harmonisierung noch hinsichtlich der Festlegung eines hohen und effektiven Datenschutzniveaus die erhoffte Wirkung erzielen würde. So resümierte die Kommission in ihrem ersten Bericht über die Durchführung der Richtlinie 2003, dass diese zwar ihren Hauptzweck in Gestalt der Gewährleistung des freien Datenverkehrs erfülle und auch der weitere Zweck der Gewährleistung eines hohen Datenschutzniveaus als erfüllt anzusehen sei, dass jedoch eine abweichende Umsetzung der Richtlinienvorgaben in nationales Recht festzustellen sei.[28] Als besonders problematisch galt, dass inakzeptable Divergenzen selbst solche Bereiche betrafen, für die eine weitgehende Harmonisierung

[23] Simitis (1995, 2001).

[24] Beispielhaft sei an dieser Stelle die Verarbeitung besonderer Kategorien personenbezogener Daten in Art. 8 DS-RL genannt. Dieser verbietet im Rahmen des ersten Absatzes zunächst die Verarbeitung, schafft im zweiten Absatz allerdings dermaßen weitreichende nationale Ausnahmeregelungen, dass vom zuvor formulierten Verbot kaum etwas übrig blieb (Simitis 2001, S. 112).

[25] Simitis (2001, S. 112)

[26] Simitis (1997, S. 282 f.)

[27] Simitis (2001, S. 111).

[28] Europäische Kommission (2003).

vorgesehen war[29,30] Dennoch vertrat die Kommission – entgegen den Forderungen der datenverarbeitenden Wirtschaft[31] – die Position, dass eine Änderung der Richtlinie in nächster Zukunft aufgrund mehrerer Faktoren nicht sinnvoll wäre. Zunächst sei aufgrund der verspäteten Umsetzung der Richtlinie in den Mitgliedstaaten keine ausreichende Erfahrungsgrundlage gegeben, eine Änderung zu dem Zeitpunkt also noch verfrüht. Daneben konstatierte die Kommission, dass viele der im Konsultationsprozess benannten Schwierigkeiten ohne eine Änderung der Richtlinie behoben werden könnten: Nicht die Richtlinie, sondern die divergierende Umsetzung in mitgliedstaatliches Recht stellten demnach das zu adressierende Problem dar. Schließlich dürfte sich die Kommission auch deshalb gegen die Änderung der Richtlinie ausgesprochen haben, da viele Akteure für den Fall einer Änderung für die Senkung des Datenschutzniveaus eintraten und die Kommission dies zu verhindern versuchte. Daher setzte die Kommission insbesondere auf freiwillige Harmonisierungsmaßnahmen der Mitgliedstaaten sowie auf die engere Zusammenarbeit zwischen den Aufsichtsbehörden unter der Anleitung der Kommission bzw. der Art.-29-Datenschutzgruppe und in einzelnen Fällen auch unter Beteiligung der Datenverarbeiter selbst.[32]

In ihrem 2007 veröffentlichten Folgebericht musste die Kommission schließlich eingestehen, dass die Divergenzen fortbestanden. Weil die Potentiale bei der Umsetzung der Richtlinie aber noch immer nicht ausgeschöpft seien und weil die fehlende Harmonisierung keine Gefahr für das Funktionieren des Binnenmarktes oder für die Gewährleistung eines hohen Schutzniveaus darstelle, formulierte die Kommission allerdings immer noch keine Notwendigkeit für eine Änderung der Richtlinie.[33]

2.2 Technologie-spezifische Datenschutz-Risiken

Die Adressierung von Datenschutz-Risiken von Technologien ist der Ausgangspunkt des Datenschutzrechts bzw. der Datenschutz-Debatten der späten 1960er- und 1970er-Jahre. Bereits die ersten Datenschutzgesetze und -debatten stellten eine Reaktion auf staatliche Kontrollvorstellungen der 1960er-Jahre dar, die eine

[29] Ebd. (2003, S. 12).

[30] So etwa im Hinblick auf Art. 8 Abs. 1 (sensible Daten), Art. 10 (Information des Betroffenen), Art. 13 (Ausnahmen im Zusammenhang mit dem Informations- und Auskunftsrecht des Betroffenen) (ebd. 2003, S. 12).

[31] Europäische Kommission (2003, S. 7 f.)

[32] Ebd. (2003, S. 8), Nr. 13, 24.

[33] Europäische Kommission (2007b, S. 10).

Zusammenführung und Auswertung von (Verwaltungs-)Datenbeständen mit Hilfe von Computern anstrebten.[34] Sowohl das hessische Landesdatenschutzgesetz aus dem Jahr 1970 als auch die weiteren Datenschutzgesetze und -instrumente, wie insb. die Europaratskonvention, stellten Versuche dar, die problematischen Aspekte der Datenverarbeitung mittels staatlicher Regulierung gesellschaftsverträglich einzuhegen.[35] Technikneutralität wurde in diesem Kontext so verstanden, dass die verabschiedeten rechtlichen Vorschriften auch bei technologischen Weiterentwicklungen grundsätzlich anwendbar bleiben und sich nicht lediglich auf bestimmte Technologien beziehen sollten.[36]

Fernab von dieser allgemeinen Technologie-Rückkopplung der Datenschutz-Gesetze setzte sich Ende der 1980er-Jahre bei einigen Vertretern der EG-Mitgliedstaaten und Europaparlamentariern sowie bei den nationalen Datenschutzaufsichtsbehörden außerdem der Gedanke durch, dass spezifische Technologien besondere Gefahren nach sich ziehen würden, die es mittels Sektor- bzw. technologie-spezifischerer Regulierung zu adressieren gelte.[37] Im Ergebnis dieser Debatten veröffentlichte die Kommission neben ihrem Vorschlag für die Datenschutz-Richtlinie auch einen Vorschlag für eine Richtlinie, mit der die Datenschutz-Gefahren neuer Telekommunikationsnetze in Gestalt von ISDN adressiert werden sollten.[38] Die ISDN-Richtlinie 97/66/EG wurde schließlich am 15. Dezember 1997 angenommen. Mit deren Überarbeitung zur sog. ePrivacy-Richtlinie 2002/58/EG wurde die Anpassung der Regelungsinhalte an den Stand der Technik bezweckt – insbesondere indem die Fokussierung auf ISDN aufgegeben und jegliche mobile, satelliten- oder kabelbasierte Kommunikationstechnologie in den Anwendungsbereich der Richtlinie aufgenommen werden sollte.[39] Von Wirtschaftsvertretern wurde der ePrivacy-Richtlinienvorschlag abgelehnt, da diese der Ansicht waren, dass die allgemeinen Rechtsvorschriften der Datenschutz-Richtlinie 95/46/EG ausreichten. Notwendige Anpassungen wären fallweise mit einem flexiblen Selbstregulierungsinstrument wie Verhaltensregeln besser zu erreichen als mit staatlicher Regulierung.[40] Nach einem konfrontativen Aushandlungsprozess, in deren Verlauf das von der Kommission vorgesehene Schutzniveau und ihre Harmonisie-

[34] Berlinghoff (2013, S. 16); Gugerli (2009).
[35] Simitis et al. (2019, S. 159 ff.)
[36] Roßnagel (2017, S. 61), §1, Rn. 42.
[37] European Commission (1990, S. 8), Nr. 18.
[38] Ebd. (1990, S. 75 ff.)
[39] Europäische Kommission (1999, S. 54, 73).
[40] Europäische Kommission (2000, S. 5, 8).

rungsvorschläge deutliche Änderungen erfuhren,[41] wurde die ePrivacy-Richtlinie (2002/58/EG) schließlich am 12. Juli 2002 angenommen.

In den Folgejahren arbeitete die Europäische Kommission an weiteren Maßnahmen zur Eindämmung technologiespezifischer Datenschutz-Risiken. Etwa zeitgleich starteten die Initiativen der Kommission zur Regulierung von datenschutzrechtlichen Auswirkungen der Radiofrequenz-Identifikation (RFID)[42] sowie zur erneuten Überarbeitung der ePrivacy-Richtlinie. Nachdem seit 2003 zunächst auf der Ebene der Mitgliedstaaten und auf der internationalen Konferenz der Datenschutzaufsichtsbehörden über die datenschutzrechtlichen Auswirkungen der RFID-Technologie diskutiert wurde, initiierte die Europäische Kommission Anfang 2006 einen öffentlichen Diskursprozess zum Thema. Ende 2005 wurde auch die Novellierung der ePrivacy-Richtlinie initiiert, mit der die Inhalte der Richtlinie an die Herausforderungen der neuen Informationssysteme und insbesondere des Internets angepasst werden sollten. Angesichts der Komplexität und Allgegenwart der neuen Informationssysteme setzte die Kommission in dieser Phase in verstärktem Maße auf die Zusammenarbeit mit den Interessenvertretern. Dazu wurden zu beiden Themensträngen umfangreiche öffentliche Konsultationen[43] durchgeführt, in deren Rahmen insgesamt mehr als 2000 Stellungnahmen bei der Kommission eingingen.[44] Schließlich veröffentlichte die Kommission im Mai 2009 eine Empfehlung zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen und im November desselben Jahres wurde auch die Novelle der ePrivacy-Richtlinie in Gestalt der sog. Cookie-Richtlinie (2009/136/EG) verabschiedet.

Die Ergebnisse beider Politikprozesse stellten eine wichtige Weiche für die künftige Kommissionspolitik im Hinblick auf die Adressierung technologie-spezifischer Risiken. Denn die RFID-Empfehlungen der Kommission fielen aufgrund des Drucks der beteiligten Akteure aus der Wirtschaft weitestgehend industriefreundlich aus: Die Kommission setzte nicht nur auf das weiche Regulierungsinstrument einer

[41] Karaboga (2021).

[42] Mit dieser neuen Technologie wurde die berührungslose Übertragung von Daten über kurze Distanzen ermöglicht. Aus der Perspektive des Datenschutzes wurde kritisiert, dass RFID-basierte Datenübertragungen für Betroffene unsichtbar seien und dadurch die informationelle Selbstbestimmung gefährdet würde (Westerholt und Döring 2004; Friedewald et al. 2009).

[43] Beim Thema RFID setzte die Kommission zudem eine ExpertInnen-Gruppe ein, die den Politikprozess zwischen Juli 2007 und März 2009 intensiv begleitete und beeinflusste (Jeuck 2009, S. 20 ff.).

[44] Jeuck (2009, S. 9); Europäische Kommission (2007a, S. 4).

Empfehlung,[45] sondern befürwortete darin anstelle verbindlicher Maßnahmen überwiegend Selbstregulierungsmaßnahmen, allen voran die Vorlage einer Datenschutzfolgenabschätzung seitens der Wirtschaftsvertreter zur Prüfung durch die Artikel-29-Datenschutzgruppe.[46] Durch den Verzicht auf ein unionsweit verbindliches Instrument war die Umsetzung der Kommissionsempfehlungen somit auf die Mitarbeit sowohl der Mitgliedstaaten als auch der datenverarbeitenden Wirtschaft angewiesen. Allerdings schaffte es die RFID-Technologie nie vollständig aus der Nische. Selbst im Jahr 2014 setzten nur etwa 10 % der in der EU ansässigen Unternehmen RFID ein.[47]

Die Cookie-Richtlinie enthielt dagegen zwar (bspw. in Art. 5 Abs. 3 und Art. 13) verbindliche Bestimmungen, die auf RFID-Systeme anwendbar waren, allerdings war deren Anwendungsbereich auf elektronische Kommunikationsdienste beschränkt.[48] Der Vorschlag der Artikel-29-Datenschutzgruppe, des Europäischen Datenschutzbeauftragten (EDSB) und des Europäischen Parlaments, den Anwendungsbereich auf jedwede Dienste der Informationsgesellschaft auszuweiten, hatte sich im Aushandlungsprozess gegenüber den Forderungen der Kommission und der Mitgliedstaaten nicht durchsetzen können. Stattdessen verwiesen Kommission und Ministerrat auf die bevorstehende Reform der Datenschutzrichtlinie.[49]

2.3 Das Ziel der Harmonisierung und die Adressierung technologie-spezifischer Datenschutz-Risiken im Aushandlungsprozess der DSGVO

Der Veröffentlichung des Kommissionsentwurfs der DSGVO am 25. Januar 2012 ging eine mehrjährige Konsultationsphase voraus. Nachdem der Reformprozess im Jahr 2008 angestoßen wurde, initiierte die Kommission in den Jahren 2009 bis 2011 zwei umfassende Konsultationsrunden, in deren Rahmen der Input hunderter Stakeholder eingeholt wurde.[50] Einen wichtigen Eckpfeiler des Reformprozesses bildete im November 2010 die Veröffentlichung des sog. Gesamtkonzepts für

[45] Im Gegensatz zu harten, also verbindlichen Regulierungsinstrumenten wie Richtlinien oder Verordnungen.

[46] Nachdem ein erster Vorschlag seitens der Art.-29-Gruppe für unzureichend befunden und abgelehnt wurde, wurde der überarbeitete Vorschlag 2011 angenommen (Spiekermann 2012).

[47] Bach et al. (2016, S. 10).

[48] Iglezakis (2013, S. 10 f.)

[49] Council (2009, S. 4).

[50] Karaboga (2021).

den Datenschutz in der EU, das die Kommissionsschlussfolgerungen aus dem ersten Konsultationsprozess enthielt.[51] Darin stellte die Kommission erstmals fest, dass die divergierende Umsetzung der Datenschutz-Richtlinie als Risiko für den freien Verkehr personenbezogener Daten im Binnenmarkt zu bewerten sei.[52] Daneben beanstandete auch eine große Mehrheit der am Konsultationsprozess beteiligten Interessenvertreter die mangelnde Harmonisierung und forderte Nachbesserungen.[53] Die Befürworter eines hohen Datenschutzniveaus versprachen sich von der Harmonisierung eine effektivere Durchsetzung der Datenschutzgesetze sowie ein Ende der Umgehung strenger Datenschutzregeln, indem Datenverarbeiter ihre Hauptniederlassung in jenem Mitgliedstaat mit dem niedrigsten Datenschutzniveau gründen.[54] Vertreter der datenverarbeitenden Wirtschaft hingegen verknüpften mit dem Wunsch nach mehr Harmonisierung die Forderung nach Abbau bürokratischer Hemmnisse beim grenzüberschreitenden Datenaustausch (so insb. im Zusammenhang mit der uneinheitlich umgesetzten Meldepflicht) und den Übergang zu einer auf Selbstregulierung fußenden Datenschutzgesetzgebung. Bestehende Probleme beim Schutz personenbezogener Daten wurden stets auf die mangelnde Harmonisierung der als zu restriktiv wahrgenommenen Regeln zurückgeführt und argumentiert, dass diese sich durch mehr Harmonisierung und Selbstregulierung statt strengerer Datenschutzregeln und neuer Rechtselemente (z. B. das Recht auf Datenportabilität oder Datenschutzfolgenabschätzungen) beheben ließen.[55] Zunächst unterstützten sowohl der Ministerrat[56] als auch das Parlament[57] die Initiative der Kommission für eine stärkere Harmonisierung.

Die durch neue Technologien und die fortschreitende Globalisierung verursachten Herausforderungen für den effektiven Schutz personenbezogener Daten waren für die Kommission sowohl Anlass für die Initiierung der Datenschutzreform[58] als auch ein maßgebliches Kriterium bei der Gestaltung des DSGVO-Kommissionsentwurfs.[59] Im Rahmen der Konsultationsprozesse standen vorwiegend die von sozialen Online-Netzwerken und Cloud-Computing ausgehenden

[51] Europäische Kommission (2010).

[52] Ebd. (2010, S. 11).

[53] European Commission (2010, S. 4 f.)

[54] BEUC (2009, S. 17 f.), Article 29 Data Protection Working Party und Working Party on Police and Justice (2009, S. 9).

[55] AmCham EU (Jan. 2011, S. 23 f.), Bitkom (2011, S. 3).

[56] Council (2011), 2, Nr. 10, 6, Nr. 26.

[57] European Parliament (2011), 5, Nr. 9.

[58] Commission (2009).

[59] Reding (2011b, S. 3); Europäische Kommission (2010); European Commission (2012).

Datenschutz-Gefährdungen[60] im Vordergrund.[61] Andere, sich entwickelnde oder absehbare, technologische Trends wie das Internet der Dinge bzw. Ubiquitous Computing, Big Data oder Künstliche Intelligenz wurden in den maßgeblichen Policy-Dokumenten hingegen an keiner Stelle erwähnt.[62]

Die Ankündigung der Kommission, die Folgen moderner Datenverarbeitungstechnologien eindämmen zu wollen, führte während des Konsultationsprozesses auf Seiten der privatwirtschaftlichen Akteure zu der Befürchtung, dass das Prinzip der Technologie-Neutralität aufgegeben werden könnte. Entsprechend vehement wurde seitens dieser Akteure argumentiert, dass die Datenschutz-Prinzipien der Richtlinie ausreichend flexibel seien, um auch auf neuere Technologien Anwendung finden zu können und dass die Einführung jedweder technologiespezifischer Regelungen unbedingt zu vermeiden sei.[63]

Die Inkorporation einer Vielzahl an delegierten und Durchführungsrechtsakten im Kommissionsentwurf zur Konkretisierung der DSGVO im Hinblick auf technologiespezifische Maßnahmen ist insbesondere als direkte Reaktion auf den Widerstand der Stakeholder zu interpretieren. Dadurch konnte es die Kommission einerseits vermeiden, unmittelbare technologiespezifische Maßnahmen zu formulieren während sie andererseits die Möglichkeit der künftigen Spezifizierung offen zu halten beabsichtigte.[64] Auf diese Weise sollten beispielsweise die abstrakten Vorgaben der Kommission im Hinblick auf den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen in Art. 23 Abs. 3 und 4, zur Sicherheit der Verarbeitung in Art. 30 Abs. 3 und 4 genauer geregelt werden können. Ebenso wurde zwar die Durchführung einer Datenschutzfolgenabschätzung bei besonders riskanten Verarbeitungen in Art. 33 Abs. 1 und 2 zur Verpflichtung gemacht, eine Spezifizierung der Risiken sollte gem. Abs. 6 allerdings erst mittels delegierter Rechtsakte erfolgen.[65]

---

[60] Reding (2011b, S. 3); Europäische Kommission (2010, S. 2); European Parliament (2011, S. 7), Nr. 18, 22; Council (2011, S. 2), Nr. 13

[61] In eingeschränkter Weise fanden auch das Web 2.0 im Allgemeinen, die zunehmend mobile Internet-Nutzung und RFID Erwähnung (Reding 2011b, S. 3; Europäische Kommission 2010, S. 2.).

[62] Reding (2011b, 2012b); European Commission (2012); Europäische Kommission (2010); Commission (2010).

[63] European Commission (2010, S. 3 f.), auch: ACT et al. (2009, S. 4).

[64] Ratsvorsitz (2012, S. 3).

[65] Für unwesentliche Aspekte der Verordnung, wie z. B. die Festlegung technischer Bedingungen (insbesondere Standardvorlagen oder Standardverfahren), sah der Kommissionsentwurf den Rückgriff auf das Instrument der Durchführungsrechtsakte vor, womit zugleich der Grad

Diese Vorgehensweise der Kommission lässt sich darüber hinaus aber auch als das Ergebnis einer notwendigen Lehre aus vergangenen Fehlschlägen in der EU-Datenschutzregulierung interpretieren: Einerseits hinkt staatliche Regulierung der Technikentwicklung stets hinterher[66] und andererseits hat sich technikneutrale Regulierung zu einem politischen Paradigma entwickelt, das in der Praxis nicht immer die intendierten Resultate mit sich gebracht hat.[67] Denn jede Regulierung bleibt, trotz des Versuchs mittels technikneutraler Regulierung Weiterentwicklungen nicht auszuschließen, stets an die realen technologischen Gegebenheiten gekoppelt, die den Ausgangspunkt eines politischen Entscheidungsprozesses bilden. Dadurch, dass Gesetzgebungsprozesse mehrere Jahre in Anspruch nehmen können, kann nicht wirksam ausgeschlossen werden, dass die verabschiedeten Regelungen selbst dann veraltet sind, wenn zum Entwurfszeitpunkt bestimmte Risiken unter Einhaltung der Technikneutralität explizit adressiert wurden. Der Blick auf die Dauer der Entscheidungsprozesse der EU-Datenschutzpolitiken zeigt, dass deren offizielle Verhandlungsphase durchschnittlich 42 Monate, also etwas mehr als drei Jahre dauerte. Noch deutlicher wird das Bild, wenn beachtet wird, dass zentrale Gestaltungsentscheidungen (das Agenda-Setting) häufig bereits in der Vorbereitungsphase eines Gesetzesvorschlags getroffen werden und nach Beginn des formellen Gesetzgebungsprozesses nur schwer modifiziert werden können.[68] Wenn auch die Vorbereitungsphasen der datenschutzpolitischen Gesetzgebungsprozesse miteinberechnet werden, ergibt sich ein noch höherer Wert von 83 Monaten bzw. sechseinhalb Jahren (vgl. Tab. 1).[69] In dieser Zeit kann sich technologisch viel verändern und fundamentale Änderungen sind nach Abschluss der Agenda-Setting-Phase nur schwer möglich. Im Falle der DSGVO bauten die vorgeschlagenen Bestimmungen wie beispielsweise das Recht auf Vergessenwerden oder das Recht auf Datenportabilität auf den spezifischen Debatten über die Einhegung der Folgen sozialer Online-Netzwerke. Die Themen Big Data und das Internet der Dinge rückten ab 2013 und insb. 2014 und somit erst nach Abschluss der Agenda-Setting-Phase in den Mittelpunkt der datenschutzpolitischen Debatte (vgl. z. B. den Debattenüberblick

der möglichen Einflussnahme des Europäischen Parlaments und des Ministerrats bei der Festlegung dieser Bedingungen reduziert worden wäre.

[66] Bräutigam et al. (1990, S. 18); Boehme-Neßler (2009).

[67] Reed (2007).

[68] Fouilleux et al. (2005, S. 617).

[69] Sofern im Falle der DSGVO nicht der Zeitpunkt ihrer Annahme, sondern ihres Wirksamwerdens zur Berechnung herangezogen wird, verlängert sich die Dauer gar auf knapp 9 Jahre (Mai 2009 bis April 2018).

Tab. 1 Überblick über die Dauer datenschutzpolitischer Gesetzgebungsprozesse auf EU-Ebene (eigene Zusammenstellung)

Datenschutz-Vorhaben	Beginn der Vorbereitungen	Offizieller Beginn	Verab-schiedung	Dauer des Verfahrens in Jahren	
				Offizieller Gesetzgebungs-prozesses	… inkl. Vor-bereitungen
EU-DSRL 95/46/EG	01.12.1989	18.07.1990	24.10.1995	5	5
ISDN-RL 97/66/EG	01.12.1989	18.07.1990	15.12.1997	7	8
EU-DS-VO 45/2001	01.12.1989	17.09.1999	18.12.2000	1	11
ePrivacy-RL 2002/58/EG	01.11.1999	12.07.2000	12.07.2002	2	2
JI-Rahmenbeschluss	27.05.1998	04.10.2005	27.11.2008	3	10
Cookie-RL 2009/136/EG	25.11.2005	13.11.2007	25.11.2009	2	4
DSGVO und JI-RL	19.05.2009	25.01.2012	15.12.2015	3	6

in: Schirrmacher 2015).[70] Mit ihren Vorschlägen beabsichtigte die Kommission, künftig schneller auf technologische Veränderungen reagieren zu können.

Alternativ hätte die Kommission auf die Spezifizierung im Rahmen von delegierten und Durchführungsrechtsakten verzichten und stattdessen die Möglichkeit von Gesetzesänderungen bzw. des Erlasses neuer Gesetze vorziehen können. Angesichts der Historie der Datenschutzpolitik konnte jedoch auch diese Option nicht infrage kommen. Denn obwohl aufgrund fortschreitender technologisch induzierter Datenschutzgefährdungen immer neuere Datenschutzgesetze erforderlich wurden, fiel es den Befürwortern datenschutzrechtlicher Regelungen in vergangenen datenschutzpolitischen Aushandlungsprozessen stets schwer, sich gegenüber den Gegnern verbindlicher Regelungen durchzusetzen. Die verabschiedeten Datenschutzgesetze stellten häufig einen Kompromiss auf dem kleinsten gemeinsamen Nenner dar, statt echte datenschutzpolitische Innovationen mit sich zu bringen. Insofern die Kommission ein Interesse an strengeren bzw. innovativen Datenschutzregelungen hatte – davon kann angesichts des Policy-Entrepreneurship der zuständigen Justizkommissare Jacques Barrot und insbesondere Viviane Reding ausgegangen werden – kam die Möglichkeit von Gesetzesänderungen oder des Erlasses neuer Regelungen nicht infrage, da hierbei stets die Gefahr bestand, dass die auf diesem Wege verabschiedeten Regelungen nur unbefriedigende Resultate bringen würden. Zudem hätte die o. g. lange Dauer von Entscheidungsprozessen stets die Gefahr

[70] Konkrete instruktive Vorschläge zur Regelung der durch das Internet der Dinge oder Big Data verursachten Datenschutz-Gefährdungen wurden sogar erst nach der Einigung im Trilog vorgelegt (Roßnagel et al. 2016; Taylor, Floridi und Sloot 2017). Das Thema KI wurde noch später zum Gegenstand der öffentlichen Debatte.

impliziert, dass auch die neuen Regelungen bereits im Moment ihres Inkrafttretens veraltet sein könnten.[71]

Schließlich war im Laufe der 2000er-Jahre zunehmend klargeworden, dass eine Praxis der Selbstregulierung im Hinblick auf den effektiven Schutz personenbezogener Daten im Kontext neuer Technologierisiken nicht die gewünschten Ergebnisse mit sich bringen würde. Weder die Erfahrungen mit Selbstregulierung im Rahmen der RFID-Empfehlungen noch im Rahmen der Umsetzung der DSRL konnten als zufriedenstellend bezeichnet werden. Die datenverarbeitende Wirtschaft zeigte wenig Interesse am Instrument der Datenschutz-Folgenabschätzung, das mit den RFID-Empfehlungen eingeführt worden war: Nachdem ein erster Industrie-Vorschlag für ein DSFA-Konzept seitens der Datenschutzgruppe für unzureichend befunden und abgelehnt wurde, wurde der überarbeitete Vorschlag 2011 angenommen – allerdings unter Auflagen, da immer noch Mängel festgestellt wurden.[72] Und auch die einzige nennenswerte Selbstregulierungsinitiative im Rahmen der Umsetzung der DSRL, die von der European Advertising Standards Alliance (EASA) Ende der 2000er-Jahre forciert wurde, war seitens der Art. 29-Datenschutzgruppe für nicht-konform mit den Vorgaben der ePrivacy-Richtlinie befunden worden.[73]

Im Kontext der Harmonisierungsthematik bezweckte die Kommission mit ihren neuen Befugnissen zudem in verstärkter Weise Einfluss auf die harmonisierte Umsetzung der Verordnung nehmen zu können, um die Entstehung neuer Divergenzen in den Mitgliedstaaten zu vermeiden.[74] Teilweise sah der Kommissionsentwurf auch vor, dass der Europäische Datenschutzausschuss für die Gewährleistung der kohärenten Anwendung der Verordnung mitverantwortlich sein sollte. Dadurch, dass die Kommission für sich selbst auch im Hinblick auf den Ausschuss die letztverantwortliche und damit maßgebliche Steuerungskompetenz vorsah, stand im Zentrum des Kommissionsentwurfs zur Gewährleistung der Kohärenz dennoch die Kommission selbst.[75] Auch dieses Agieren der Kommission war ein Ergebnis des Widerstands der Mitgliedstaaten hinsichtlich der Harmonisierung ihrer Datenschutzregelungen. Diese Ablehnung gemeinsamer Standards seitens der Mitgliedstaaten hat Tradition und reicht über die Ablehnung wirksamer und harmonisierter Anti-Spam-Regelungen im Kontext der Cookie- und ePrivacy-Richtlinie,[76] der Verabschiedung eines angemessenen Datenschutz-Standards für den Bereich der

[71] Karaboga (2021).
[72] Spiekermann (2012).
[73] Artikel-29-Datenschutzgruppe (2011).
[74] Reding (2012a).
[75] Hornung (2012, S. 105).
[76] Karaboga (2021).

ehemaligen dritten Säule im Kontext des JI-Rahmenbeschlusses[77] bis hin zur Aufweichung der Regelungen der Datenschutz-Richtlinie zurück.[78] In allen genannten Politikprozessen führte der Druck der Mitgliedstaaten zu einer Reduktion des Harmonisierungsniveaus. Dabei wurde einerseits argumentiert, dass eine gewisse Regelungsdivergenz bereichernd wirke und andererseits, dass während der Implementierung die Entstehung von zu starken Divergenzen vermieden würde. Während einige Beobachter bereits früh Kritik an dieser Form der politisch vom Ministerrat intendierten Divergenz übten,[79] zeigte sich auch in den Gesetzesbegründungen der späteren Gesetzesreformen (s. insb. die DSGVO und JI-Richtlinie), dass die entstandenen Divergenzen als untragbar eingestuft und zum Anlass für die Reformen herangezogen wurden.

Seit der Veröffentlichung der Kommissionsvorschläge stand sowohl im politischen Aushandlungsprozess als auch in der Fachliteratur insbesondere das Handeln der Europäischen Kommission, also der Vorschlag auf eine Vielzahl von delegierten und Durchführungsrechtsakten zu setzen, in mehrfacher Hinsicht im Zentrum der Kritik. Zum einen wurde angesichts der enormen Anzahl an delegierten und Durchführungsrechtsakten die offensichtlich beabsichtigte Machtkonzentration bei der Kommission bemängelt, die dem komplexen Regelungsbedarf auf nationaler Ebene nicht gerecht werde.[80] Zum anderen wurde kritisiert, dass die vorgeschlagenen Rechtsakte sich entgegen des EU-Primärrechts auch auf wesentliche Vorschriften der Verordnung erstreckten und damit rechtswidrig seien.[81] Roßnagel u. a.[82] begrüßten stattdessen, dass die Kompetenzen, welche die Kommission für sich selbst vorgesehen hatte, den Mitgliedstaaten übertragen werden sollten. Hornung[83] trat dagegen einerseits dafür ein, Spezifizierungen möglichst im Verordnungstext selbst vorzunehmen und andererseits dafür, einen Teil der Verantwortung an den EDSA zu delegieren. Auch die privatwirtschaftlichen Akteure reagierten durchweg ablehnend auf die Kommissionsvorschläge und traten für die Löschung der Kommissionskompetenzen und die Regelung von Kernaspekten in der Verordnung selbst ein. Dabei fokussierte ein Teil der Kritik eher auf die im Rahmen der Festlegung

[77] Hert und Papakonstantinou (2009).

[78] Pearce und Platten (1998); Simitis (1997).

[79] vgl. zur DS-RL: Simitis (1997, S. 282 f.), vgl. zum JI-Rahmenbeschluss: Hert und Papakonstantinou (2009).

[80] Roßnagel (2017, S. 54 f.), Rn. 17.

[81] Hornung (2012, S. 105).

[82] Roßnagel et al. (2016, 2018).

[83] Hornung (2012).

technischer Details befürchtete Gefährdung der Technikneutralität,[84] während ein anderer Teil die absehbare Machtkonzentration bei der Kommission kritisierte[85]

Lediglich die Artikel-29-Datenschutzgruppe und der EDSB begrüßten das Instrument der delegierten und Durchführungsrechtsakte, missbilligten allerdings deren große Zahl insb. im Hinblick auf ihre Zulässigkeit und Notwendigkeit.[86] Beispielsweise lehnte die Artikel-29-Datenschutzgruppe den Kommissionsvorschlag zur Festlegung der Kriterien und Anforderungen im Hinblick auf den Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen[87] oder zur Spezifizierung des Stands der Technik im Kontext von Art. 30 (Sicherheit der Verarbeitung) ab.[88] Der Vorschlag, die Spezifizierung der Risiken, wann eine DSFA durchgeführt werden sollte, mittels eines delegierten Rechtsaktes durchzuführen, wurde hingegen unterstützt.[89]

Nachdem sich auch Parlament und Ministerrat ablehnend gegenüber den Kommissionsvorschlägen äußerten, legte die Kommission in den interinstitutionellen Verhandlungen Alternativvorschläge vor, insbesondere in Form 1) der Aufnahme von Verfahrensvorschriften in die Befugnis, 2) der Festlegung inhaltlicher Bedingungen für die Befugnis oder 3) der Einschränkung des Umfangs der Befugnis.[90] Das Europäische Parlament sah in seinen Änderungsvorschlägen schließlich die Reduzierung der Zahl der delegierten Rechtsakte von 26 auf 10, der Zahl der Durchführungsrechtsakte von 23 auf 1 und die Regelung vieler der entsprechenden Sachverhalte in der Verordnung selbst vor.[91] Da das Parlament seine Position bereits im Laufe der Jahre 2012 und 2013 festgezurrt hatte, fanden zudem die Debatten zum Internet der Dinge und zu Big Data praktisch keinen Widerhall in seiner Position. Kommission und Parlament hätten also gar nicht auf die Gefährdungslage durch Big Data, das Internet der Dinge oder gar KI eingehen können, weil die Entscheidungsprozesse in beiden Organen vor der Hochphase dieser Debatten weitestgehend abgeschlossen waren. Der Parlamentsvorschlag, einen Teil der Kommissionsvollmachten in der Verordnung selbst zu regeln, wurde jedoch vom Ministerrat mehrheitlich abgelehnt. Stattdessen sah der Ratsentwurf vor, die Mitgliedstaaten selbst in die Rolle zu versetzen, etwaige Präzisierungen und Änderungen vornehmen zu

[84] AmCham (Jan. 2012, S. 15 f.), Microsoft (2012, S. 14 f.)
[85] DigitalEurope (2012, S. 2); ACCIS (2012, S. 20).
[86] Artikel-29-Datenschutzgruppe (2012, S. 9); EDSB (2012, S. 10).
[87] Artikel-29-Datenschutzgruppe (2012, S. 26).
[88] Ebd. (2012, S. 29).
[89] Ebd. (2012, S. 32).
[90] Ratsvorsitz (2012, S. 3).
[91] Roßnagel (2017, S. 56), §1, Rn. 21.

können bzw. zu müssen.[92] Zudem wäre der Ministerrat zwar in der Lage gewesen, auf die Diskurse zum Internet der Dinge und Big Data zu reagieren, da er seine Position erst Mitte 2015 verabschiedete. Der Rat war jedoch weniger daran interessiert, risikoadäquate Schutzregelungen zu treffen, als in die Verordnung Freiräume für Big Data-Anwendungen zu integrieren.[93,94]

Im Trilog konnte sich schließlich der Ministerrat mit der Streichung der meisten delegierten und Durchführungsrechtsakte durchsetzen, sodass nur noch zwei Ermächtigungen für delegierte Rechtsakte und sieben für Durchführungsrechtsakte übrigblieben.[95] Die von der Kommission für sich selbst vorgesehene Rolle der Konkretisierung der Vorgaben der DSGVO im Hinblick auf neue Technologien wurde somit teilweise an die Mitgliedstaaten delegiert.[96] Die von der Kommission für sich selbst vorgesehene Rolle zur Gewährleistung der kohärenten Anwendung wurde hingegen teilweise an den Europäischen Datenschutzausschuss (EDSA) übertragen. Dieser wurde dahingehend ermächtigt, Leitlinien, Empfehlungen und bewährte Verfahren zu datenschutzspezifischen Fragestellungen zu erarbeiten und im Falle von Meinungsverschiedenheiten zwischen den nationalen Aufsichtsbehörden unter Rückgriff auf das sog. Kohärenzverfahren rechtsverbindliche Beschlüsse fassen zu dürfen.[97]

Insofern ist der Vorwurf gegen Kommission und Parlament unberechtigt. Da er seine Position erst Mitte 2015 verabschiedete und selbst wichtige zwischenstaatliche Einigungen erst im Laufe des Jahres 2015 erfolgten, ist der angemessene Adressat der Kritik also vielmehr der Ministerrat.

---

[92] Roßnagel (2017, S. 56), §1, Rn. 22 f.

[93] Albrecht (2015); EDRi et al. (2015, S. 3).

[94] Deshalb überrascht es auch nicht, dass Parlament und Kommission 2015 ein äußerst geringes Interesse daran zeigten, auf den Vorschlag des Ministerrats einzugehen, fundamentale Aspekte der Datenschutzregulierung vor dem Hintergrund neuer Technologien neu zu verhandeln. Da der Ministerrat bzw. die EU-Mitgliedstaaten sich in der DSGVO-Debatte stets hinter die datenverarbeitende Industrie gestellt hatten, wurde befürchtet, dass die Debatte bloß zu einer Abschwächung des historisch gewachsenen Datenschutzniveaus führen würde. Im Ergebnis vertraten Kommission wie auch Parlament die Position, dass ein Zurückfallen hinter das Schutzniveau der DSRL nicht infrage komme (Albrecht 2015).

[95] Albrecht (2016, S. 97).

[96] Roßnagel et al. (2018).

[97] Bieker (2016).

3 Wirkungen der DSGVO: Innovation, Wettbewerbsfähigkeit und Sanktionen

3.1 Datenschutz, Wettbewerbsfähigkeit und Innovation

Empirische Forschung zu den Innovationsauswirkungen von Regulierung im Allgemeinen (und von Datenschutzregulierung im Besonderen) liegt soweit nur begrenzt vor. Bisherige Arbeiten haben sich vor allem auf die Auswirkungen von Umweltverordnungen konzentriert, mit mehreren Ergebnissen, die für die Debatte um die DSGVO relevant sind und im Folgenden knapp zusammengefasst werden.[98] Zum einen kann die in der öffentlichen Debatte häufig vertretene These, dass Regulierung grundsätzlich Innovationen hemme, so nicht bestätigt werden. Im Gegenteil haben statistische Studien wiederholt positive Korrelationen zwischen Innovationsintensität und der Strenge von Umwelt- und Verbraucherschutzregulierungen identifiziert.[99] Von naiven Interpretationen dieser Ergebnisse, wonach mehr Regulierung zu mehr Innovation führt, ist natürlich abzusehen; zumal sich zahlreiche Fallstudien finden, die zeigen, dass Regulierung durchaus Technologieentwicklung blockieren kann.[100] Jedoch zeigen sie, dass die tatsächlichen Wechselwirkungen zwischen Regulierung und Innovation (sowie Wettbewerbsfähigkeit im weiteren Sinne) komplexer sind als häufig angenommen wird.

Auf der negativen Seite kann man mindestens zwei Wirkmechanismen identifizieren, wie Regulierung Innovation blockieren kann: Zum einen aufgrund des Compliance-Aufwandes gestiegene Kosten, welche (rein rechnerisch) die für Innovationsausgaben zur Verfügung stehenden Ressourcen schmälern, bzw. den Profitabilitätsgrad, welchen die Innovation erzielen muss um sich betriebswirtschaftlich zu lohnen, steigert. Zum anderen führen direkte Verbote bestimmter Anwendungen oder Prozesse dazu, dass sich die ihnen zugrunde liegenden technischen oder organisatorischen Neuerungen nicht entfalten können.[101] Weniger häufig in der Literatur diskutiert, für die Frage der DSGVO aber hoch relevant, ist ein dritter Faktor: die Rechts(un)sicherheit. Wenn Firmen nicht sicher sein können, ob ein Innovationsvorhaben erlaubt ist, werden sie es im Zweifel aufgeben, um Fehlinvestitionen zu vermeiden.

---

[98] Martin et al. (2019).

[99] Blind (2012); Rennings und Rammer (2011).

[100] z. B. Blind et al. (2004); Ollinger und Fernandez-Cornejo (1998).

[101] Martin et al. (2019).

Umgekehrt beschreibt die Literatur aber auch Mechanismen, über welche Regulierung Innovation und sogar Wettbewerbsfähigkeit stimulieren kann.[102]. Insofern Regulierung Firmen Auflagen macht, besteht ein Anreiz, technische oder organisatorische Lösungen (d. h. Innovationen) zu entwickeln, um diese Auflagen zu erfüllen. Regulierung kann damit Märkte für neue Lösungen oder Produkte schaffen. Insofern die fragliche Regulierung später von anderen Ländern übernommen wird[103] können sich dadurch Export- und Wettbewerbsvorteile für heimische Firmen ergeben.[104] Ein weiterer möglicher innovationsfördernder Mechanismus von Regulierung liegt in dem Vertrauen, das Regulierung schaffen kann. Je größer das potentielle Risiko, dem sich Verbraucher mit der Nutzung eines Produktes ausgesetzt fühlen, desto höher ihre vermutlichen Hemmungen, das Produkt tatsächlich zu nutzen. Dies dürfte insbesondere für neue, komplexe Technologien gelten, bei denen Verbraucher glauben, sie unzureichend zu verstehen oder meinen, nicht genug Erfahrungswerte zu besitzen, um Risiken einschätzen zu können. Insofern (Risiko-)Regulierung Verbrauchern glaubhaft beteuern kann, etwaige Risiken einzudämmen, kann sie deren Bereitschaft, neue Technologien zu nutzen, erhöhen und damit letztlich den Markt und die Anreize zur Innovation neuer Technologien stärken.

In Summe ist also zu konstatieren, dass die möglichen Auswirkungen von Regulierung auf Innovation vielschichtig und gegenläufig sein können. Bislang konnten keine allgemeingültigen Gesetzmäßigkeiten darüber identifiziert werden, wann und unter welchen Umständen Regulierung Innovation eher positiv bzw. negativ beeinflusst. Tatsächlich ist davon auszugehen, dass auch keine solchen Gesetzmäßigkeiten existieren, sondern dass die jeweiligen Auswirkungen auf spezifische, nur schwer verallgemeinerbare Wechselwirkungen zwischen den spezifischen Rechtsvorschriften und den Besonderheiten der jeweiligen Technik zurückgehen.

Wie sieht es nun bei der DSGVO aus? Zeigt sie eher innovationsfördernde oder -hemmende Wirkungen? Diese Frage ist leider immer noch nur sehr bedingt zu beantworten, da soweit nur eine geringe Zahl meist kleinerer Studien und Erhebungen zu diesem Thema vorliegt. Es fehlen weiterhin größere quantitative Untersuchungen, die es erlauben würden, Auswirkungen verlässlich und nach Strukturmerkmalen (Unternehmensgröße, Branche, Geschäftsmodell, Verarbeitungskontext etc.) aufgeschlüsselt nachzuzeichnen und die zu Grunde liegenden Wirkmechanismen klar zu identifizieren.

Zunächst ist zu konstatieren, dass Untersuchungen aus dem ersten Jahr nach Verabschiedung der DSGVO (2017) eher auf (wenn auch verhalten) positive

[102] Ebd. (2019), und die dort diskutierte Literatur.

[103] Bradford (2020).

[104] Jacob et al. (2005).

Auswirkungen hindeuteten. Ein Bild das sich in folgenden Jahren allerdings eintrübt. So stellen Martin u. a.[105] in Interviews mit Unternehmensgründern und auf Datenschutz spezialisierten Rechtsanwälten (N = 19) fest, dass die DSGVO (zumindest bei den interviewten Firmen) anscheinend nur in wenigen Fällen zur Aufgabe geplanter neuer Produkte oder Features führte. Umgekehrt hatten die meisten dieser Firmen aufgrund der DSGVO neue Technologien zur Unterstützung von Datensicherheits- und Datenschutz-Compliance eingeführt. Insofern alle der interviewten Firmen datenintensive Dienste anboten, mit besonders sensiblen Daten arbeiteten oder risikoreiche Verarbeitungen durchführten, kann dieses Ergebnis als Hinweis gewertet werden, dass die DSGVO zumindest keine unmäßig innovationshemmenden Wirkungen entfaltete. Ganz im Gegenteil hat sie die Entwicklung von Märkten für neue Produkte und Lösungen angestoßen, wirkte also durchaus innovationsfördernd.

Der letzte Punkt, die Entstehung neuer Märkte für Produkte und Technologien um Datenschutz umzusetzen, wird auch durch entsprechende Branchenregister bestätigt, die seit 2017 kontinuierliches und rasches Wachstum in der Zahl der einschlägigen Firmen nachweisen. Innovationsaktivitäten fokussieren sich auf ein breites Spektrum von Lösungen, von Produkten zur Governance von Datenbeständen und Datenschutz-Management über IT-Sicherheit bis zu Verfahren zur Anonymisierung bzw. Pseudonymisierung von Daten und deren Auswertung.[106]

Unglücklicherweise legen die wenigen verfügbaren quantitativen Erhebungen nahe, dass die Erfahrungen der Firmen seitdem negativer geworden sind, wobei das Gesamtbild nichtsdestotrotz widersprüchlich bleibt. Abb. 1 und 2 zeigen Ergebnisse aus mehreren repräsentativen Erhebungen des IT-Branchenverbands Bitkom. Demnach ist die Zahl der Unternehmen, welche die DSGVO als „einen Wettbewerbsvorteil für europäische Unternehmen“ sehen, seit 2017 kontinuierlich gestiegen, um mehr als die Hälfte: von nur 38 % auf 62 %. Paradoxerweise ist der Anteil der Firmen, die sagen, die DSGVO „bring[e] [ihrem eigenen] Unternehmen Vorteile“ ebenso stetig gefallen, ebenfalls um fast die Hälfte: von 39 % in 2017 auf 20 % in 2020. Gleichzeitig ist die Zahl der Firmen, die angaben, die DSGVO stelle „eine Gefahr für [ihr] Geschäft dar“ fast konstant geblieben, bei jeweils etwa 13 % (Abb. 1).

Auch die Aussagen zu den spezifischen Auswirkungen auf Innovation sind widersprüchlich. Einerseits ist die Zahl derer, die glauben, die DSGVO „verhinder[e] Innovationen in der EU“ leicht gefallen, von 37 % auf 29 %. Andererseits ist die Zahl derer, die angaben, dass „neue, innovative Projekte [in ihrem eigenen]

[105] Martin et al. (2019).

[106] IAPP (2018, 2019, 2020), IAPP und TrustArc (2019).

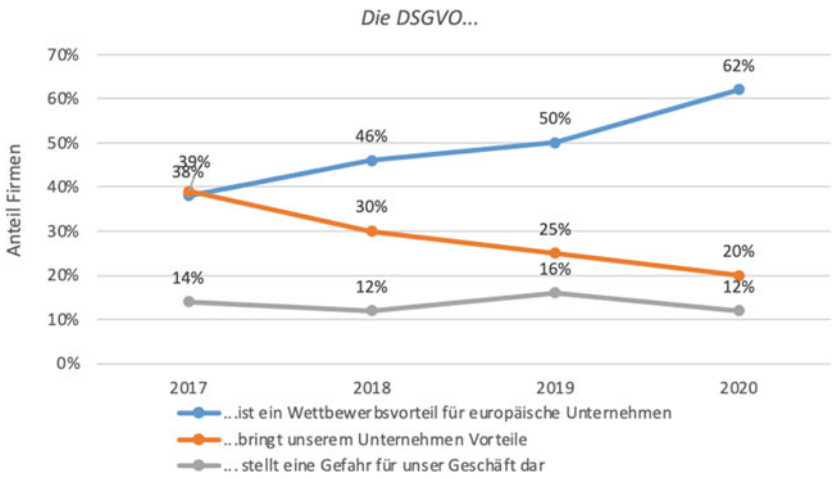

Abb. 1 Datenschutz und Wettbewerbsfähigkeit. (Quelle: Bitkom (2017, 2018, 2019, 2020))

Unternehmen aufgrund der DSGVO gescheitert sind" von lediglich 14 % im Jahr 2019 auf volle 56 % im Jahr 2020 hochgeschnellt (Abb. 2). Eine Umfrage des Wirtschaftsforschungsinstituts ZEW unter Firmen der Informationswirtschaft kommt zu ähnlichen Ergebnissen: bei 24 % hat die DSGVO „Innovationen gebremst", bei 13 % den „Einsatz neuer Technologien erschwert oder verhindert".[107] Im Android App-Markt (Google Playstore) hat die DSGVO zu massiven Rückgängen in der Entwicklung neuer Apps und zum Rückzug vieler Entwickler geführt.[108]

Eine sinnvolle positive wie normative Einordnung dieser Zahlen ist jedoch schwierig, da wesentliche Kontextinformationen fehlen. Zum einen muss grundsätzlich betont werden, dass nicht jede Innovation gesellschaftlich oder wirtschaftlich wünschenswert ist. Wenn eine im Vergleich zur Zeit vor der DSGVO peniblere Einhaltung von Datenschutzgesetzen heute dazu führt, dass z. B. ein Startup daran gehindert wird, sensible Finanzinformationen ungesichert zu verarbeiten oder eine Firma ein angedachtes Produkt stornieren muss, das Jobbewerbungen mit „Hintergrundinformationen" aus den Social-Media-Profilen der Bewerber „anreichern" sollte,[109] dann ist das vielleicht weniger ein Hinweis darauf, dass die DSGVO Innovation unmäßig einschränkt, als dass sie vielmehr ihren Zweck erfüllt. Das Problem

[107] Erdsiek (2020).
[108] Janssen et al. (2020).
[109] Martin et al. (2019).

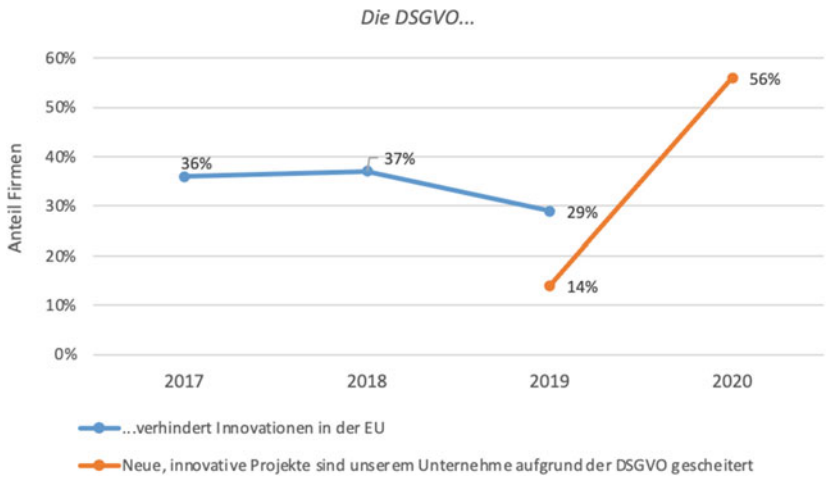

Abb. 2 Datenschutz und Innovation. (Quelle: Bitkom (2017, 2018, 2019, 2020))

ist jedoch, dass weiterhin sehr wenig darüber bekannt ist, welche „neuen, innovativen Projekte" aufgrund der DSGVO tatsächlich scheitern.

Die bereits zitierte Umfrage des Bitkom[110] legt nahe, dass insbesondere der „Aufbau von Datenpools, z. B. um Daten mit Partnern zu teilen" sowie der „Einsatz neuer Technologien, wie z. B. Big Data und KI" aufgrund der DSGVO scheitern. Aber zu welchen Zwecken sollten diese Technologien bzw. Pools eingesetzt werden? In welchen Branchen sind die betroffenen Firmen aktiv und welche Geschäftsmodelle verfolgen sie? Geht es hier um die Entwicklung von Zukunftstechnologien mit erheblichem wirtschaftlichen und ökologisch-gesellschaftlichem Mehrwert, die etwa die Energie- und Verkehrswende vorantreiben könnten? Oder geht es um Online-Werbetechnologien, die Konsument:innen immer umfassender ausspähen[111] – mit fragwürdigem gesellschaftlichen oder volkswirtschaftlichen Mehrwert?[112]

Ebenso unklar ist, was für Folgen das Scheitern dieser „neuen, innovativen Projekte" für die befragten Firmen hatte, und was „Scheitern" konkret bedeutet. Ging es hier oft um strategisch wichtige Projekte, deren Scheitern die Wettbewerbsfähigkeit der Firma maßgeblich schädigt? Oder um eine Innovationsidee unter vielen,

[110] Bitkom (2020).

[111] Christl und Spiekermann (2016).

[112] Marotta et al. (2019); Frederik und Martijn (2019).

die vielleicht sogar in abgeänderter Form in einem anderen Projekt fortentwickelt wird? Wir wissen es nicht.

Dass jedoch unter den befragten Firmen der Anteil jener, der angibt, Innovationsprojekte seien wegen der DSGVO gescheitert, massiv steigt (von 14 % auf 56 % zwischen 2019 und 2020), gleichzeitig aber der Anteil derjenigen, der angibt, sie seien durch die DSGVO bedroht, zurückgeht und auf niedrigem Niveau verharrt (12 %) und der Anteil, der in der DSGVO einen allgemeinen Wettbewerbsvorteil für europäische Firmen erblickt, ebenfalls weiterhin stark wächst (von 50 % auf 62 %) legt nahe, dass die DSGVO Innovationsaktivitäten allgemein nicht in einem kritischen Ausmaß behindert.[113]

Fast noch weniger als über die negativen Innovationsauswirkungen der DSGVO wissen wir über ihre positiven Auswirkungen. Etwa zwei Drittel der von Bitkom befragten Firmen hält sie für einen Wettbewerbsvorteil für europäische Unternehmen, wenngleich nur 20 % einen Vorteil für sich selbst erblicken. Welche konkreten Vorteile sehen diese Firmen also in der DSGVO für sich und andere? Warum ist dennoch die Hoffnung vieler Firmen, Vorteile aus der DSGVO zu ziehen, anscheinend enttäuscht worden? Schließlich hatten im Jahr 2017 noch 38 % der Befragten in ihr einen Vorteil für das eigene Geschäft gesehen. Auch auf diese Fragen gibt es soweit noch keine klaren Antworten.

Drei mögliche Wirkmechanismen, über die die DSGVO Firmen Vorteile verschaffen könnte, sind Marktvorteile, Angleichung von Wettbewerbsbedingungen und gestiegenes Verbrauchervertrauen.

Marktvorteile: Martin u. a.[114] identifizieren in ihren Interviews einen „Buy European"-Effekt: Firmen gaben an, bei Datenschutz-relevanten Produkten neuerdings europäische Anbieter zu bevorzugen, oder sogar ganz auf außereuropäische Anbieter zu verzichten, da sie glaubten, sich bei Europäern eher darauf verlassen zu können, dass die DSGVO tatsächlich eingehalten wird. Die nach dem Schrems II-Urteil weiter gestiegenen Hürden, Daten ins außereuropäische Ausland zu transferieren, dürften diesen Effekt weiter stärken.

Zwar sind solche de facto protektionistischen Effekte grundsätzlich eher wettbewerbs-, wohlstands- und innovationsschmälernd; aufgrund der Größe des europäischen Binnenmarktes dürfte dieser Schaden aber gering bleiben. Im Gegenteil,

[113] Dass der Anteil Firmen, die in der DSGVO eine direkte Gefahr für das eigene Geschäft erblickt, in den Bitkom-Umfragen seit 4 Jahren relativ stabil ist, kann ebenfalls als Hinweis interpretiert werden, dass diese Firmen-Einschätzungen zu pessimistisch sein könnten: wären diese Firmen tatsächlich ernsthaft gefährdet wäre zu erwarten, dass sie sich nach und nach aus dem fraglichen Geschäft zurückziehen, so dass ihr Anteil in den Erhebungen mit den Jahren sinken würde.

[114] Martin et al. (2019).

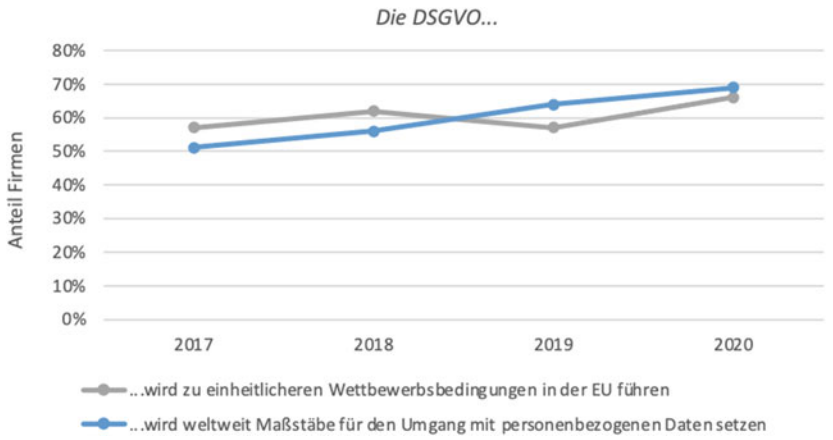

Abb. 3 Angleichung von Wettbewerbsbedingungen. (Quelle: Bitkom (2017, 2018, 2019, 2020))

wenn solche DSGVO-bedingten Marktvorteile das Wachstum europäischer Alternativen zu den dominierenden US-Konzernen befördern, könnten sie langfristig für mehr Wettbewerb und damit mehr Wohlstand und Innovation sorgen.

Angleichung von Wettbewerbsbedingungen: Die DSGVO bietet die Chance, einheitlichere Datenschutzstandards in Europa und potentiell sogar weltweit durchzusetzen, wenn sie von anderen Wirtschaftsregionen oder außereuropäischen Firmen teilweise übernommen wird. Dieses Phänomen, der sog. „Brussels Effect" kann in diversen Regulierungsfeldern beobachtet werden, einschließlich dem des Datenschutzes.[115] Das dürfte insbesondere deutschen Firmen zugutekommen, da deutsche Standards auch bisher zu den höchsten in Europa zählten. Wie Abb. 3 zeigt, erwartet eine klare Mehrheit deutscher Firmen solche Angleichungen des Datenschutzstandards und somit der Wettbewerbsbedingungen durch die DSGVO.

Verbrauchervertrauen: Verbraucherumfragen legen nahe, dass Sorgen um Datenmissbrauch weiterhin ein wichtiger Grund für die Nicht-Nutzung neuer Digitalprodukte wie z. B. Sprachassistenten sind.[116] Interviews mit Firmenvertretern bekräftigen, dass allgemeines Konsumentenmisstrauen um „Ausspähung" bisweilen auch rechtlich wie gesellschaftlich unproblematische Innovationen scheitern lässt, da

[115] Bradford (2020).

[116] Gentemann, Böhm und Esser (2018).

Unternehmen davon absehen, Technologien zu nutzen oder zu entwickeln, die Verbrauchermisstrauen wecken könnten.[117]

Regulierung ist grundsätzlich geeignet, derartige Sorgen zu nehmen und Vertrauen herzustellen. Ob die DSGVO dies bisher geschafft hat, ist indes fraglich. Die DSGVO und die in ihr verbrieften Rechte sind den meisten EU-Bürgern wenigstens in Ansätzen bekannt. 57 % (und damit 20 % mehr als 2015) wissen auch um die Existenz der Datenschutz-Aufsicht. Dieses Wissen könnte das Vertrauen der Bürger in den Schutz und die Kontrollierbarkeit ihrer Daten (und damit Technologieakzeptanz) stärken. Tatsächlich aber ist seit 2015 die Zahl der Bürger, die glauben wenigstens begrenzte Kontrolle über ihre Daten zu haben, in den meisten EU-Staaten nur unwesentlich gestiegen oder sogar gefallen. Allerdings ist auch die Zahl derer, denen diese fehlende Kontrolle Sorgen bereitet, in den meisten EU-Ländern (leicht) gefallen, wobei sie weiterhin fast überall die Mehrheit bilden.[118] Ein Paradigmenwechsel im Hinblick auf Vertrauen zeichnet sich somit noch nicht ab. Andererseits wäre ein signifikanter Vertrauensanstieg innerhalb von ein bis zwei Jahren nach Einführung der DSGVO auch kaum zu erwarten. Vertrauen dürfte sich, wenn überhaupt, langsam und über längere Zeiträume aufbauen. Insofern erscheint es eher unwahrscheinlich, dass der Faktor „Vertrauen“ schon jetzt positive Innovationswirkungen hat.

3.2 DSGVO-Sanktionen

Eine der wesentlichsten Veränderungen im deutschen und europäischen Datenschutzregime, das die DSGVO gebracht hat, ist die Verschärfung des Sanktionsregimes. Konnte vor der DSGVO in Deutschland ein Bußgeld von maximal 300.000 EUR für einen Datenschutzverstoß verhängt werden,[119] so sind jetzt Bußgelder von bis zu 20 Mio. EUR oder vier Prozent des weltweiten jährlichen Unternehmensumsatzes möglich. Zweck dieser massiven Erhöhung war es, das in den Vorjahren vielfach konstatierte „Vollzugsdefizit“ im Datenschutz – bzw. die auf Unternehmensseite verbreitete Wahrnehmung, dass Datenschutzverstöße nur

[117] Martin et al. (2019).

[118] Kantar (2019).

[119] Durch die Akkumulation mehrerer einzeln geahndeter Verstöße konnten auch vorher schon höhere Gesamtzahlungen fällig werden. So verhängte der Landesdatenschutzbeauftragte von Rheinland-Pfalz 2014 Bußgelder von insgesamt 1,3 Mio. EUR gegen ein Unternehmen.

„Kavaliers- und Bagatelldelikte“ seien[120] – zu beheben.[121] Entsprechend großes Interesse kam im Vorfeld daher der Frage zu, wie die Datenschutzbehörden mit den neuen Zwangsmitteln umgehen würden.

Wie die aktuelle Forschung darlegt, spielten Bußgelder in der Aufsichtspraxis und dem Amtsverständnis der deutschen Landesbehörden in der „vor-DSGVO-Zeit“ eher eine untergeordnete Rolle.[122] Der Fokus der Behörden lag eher auf Aufklärung, Sensibilisierung und Beratung der Öffentlichkeit und der Verantwortlichen sowie auf der Bearbeitung von Eingaben und Beschwerden betroffener Personen. Gerade bei kleinen und mittleren Unternehmen wurde (und wird) der Schwerpunkt eher darauf gelegt, datenschutzkonforme Zustände (wieder-)herzustellen – und nicht, eventuelle Verstöße möglichst hart zu sanktionieren. Vorausgesetzt, dass sich Verantwortliche kooperativ und reformwillig zeigten (und Verstöße nicht vorsätzlich begangen oder die betroffenen Personen unzumutbar hohen Risiken ausgesetzt wurden), blieben Bußgelder meist niedrig oder es wurde ganz auf sie verzichtet. Dieser eher auf Sensibilisierung und Beratung als auf aktivem „Eintreiben“ von Bußgeldern fokussierte Ansatz grenzte sich auch vom aufsichtsbehördlichen Stil mancher anderer EU-Mitgliedstaaten ab, in denen Bußgeldern schon vor der Datenschutz-Grundverordnung eine wichtigere Rolle zukam, auch zur Finanzierung der Behörden.[123]

In Interviews im Frühjahr und Sommer 2018 betonten Behördenvertreter, dass sie sich zwar einerseits verpflichtet sahen, die Spielräume des neuen Bußgeldrahmens zu nutzen und dies auch wollten, um eine bislang häufig fehlende Disziplin in den Markt zu tragen. Andererseits sahen sie aber weiterhin ihre Amtsaufgabe nicht primär im Verteilen von Bußgeldern. Ihre Botschaft lautete aber, dass bei eklatanten Missbräuchen Bußgelder künftig merkbar steigen würden, während man kooperative Akteuren, die Fehler eingestehen und abstellen wollen, konstruktiv unterstützen werde.[124]

Wie Abb. 4 zeigt, ist die Höhe sowie die Zahl der verhängten Bußgelder dennoch erheblich angestiegen.[125] Bewegte sich der durchschnittliche Gesamtwert[126] der jährlich von allen deutschen Datenschutz-Aufsichtsbehörden verhängten Bußgelder

[120] Caspar (2018).

[121] Martin et al. (2019).

[122] Martin et al. (2019); Schütz (2021).

[123] Bamberger und Mulligan (2013, 2015).

[124] Martin et al. (2019).

[125] Wie weiter unten besprochen, wurden mehrere dieser Bußgelder allerdings später von Gerichten wieder erheblich reduziert oder aus formalen Gründen aufgehoben.

[126] Unglücklicherweise finden sich vor 2019 nur spärliche und oft nicht direkt vergleichbare Daten zu den verhängten Bußgeldern in den Tätigkeitsberichten der Aufsichtsbehörden.

in den Jahren 2010 bis 2018 noch im unteren sechsstelligen Bereich, wurden 2019 bereits Bußgelder von insgesamt mehr als 25 Mio. EUR verhängt, und im Jahr 2020 waren es bis Herbst bereits mindestens 36,5 Mio. EUR.[127] Gleiches gilt für die Anzahl der Bußgelder. Es scheint, dass in keinem Jahr zwischen 2010 und 2018 mehr als 191 Bußgelder verhängt wurden, meist erheblich weniger als 150. Dagegen waren es 2019 bereits 494.[128]

Welche Auswirkungen dürfte die verschärfte Bußgeldpraxis auf Unternehmen haben? Wie die sozialwissenschaftliche Forschung zu Compliance-Verhalten von Firmen herausgearbeitet hat, sind die Faktoren, die in Unternehmensentscheidungen, sich an Recht und Gesetz zu halten, oder eben nicht, komplex.[129] Neben „ökonomischen" Erwägungen wie der erwarteten Höhe des durch Rechtsbruch zu erzielenden Gewinns diskontiert um die Wahrscheinlichkeit, entdeckt zu werden und die Schwere der zu erwartenden Strafe[130] spielen auch Fragen gesellschaftlicher Erwartungen wie etwa Reputationsverluste sowie innere normative Vorstellungen eine wichtige Rolle.[131]

Zwar ist mit dem höheren Bußgeldrahmen die zu erwartende Strafe im Entdeckungsfall wesentlich gestiegen, die weiterhin begrenzten Personalkapazitäten der Aufsichtsbehörden lassen die Wahrscheinlichkeit einer Entdeckung durch „Initiativfahndung" seitens der Aufsichtsbehörden jedoch weiterhin sehr gering erscheinen. Wichtiger für die Aufdeckung dürften Eingaben und Beschwerden aus der Bevölkerung sowie ggf. von Wettbewerbern sein. Diese sind in den vergangenen zwei Jahren ebenfalls massiv gestiegen. Hohe, medienwirksame Bußgelder

---

Sofern die einzelnen Behörden überhaupt Daten zu Zahl und Höhe der verhängten Sanktionen veröffentlichten, taten sie dies zumeist nicht jahresfein, sondern summierten Zahlen für jeweils 2 Jahre – ohne aber einen einheitlichen Zweijahresrhythmus über alle Behörden hinweg festzulegen. (D. h. Behörde A berichtete die Zahlen für 2012/2013 und 2014/2015 jeweils als Summe; Behörde B aber für 2013/2014 und 2015/2016, usw.) Um eine minimale Vergleichbarkeit herzustellen wurde daher auf Basis der verfügbaren Daten für jede Behörde für jedes Jahr von 2010 bis 2019 bzw. 2020 ein Durchschnittswert berechnet. Vor 2019 müssen die jährlichen Zahlen sowohl für die Anzahl wie den Gesamtwert der Bußgelder als lediglich grobe Schätzwerte verstanden werden. Die Entwicklung über den Zeitverlauf (Trendlinie) dürfte dennoch akkurat sein.

[127] Diese Zahlen geben die von den Aufsichtsbehörden erstinstanzlich verhängten Bußgelder wieder. Etwaige spätere Anpassungen der Summen durch Gerichte sind nicht eingerechnet, da hierzu kaum systematische Zahlen vorliegen.

[128] Bei der Kalkulation der Anzahl der Bußgelder ergab sich das gleiche Problem wie schon bei ihrem Gesamtwert, und das gleiche Berechnungsverfahren fand Anwendung.

[129] Martin et al. (2019).

[130] Becker (1968); Stigler (1970).

[131] Kagan et al. (2011).

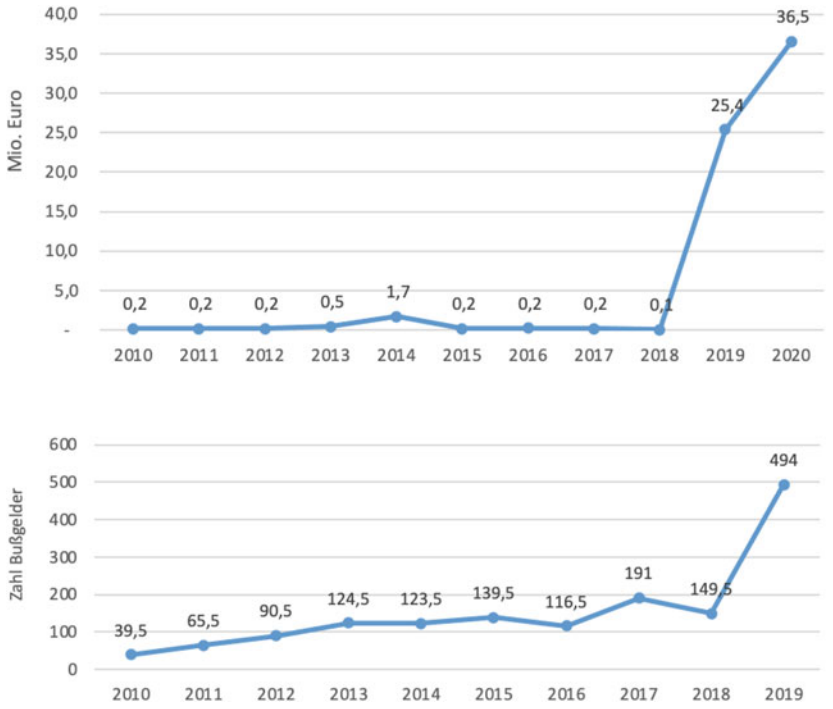

Abb. 4 Gesamtwert (oben) und Gesamtzahl (unten) verhängter Datenschutz-Bußgelder (Schätzwerte, jährlicher Durchschnitt). (Quelle: Tätigkeitsberichte der Landes- und Bundesaufsichtsbehörden, Presseberichte)

dürften diesen Zustrom am Laufen halten, insofern sie das Thema Datenschutz und Datenschutzverstöße in der öffentlichen Wahrnehmung halten.

Die Androhung von Sanktionen ist jedoch oft nicht der Hauptgrund, warum sich Firmen wie Einzelpersonen an Regeln halten. Im Gegenteil wollen sich die meisten Menschen und Organisationen aus innerer Überzeugung an Recht und Gesetz halten. Wie[132] ausführen, können hohe Strafen diesen Willen durchaus bestärken, nicht im Sinne der Abschreckung, sondern indem sie eine „kalibrierende" Wirkung entfalten: Das Sanktionsmaß ist auch eine Messlatte für Bewertung des Rechtsbruchs in der Gesellschaft: Niedrige Sanktionen deuten auf Bagatelldelikte hin, die man sich auch mit gutem Gewissen „einmal leisten kann"; schwere Sanktionen auf Verfehlungen,

[132] Martin et al. (2019).

die erhebliche moralische Schuld nach sich ziehen. Dies ist insofern relevant, als dass Datenschutzverfehlungen bislang eben doch sehr häufig als Bagatellen aufgefasst worden sind und nicht als Grundrechtsverstöße.

Der neue Bußgeldrahmen könnte helfen, diese Wahrnehmung zu verändern – vorausgesetzt, dass er tatsächlich zur dauerhaften Etablierung wesentlich höherer Bußgelder für Datenschutzverstöße führt. Bis zu welchem Grad das tatsächlich geschehen wird, scheint bislang noch offen. Gemäß Art. 83(1) DSGVO müssen Bußgelder „in jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sein. Darüber hinaus legt die DSGVO zwei Obergrenzen für Bußgelder fest (10 bzw. 20 Mio. EUR oder 10 bzw. 20 % des konzernweiten Jahresumsatzes) (Art. 83(4)(5) DSGVO). Zudem benennt sie Kriterien, anhand derer die Schwere von Verstößen bestimmt werden kann (Art. 83(2) DSGVO) und legt zumindest grob fest, dass Verstöße gegen bestimmte Auflagen schwerer wiegen (und daher mit bis zu 20 Mio. EUR Bußgeld geahndet werden können) als andere (für die maximal 10 Mio. EUR Bußgeld fällig werden können) (Art. 83(4)(5) DSGVO). Eine Untergrenze für Bußgelder legt sie jedoch nicht fest. Festzulegen, wie hoch ein „wirksames, verhältnismäßiges und abschreckendes" Bußgeld ist, bleibt damit letztlich der Auslegung der Aufsichtsbehörden vorbehalten – und der Rechtsprechung durch die Gerichte. Wie oben ausgeführt, sind die Datenschutzbehörden offensichtlich Willens, wesentlich höhere Bußgelder zu verhängen. Die kritische – soweit noch nicht beantwortbare – Frage ist, inwiefern die Gerichte dies mittragen werden. Zumindest in einem Fall – dem 9,55 Mio. EUR Bußgeld des Bundesdatenschutzbeauftragten gegen den Telefonanbieter 1&1 - hat das Gericht ein sehr hohes Bußgelder um 90 % (!) reduziert, was vom Bundesbeauftragten akzeptiert wurde.[133] Inwiefern diesem Fall breitere Bedeutung zukommt, bleibt abzuwarten; was er aber verdeutlicht, ist dass die DSGVO einen Prozess der „Rekalibrierung" der rechtlichen wie moralischen Schwere von Datenschutzverstößen eingeleitet hat, in dem wir uns noch befinden. Das tatsächlich zu erwartende Strafmaß bei Verstößen liegt damit noch im Fluß.

4 Schluss

Als die Kommission im Jahre 2012 ihren DSGVO-Entwurf vorlegte, wurden mehrere ambitionierte Ziele ins Auge gefasst: Die neue Verordnung sollte nicht nur neue innovative datenschutzrechtliche Instrumente wie die DSFA einführen, sie sollte auch den datenschutzrechtlichen Rahmen über alle EU-Mitgliedstaaten

[133] Anger (2021).

hinweg harmonisieren und zukunftstaugliche, technikneutrale Formulierungen enthalten. Damit sollte die DSGVO letzten Endes ein wirkungsvolles, neues Datenschutz-Regime etablieren, das Innovationen fördert, sofern sie keine Einschränkung des EU-Grundrechts auf Datenschutz darstellen, während zugleich mittels des neuen Sanktionsregimes böswillige Akteure von Zuwiderhandlungen abgehalten werden sollten.

Da im Hinblick auf die Aspekte der Harmonisierung und Technikneutralität bereits zum Zeitpunkt der Verabschiedung der DSGVO ein Nichterreichen der selbstgesteckten Ziele attestiert wurde, hat sich der vorliegende Beitrag im Rahmen der ersten Frage der Frage gewidmet, weshalb die Einführung datenschutzrechtlicher Innovationen durch eine unzureichende Harmonisierung und eine falsch verstandene Technikneutralität begleitet wurde. Im Rahmen der zweiten Frage wurde hingegen untersucht, welche Effekte die DSGVO auf die Innovationsfähigkeit hat und wie das neue Sanktionsregime wirkt.

Obwohl die Europäische Kommission für die vorgesehene Kompetenzverlagerung hin zur Kommission selbst während der Datenschutzreform viel gescholten wurde, hätten die initialen Kommissionsvorschläge als auch die späteren Alternativvorschläge von Kommission und Parlament die flexible Anpassung und Spezifizierung der Datenschutz-Bestimmungen an die Datenschutz-Risiken künftiger Technologien erlaubt. Dadurch wäre zudem die Wahrscheinlichkeit reduziert worden, dass bei künftigen Spezifizierungsdebatten gleich die Neuverhandlung der gesamten Verordnung aufs Tablett gebracht wird oder gar, dass sich bei einer vollumfänglichen Reform die Perspektive der Gegner eines hohen Datenschutzniveaus durchsetzen könnte, wie es in der Datenschutzpolitik regelmäßig der Fall gewesen ist und wie es auch im Falle der DSGVO wahrscheinlich der Fall gewesen wäre, wenn sich die Community der Datenschutzbefürworter einer Absenkung des Schutzniveaus nicht entschieden entgegengestellt und wenn die Snowden-Enthüllungen ihren Argumenten keinen Auftrieb verschafft hätten. [134]

In Summe wurde die DSGVO durch die Streichung der delegierten und Durchführungsrechtsakte sowohl der wirksamen Gewährleistung der Harmonisierung als auch der Möglichkeit zur Adressierung technologie-spezifischer Risiken beraubt, ohne dass im Rahmen des Trilogs geeignete Alternativen beschlossen wurden. Weder die von der Kommission vorgeschlagene Selbstermächtigung noch die vom Parlament vorgeschlagene Spezifizierung im Verordnungstext selbst konnten sich angesichts des Widerstands des Ministerrats durchsetzen.

[134] Karaboga (2021).

Die mangelnde Harmonisierung des europäischen Datenschutzrechts und die Verabschiedung einer falsch verstandenen Technikneutralität, die als Risikoneutralität wirkt, sind somit Ergebnis des Widerstands des Ministerrats bzw. der darin versammelten Mehrheit der Mitgliedstaaten, die historisch stets gegen die EU-weite Harmonisierung der datenschutzrechtlichen Regelungen eingetreten waren. Dies lässt die Hoffnung darüber, dass sich auf Ebene und unter der Verantwortung der Mitgliedstaaten mittels der Öffnungsklauseln etc. eine Anhebung des Schutzniveaus durchsetzen ließe, aussichtslos erscheinen.

Die Analyse der Wirkung der DSGVO hat gezeigt, dass es klare Hinweise darauf gibt, dass die DSGVO Innovationshindernisse schafft. Da der allgemein als legitim anerkannte Zweck der DSGVO allerdings auch gerade darin liegt, bestimmte Datenverarbeitungen (somit auch Innovationen) auszubremsen, um Rechte und Freiheiten der Betroffenen zu schützen, ist dies an sich nicht problematisch, sondern kann im Gegenteil als Beleg für die Wirksamkeit der DSGVO gewertet werden. Problematisch wäre jedoch, wenn die DSGVO die Entwicklung wichtiger Zukunftstechnologien, die etwa für die Sicherung des Wohlstandes oder den ökologischen Umbau von Wirtschaft und Gesellschaft benötigt werden, ausbremsen würde. Die wenigen Studien suggerieren aber, dass große Mehrheiten deutscher Firmen die DSGVO eher als Wettbewerbsvorteil denn als -nachteil sieht. Dies kann als Hinweis interpretiert werden, dass sie strategisch wichtige Innovation eher nicht in einem kritischen Ausmaß behindert. Aufgrund der begrenzten Datenlage sind dies jedoch letztlich Spekulationen. Wir brauchen daher detailliertere, branchen- und technologiespezifische Studien zu den Auswirkungen des Datenschutzes auf Innovation.

Der neue Sanktionsrahmen wird zunehmend von den deutschen Datenschutzbehörden angewandt. Bußgelder in Millionenhöhe werden verhängt. Die bislang verbreiteten Wahrnehmungen (i) eines „Vollzugsdefizits“ im Datenschutz und dass (ii) Datenschutzverstöße Bagatelldelikte seien, dürften somit mehr und mehr der Vergangenheit angehören. Gleichzeitig ist davon auszugehen, dass die Aufsichtsbehörden ihre Amtsaufgabe weiterhin primär nicht in der Verhängung von Bußgeldern sehen werden.

Die mit großen Ambitionen gestartete Datenschutz-Grundverordnung befindet sich nun seit mehreren Jahren in der Anwendung und wie sich zeigt, ist sie weder der ambitionierte Heilsbringer für die Europäische Digitalwirtschaft, wie sie während des Aushandlungsprozesses immer wieder beworben wurde,[135] noch ist sie die vonseiten vieler Mitgliedstaaten und der datenverarbeitenden Wirtschaft befürchtete massive Innovationsbremse, die Europa aus dem Rennen um technologische

[135] Reding (2012b, S. 128), (2011a).

Hoheit wirft. Stattdessen zeigt sich, dass die DSGVO komplexe Effekte entfaltet, die noch weiterer Untersuchung und Konkretisierung bedürfen.

Literatur

ACCIS. (2012). *Proposal for amendments to the proposed review of the EU's Data Protection Legal Framework*. Brussels. https://wiki.laquadrature.net/images/3/37/ACCIS_Position_Paper_on_Proposed_Data_Protection_Regulation_May_2012.pdf.

ACT u. a. (2009). *Joint Response by ACT, AER, AIG, EACA, EGTA, EPC, FEDMA, IAB Europe and the WFA to the European Commission Consultation on the Data Protection Directive*. https://ec.europa.eu/home-affairs/sites/default/files/what-is-new/public-consultation/2009/pdf/contributions/registered_organisations/act_joint_response_en.pdf.

Albrecht, J. P. (2015). "No EU Data Protection Standard Below the Level of 1995". *European Data Protection Law Review, 1*(1), 3–4. https://doi.org/10.21552/edpl/2015/1/4.

Albrecht, J. P. (2016). "Das neue EU-Datenschutzrecht – von der Richtlinie zur Verordnung". *Computer und Recht, 32*(2). https://doi.org/10.9785/cr-2016-0205.

AmCham, E. U. (2011). *Am Cham EU's response to the Commission communication on a comprehensive approach on data protection in the European Union*. American Chamber of Commerce to the European Union.

AmCham, E. U. (2012). *Am Cham EU – Position Paper on Data Protection*. American Chamber of Commerce to the European Union.

Anger, H. (2021). "Bußgeld wegen Datenschutzverstößen: Urteil gegen 1&1 ist rechtskräftig". *Handelsblatt*. https://www.handelsblatt.com/politik/deutschland/dsgvo-bussgeld-wegen-datenschutzverstoessenurteil-gegen-1und1-ist-rechtskraeftig/26826800.html.

Article 29 Data Protection Working Party und Working Party on Police and Justice. (2009). *The Future of Privacy: Joint Contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*. Working Paper 02356/09/EN, WP 168. Brussels.

Artikel-29-Datenschutzgruppe. (2011). *Stellungnahme 16/2011 zur Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung*. Working Paper 02005/11/DE, WP 188.

Artikel-29-Datenschutzgruppe. (2012). *Stellungnahme 08/2012 mit weiteren Beiträgen zur Diskussion der Datenschutzreform*. Working Paper 01574/12/DE, WP199.

Bach, M. P., Zoroja, J., & Loupis, M. (2016). "RFID usage in European enterprises and its relation to competitiveness". *International Journal of Engineering Business Management, 8*, 184797901668509. https://doi.org/10.1177/1847979016685093.

Bainbridge, David. (1996). *EC Data Protection Directive*. Butterworths.

Bamberger, K. A., & Mulligan, D. K. (2013). "Privacy in Europe: Initial Data on Governance Choices and Corporate Practices". *George Washington Law Review, 81*(5), 1529–1664.

Bamberger, K. A., & Mulligan, D. K. (2015). *Privacy on the ground: Driving corporate behavior in the United States and Europe*. The MIT Press.

Becker, G. S. (1968). "Crime and Punishment. An Economic Approach". *Journal of Political Economy, 76*(2), 169–217. DOI: 1010.1086/259394.

Bennett, C. J., & Raab, C. D. (2006). *The Governance of Privacy: Policy Instruments in Global Perspective*. 2nd and updated ed. MIT Press.

Berlinghoff, M. (2013). "Computerisierung und Privatheit – Historische Perspektiven". *Aus Politik und Zeitgeschichte, 63*(15-16), 14–19.

BEUC. (2009). *EU General Data Protection Framework – BEUC answer to the consultation*. Bureau Europées Unions de Consommateurs.

Bieker, F. (2016). "Enforcing Data Protection Law – The Role of the Supervisory Authorities in Theory and Practice". *Privacy and Identity Management. Facing up to Next Steps. Springer International Publishing*, 125–139. https://doi.org/10.1007/978-3-319-55783-0_10.

Bignami, F. (2005). "Transgovernmental Networks vs. Democr ernmental Networks vs. Democracy: The Case of the acy: The Case of the European Information Privacy Network". *Michigan Journal of International Law, 26*(3), 807–868.

Bitkom. (2011). *Response on the consultation for the purpose of reforming of Directive 95/46/EC*. Berlin.

Bitkom. (2017). *EU-Datenschutzgrundverordnung – Wie gut ist die deutsche Wirtschaft vorbereitet?* https://www.bitkom.org/sites/default/files/file/import/Bitkom-Charts-PK-DSGVO-17-05-2018.pdf.

Bitkom. (2018). *EU-Datenschutz-Grundverordnung – wie weit ist die deutscheWirtschaft?* https://www.bitkom.org/sites/default/files/file/import/Bitkom-Charts-PK-Privacy-Conference-19-09-2017-final.pdf.

Bitkom. (2019). *Bitkom zieht gemischte Jahresbilanz zur DS-GVO*. Berlin. https://www.bitkom.org/Presse/Presseinformation/Bitkomzieht-gemischte-Jahresbilanz-zur-DS-GVO.

Bitkom. (2020). *DS-GVO und Corona – Datenschutzherausforderungen für die Wirtschaft*. Berlin. https://www.bitkom.org/sites/default/files/2020-09/bitkom-charts-pk-privacy-29-09-2020.pdf.

Blind, K. (2012). "The influence of regulations on innovation: A quantitative assessment for OECD countries". *Research Policy, 41*(2), 391–400.

Blind, K. et al. (2004). *New products and services: Analysis of regulations shaping new markets*. Karlsruhe: Fraunhofer Institute for Systems und Innovation Research. http://publica.fraunhofer.de/documents/N-24301.html.

Boehme-Neßler, V. (2009). "Das Ende des Staates? Zu den Auswirkungen der Digitalisierung auf den Staat". *Zeitschrift für öffentliches Recht, 64*(2), 145–199. https://doi.org/10.1007/s00708-009-0024-8.

Bradford, A. (2020). *The Brussels Effect: How the European Union Rules the World*. Oxford: Oxford University Press.

Bräutigam, L., Höller, H. & Scholz, R. (1990). *Datenschutz als Anforderung an die Systemgestaltung*. VS Verlag. https://doi.org/10.1007/978-3-322-93610-3.

Caspar, J. (15. März 2018). *Die neue Architektur der Datenschutzaufsichtsbehörden in Europa*. Vortrag im Rahmen des CAST-Workshops "Recht und ITSicherheit". Darmstadt.

Christl, W., & Spiekermann, S. (2016). *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data and Privacy*. Wien: Facultas. https://crackedlabs.org/dl/Christl_Spiekermann_Networks_Of_Control.pdf.

Council. (2009). *Review of the Regulatory Framework for Electronic Communications Networks and Services*. 7062/09. Brussels: Council of the European Union. https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf.

Council. (2011). *Council Conclusions on the Communication from the Commission to the European Parliament and the Council - A Comprehensive Approach on Personal Data Protection in the European Union*. 3071st Justice and Home Affairs Council meeting Brussels, 24 and 25 February 2011. Brussels: Council of the European Union. https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf.

DigitalEurope. (2012). *DigitalEurope's Comments on Proposed European Commission's Regulation on Data Protection*. Brussels.

EDC. (2015). *Coalitions statement on the outcome of the trilogue negotiations: After more than 4 years of hard work it's disappointing that EU policy makers have stumbled at the finishing line*. European Data Coalition.

EDRi et al. (2015). *Data Protection – Badly Broken*. https://edri.org/files/DP_BrokenBadly.pdf.

EDSB. (7. März 2012). *Stellungnahme des Europäischen Datenschutzbeauftragten zum Datenschutzreformpaket*. Brussels: Der Europäische Datenschutzbeauftragte. https://edps.europa.eu/sites/default/files/publication/12-03-07_edps_reform_package_de.pdf.

Erdsiek, D. (2020). *Viele Unternehmen stellen DSGVOschlechtes Zeugnis aus. ZEW Branchenreport Informationswirtschaft*. Mannheim: Zentrum für Europäische Wirtschaftsforschung.

Europäische Kommission. (10. Nov. 1999). *Entwicklung neuer Rahmenbedingungen für elektronische Kommunikationsinfrastrukturen und zugehörige Dienste: Kommunikationsbericht 1999. KOM(1999)* 539 endg. Brüssel. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:51999DC0539&from=DE.

Europäische Kommission. (26. Apr. 2000). *Die Ergebnisse der öffentlichen Anhörung zum Kommunikationsbericht 1999 und Leitlinien für den neuen Rechtsrahmen*. KOM(2000) 239 endg. Brüssel. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0239:FIN:DE:PDF.

Europäische Kommission (15. Mai 2003). *Erster Bericht über die Durchführung der Datenschutzrichtlinie (EG 95/46). KOM(2003)* 265 endg. Brüssel. https://www.bing.com/search?q=https%3A%2F%2Feur-+lex.europa.eu%2Flegal-+content%2FDE%2FTXT%2FPDF%2F%3Furi%3DCELEX%3A52003DC0265%26amp%3Bfrom%3DE&cvid=5f90ef09474d4c279a36d404d70207f7&aqs=edge..69i57j69i58.916j0j4&FORM=ANAB01&PC=DCTS.

Europäische Kommission. (13. Nov. 2007a).*Bericht über das Ergebnis der Überprüfung des EU-Rechtsrahmens für elektronische Kommunikationsnetze und -dienste gemäß der Richtlinie 2002/21/EGund Zusammenfassung der Reformvorschläge 2007*. KOM(2007) 696 endg. Brüssel. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0696:FIN:DE:PDF.

Europäische Kommission. (7. März 2007b). *Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie*. KOM(2007) 87 endg. Brüssel. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52007DC0087&from=de.

Europäische Kommission. (4. Nov. 2010). *Gesamtkonzept für den Datenschutz in der Europäischen Union*. KOM(2010) 609 endg. Brüssel. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/uri=CELEX:52010DC0609&from=de.

European Commission. (13. Sep. 1990). *Commission Communication on the protection of individuals in relation to the processing of personal data in the community and information security*. COM(90) 314 final. Brussels. http://aei.pitt.edu/3768/1/3768.pdf.

European Commission. (2009). *Data Protection Conference "Personal Data – More Use, More Protection?*– Brüssel: Press Release.

European Commission. (2010). *Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data*. Brussels.

European Commission. (2012). *Impact Assessment Accompanying the Document Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data. Commission Staff Working Paper SEC(2012) 72 final. Brussels*. https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf.

European Parliament. (2011). *European Parliament resolution of 6 July 2011 on a comprehensive approach on personal data protection in the European Union (2011/2025(INI)*. Resolution P7_7 TA(2011)0323. https://www.europarl.europa.eu/doceo/document/TA-7-2011-0323%5C_EN.pdf.

Fouilleux, E., de Maillard, J. & Smith, A. (2005). "Technical or political? The working groups of the EU Council of Ministers". *Journal of European Public Policy, 12*(4), 609–623. https://doi.org/10.1080/13501760500160102.

Frederik, J., & Martijn, M. (2019). "The new dot com bubble is here: it's called online advertising". *The Correspondent*. https://thecorrespondent.com/100/the-new-dot-com-bubble-is-here-its-calledonline-advertising/872445200-5450b1fe.

Friedewald, M. et al. (29. März 2009). *Privacy and Trust in the Ubiquitous Information Society: Analysis of the impact of convergent and pervasive ICT on privacy and data protection and needs and options for development of the legal framework*. Final Study Report (D4), Prepared for the European Commission, DG INFSO. Karlsruhe: Fraunhofer ISI. https://bookshop.europa.eu/en/privacy-and-trust-in-the-ubiquitous-information-society-pbKK0414601/.

Gentemann, L., Böhm, K.,& Esser, R. (2018). *Zukunft der Consumer Technology 2018: Marktentwicklung, Trends, Mediennutzung,Technologien, Geschäftsmodelle*. Berlin: Bitkom. https://www.bitkom.org/sites/default/files/file/import/180822-CT-Studie-2018-online.pdf.

González Fuster, G. (2014). The Emergence of Personal Data Protection as a Fundamental Right of the EU. *Springer International Publishing*. https://doi.org/10.1007/978-3-319-05023-2.

Greenleaf, G. (2012). "The influence of European data privacy standards outside Europe: implications for globalization of Convention 108". *International Data Privacy Law, 2*(2), 68–92. https://doi.org/10.1093/idpl/ips006.

Gugerli, D. (2009). *Suchmaschinen. Die Welt als Datenbank*. Berlin: Suhrkamp.

Hert, Paul de und Vagelis Papakonstantinou. (2009). "The data protection framework decision of 27 November 2008 regarding police and judicial cooperation in criminal matters – A modest achievement however not the improvement some have hoped for". *Computer Law & Security Review, 25*(5), 403–414. https://doi.org/10.1016/j.clsr.2009.07.008.

Hornung, G. (2012). "Eine Datenschutz- Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.1.2012". *ZD – Zeitschrift für Datenschutz, 2012*(3), 99–106.

IAPP. (2018). *Privacy Tech Vendor Report*. Version 2.4e. Portsmouth, NH: International Association of Privacy Professionals. https://iapp.org/media/pdf/resource_center/2018TechVendorReport.pdf.

IAPP. (2019). *2019 Privacy Tech Vendor Report*. Version 3.2. Portsmouth, NH: International Association of Privacy Professionals. https://iapp.org/media/pdf/resource_center/2019TechVendorReport.pdf.

IAPP. (2020). *2020 Privacy Tech Vendor Report*. Version 4.2. Portsmouth, NH: International Association of Privacy Professionals. https://iapp.org/media/pdf/resource_center/2020TechVendorReport.pdf.

IAPP und TrustArc. (2019). *How Privacy Tech Is Bought and Deployed*. https://iapp.org/media/pdf/resource_center/privac_tech_bought_and_deployed_IAPPTrustArc_2019.pdf.

ICDP. (2015). *Europe's New Data Rules Take a Wrong Turn*. Press Release. Brussels: Industry Coalition for Data Protection.

Iglezakis, I. (14. Juni 2013). *Regulation Models Addressing Data Protection Issues in the EU Concerning RFID Technology*. https://doi.org/10.2139/ssrn.2279433. https://ssrn.com/abstract=2279433.

Jacob, K. et al. (2005). *Lead Markets for Environmental Innovations*. Bd. 27. ZEW Economic Studies. Mannheim: Physica.

Janssen, R. et al. (7. Mai 2020). *GDPR and the Lost Generation of Innovative Apps*. Vortrag im Rahmen des MaCCI EpoS Virtual IO Seminar. https://www.youtube.com/watch?v=vByIitkHeMc.

Jeuck, L. (2009). *Datenschutz in der EU: Der Einfluss transnationaler Akteure auf die RFID-Empfehlung der Europäischen Kommission*. PIPE – papers on international political economy 2/2009. Berlin: Arbeitsstelle Internationale Politische Ökonomie. http://nbn-resolving.de/urn:nbn:de:101:1-20100422167.

Kagan, Robert A., Neil Gunningham und Dorothy Thornton (2011). "Fear, Duty, and Regulatory Compliance. Lessons from Three Research Projects". *Explaining Compliance: Business Responses to Regulation*. Hrsg. von Christine Parker, Vibeke Lehmann Nielsen und Neil Gunningham. Cheltenham: Edward Elgar, S. 37–58. https://doi.org/10.4337/9780857938732.0000.

Kantar. (2019). *The General Data Protection Regulation*. Special Eurobarometer 487a. https://doi.org/10.2838/579882.

Karaboga, M. (2021). "Die Entstehung der EU-Datenschutz-Grundverordnung: Policy- Analyse unter besonderer Berücksichtigung der Rolle zeitgenössischer Privatheitsverständnisse". Inauguraldissertation. Frankfurt am Main: Johann-Wolfgang-Goethe-Universität.

Marotta, V., Vibhanshu, A., & Acquisti, A. (2019). "Online Tracking and Publishers' Revenues: An Empirical Analysis". *2019 Workshop on the Economics of Information Security*. https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_38.pdf.

Martin, N., & Bile, T. et al. (2019). *Das Sanktionsregime der Datenschutz-Grundverordnung: Auswirkungen auf Unternehmen und Datenschutzaufsichtsbehörden*. Forschungsbericht. Karlsruhe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt.

Martin, N., & Matt, C. et al. (2019). "How Data Protection Regulation Affects Startup Innovation". *Information Systems Frontiers, 21*(6), 1307–1324. https://doi.org/10.1007/s10796-019-09974-2.

Microsoft. (2012). *The EU's Proposed Data Protection Regulation: Microsoft's Position*.

Newman, A. L. (2008). "Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive". *International Organization, 62*(1). https://doi.org/10.1017/s0020818308080041.

OECD. (2011). *The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines*. DSTI/ICCP/REG(2010)6/FINAL Unclassified. Paris: OECD Directorate for Science, Technology and Industry: Committee for Information, Computer and Communications Policy: Working Party on Information Security and Privacy. https://doi.org/10.1787/5kgf09z90c31-en.

Ollinger, M., & Fernandez-Cornejo, J. (1998). "Innovation and regulation in the pesticide industry". *Agricultural and Resource Economics Review, 27*(1), 15–27.

Pearce, G., & Platten, N. (1998). "Achieving personal data protection in the European Union". *JCMS: Journal of Common Market Studies, 36*(4), 529–547. https://doi.org/10.1111/1468-5965.00138.

Raab, C. D. (2006). "The Governance of Global Issues: Protecting Privacy in Personal Information". In von Mathias, K.-A. & Zürn, M. (Hrsg.),*New Modes of Governance in the Global System* (S. 125–153). London: Palgrave Macmillan. https://doi.org/10.1057/9780230372887_6.

Ratsvorsitz. (2012). *Datenschutzpaket – Bericht über die unter zyprischem Vorsitz erzielten Fortschritte*. Vermerk des Vorsitzes für den Rat 16525/1/12 REV 1. Brüssel: Rat der Europäischen Union. https://data.consilium.europa.eu/doc/document/ST-16525-2012-REV-1/de/pdf.

Reding, V. (18. Mai 2011a). *The reform of the EU Data Protection Directive: the impact on businesses*. SPEECH/11/349. Brussels. https://ec.europa.eu/commission/presscorner/detail/hr/SPEECH_11_349.

Reding, V. (2011b). "The upcoming data protection reform for the European Union". *International Data Privacy Law, 1*(1), 3–5. https://doi.org/10.1093/idpl/ipq007.

Reding, V. (26. Okt. 2012a). *Justice Council: Making Good Progress on Our Justice for Growth Agenda*. SPEECH/12/764. Luxembourg. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_12_764.

Reding, V. (2012b). "The European data protection framework for the twenty-first century". *International Data Privacy Law, 2*(3), 119–129. https://doi.org/10.1093/idpl/ips015.

Reed, Chris (Sep. 2007). "Taking Sides on Technology Neutrality". *SCRIPT-ed, 4*(3), 263–284. https://doi.org/10.2966/scrip.040307.263.

Rennings, K., & Rammer, C. (2011). "The impact of regulation-driven environmental innovation on innovation success and firm performance". *Industry and Innovation, 18*(3), 255–283. https://doi.org/10.1080/13662716.2011.561027.

Richtlinie 2002/58/EG. (31. Juli 2002). "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 (Datenschutzrichtlinie für elektronische Kommunikation)". *Amtsblatt der Europäischen Gemeinschaften* L 201, S. 37–47. http://eur-lex.europa.eu/LexUriServ/LexUriServ.douri=CELEX:32002L0058:de:HTML.

Richtlinie 2009/136/EG. (18. Dez. 2009). "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". *Amtsblatt der Europäischen Gemeinschaften* L 337, S. 11–36. https://eur-lex.europa.eu/LexUriServ/LexUriServ.douri=OJ:L:2009:337:0011:0036:de:PDF.

Roßnagel, A. (Hrsg.). (2017). *Europäische Datenschutz-Grundverordnung*, (S. 342). Baden-Baden: Nomos.

Roßnagel, A., Bile, T., & Friedewald, M. et al. (2018). *Nationale Implementierung der Datenschutz-Grundverordnung: Herausforderungen – Ansätze -Strategien*. Policy Paper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. https://www.forum-privatheit.de/forumprivatheit-de/publikationen-und-downloads/veroeffentlichungendes-forums/positionspapiere-policy-paper/Policy-Paper-Nationale-Implementierung-der-DSGVO_DE.pdf.

Roßnagel, A., Bile, T., & Geminn, C.L. et al. (2021). "Neue Konzepte für den Grundrechtsschutz in der digitalen Welt". In: *Die Zukunft von Privatheit und Selbstbestimmung: Analysen und Empfehlungen zum Schutz der Grundrechte in der digitalen Welt*. Hrsg. von Michael Friedewald und Alexander Roßnagel. DuDFachbeiträge. Wiesbaden: Springer Vieweg.

Roßnagel, A., Geminn C. L. et al. (2016). *Datenschutzrecht 2016. "Smart" genug für die Zukunft?, Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts*. Bd. 4. ITeG - Interdisciplinary Research on Information System Design. Kassel: Kassel University Press. http://www.upress.uni-kassel.de/katalog/abstract.php?978-3-7376-0154-2.

Roßnagel, A., Nebel, M. & Richter, P. (2015). "Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO". *ZD - Zeitschrift für Datenschutz, 10*, 455–460.

Schiedermair, S. (2012). *Der Schutz des Privaten als internationales Grundrecht*. Tübingen: Mohr Siebeck.

Schirrmacher, F. (2015). *Technologischer Totalitarismus: Eine Debatte*. Berlin: Suhrkamp.

Schütz, P. (2021). "Data Protection Authorities under the EU General Data Protection Regulation - a new global benchmark?" In: *The Handbook on Regulatory Authorities*. Hrsg. von Martino Maggetti, Fabrizio Di Mascio und Alessandro Natalini. Cheltenham: Edward Elgar.

Simitis, S. . (1995). From the market to the polis: The EU Directive on the protection of personal data. *Iowa Law Review, 80*, 445–469.

Simitis, S. (1997). "Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz?" *Neue Juristische Wochenschrift, 50*(5), 281–288.

Simitis, S. (2001). "Data Protection in the European Union - The Quest for Common Rules". *1997 European Community Law*, (S. 95–142). Hrsg. von Philip Alston. Bd. VIII/1. Collected Courses of the Academy of European Law. The Hague: Kluwer Law International.

Simitis, S. et al. (2019). "Einleitung". *Datenschutzrecht: DSGVO mit BDSG*, (S. 158–240). Hrsg. von Spiros Simitis, Gerrit Hornung und Indra Spiecker gen. Döhmann. Baden-Baden: Nomos.

Spiekermann, S. (2012). "The RFID PIA - Developed by Industry, Endorsed by Regulators". *Privacy Impact Assessment* (S. 323–346). Hrsg. von David Wright und Paul De Hert. Bd. 6. Law, Governance, and Technology. Dordrecht: Springer.

Stigler, G. J. (1970). "The Optimum Enforcement of Laws". *Journal of Political Economy, 78*(3), 526–536. https://doi.org/10.1086/259646.

Taylor, L., Luciano, F. & van der Sloot, B. (2017). Group Privacy. *Springer International Publishing*. https://doi.org/10.1007/978-3-319-46608-8.
Westerholt, M. von, & Döring, W. (2004). "Datenschutzrechtliche Aspekte der Radio Frequency Identification (RFID)". *Computer und Recht, 20*(9), 710–716.
Zerdick, T. (1995). "European Aspects of Data Protection: What Rights for the Citizen?" *Legal Issues of Economic Integration, 22*(2), 59–86.

Dr. des. Murat Karaboga ist Wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für System- und Innovationsforschung ISI im Competence Center Neue Technologien.

Dr. Nicholas Martin ist Wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für System- und Innovationsforschung ISI im Competence Center Neue Technologien.

Dr. Michael Friedewald leitet das Geschäftsfeld „Inofmations- und Kommunikationstechnik" am Fraunhofer-Institut für System- und Innovationsforschung ISI in Karlsruhe. Er ist Koordinator des „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt".

Datenökonomien: Verbraucherverhältnisse und Geschäftsmodelle

Zum Zusammenspiel zwischen Unternehmen und Verbrauchern in der Datenökonomie

Herausforderungen und neue Gestaltungsansätze

Thomas Hess, Christian Matt, Verena Thürmel und Mena Teebken

1 Einführung

Durch die immer stärkere Durchdringung von Wirtschaft und Gesellschaft mit digitalen Technologien werden in bislang ungekanntem Maß Daten (teil-) automatisch erhoben, gespeichert und verarbeitet. Exemplarisch sind Technologien wie künstliche Intelligenz, Web-Tracking oder Blockchain zu nennen. Der Zugang zu großen Datenbeständen kann wiederum das Entscheidungsverhalten von Unternehmen und Verbrauchern verändern, mitunter sogar auch über die Grenzen von physischer und digitaler Welt hinweg. Heutzutage ist es einfacher möglich, Daten aus unterschiedlichen Quellen miteinander zu verknüpfen und auszuwerten.

T. Hess (✉) · V. Thürmel · M. Teebken
Institut für Digitales Management und Neue Medien,
Ludwig-Maximilians-Universität München, München, Deutschland
E-Mail: thess@lmu.de

V. Thürmel
E-Mail: thuermel@lmu.de

M. Teebken
E-Mail: teebken@lmu.de

C. Matt
Institut für Wirtschaftsinformatik, Universität Bern, Bern, Schweiz
E-Mail: christian.matt@iwi.unibe.ch

A. Roßnagel und M. Friedewald (Hrsg.), *Die Zukunft von Privatheit und Selbstbestimmung,* DuD-Fachbeiträge,
https://doi.org/10.1007/978-3-658-35263-9_3

Ebenso stehen leistungsfähige, IT-gestützte Verfahren zur Auswertung dieser Daten zur Verfügung, die darauf aufbauend Prognosen zukünftiger Entwicklungen ableiten können.[1]

In einer derartigen „Datenökonomie“ entstehen zahlreiche Möglichkeiten für Unternehmen, wie etwa bessere Einblicke in das Konsumentenverhalten oder die Identifikation von Interessen und Verhaltensmustern.[2] Verfügt ein Anbieter über mehr Informationen über (potentielle) Kunden, so kann er generell ein zielgruppengerechteres Angebot erstellen und komplementäre Güter anbieten. Auch ist die Nutzung von Kundendaten teils essentiell für das Erbringen bestimmter datengetriebener Dienstleistungen und kritisch für die Innovationstätigkeit zahlreicher Unternehmen, insbesondere für Startups.[3] So erproben Unternehmen aktuell Erlösmodelle, die auf der verstärkten Verwertung „personenbezogener Daten“ beruhen. Ebenfalls bieten Daten auch direktes Monetarisierungspotenzial; sie werden zu einem ökonomisch handelbaren Gut, welches durch spezialisierte Anbieter auf sogenannten Datenmärkten angeboten wird.[4]

Auch für Konsumenten hat diese Entwicklung durchaus Vorteile, wie etwa eine bessere Anpassung von Dienstleistungen anhand von deren Präferenzen sowie schnellere und zielgerichtetere Suchmöglichkeiten. Ebenso haben Konsumenten verstärkt die Möglichkeit, personenbezogene Daten als eine Art Zahlungsmittel einzusetzen, um hierdurch bspw. Apps kostenfrei nutzen zu können. Im ersten Schritt ist hierfür jedoch die Preisgabe von Daten durch den Konsumenten erforderlich und diese wird im Kontext der zunehmenden Digitalisierung häufig kritisch diskutiert. Auch hier ist das Zusammenspiel von Anbieter und Nachfrager eine geeignete Sichtweise zur Illustration des Basiskontexts. Ein (potentieller) Kunde wird generell abwägen, ob er der Verwendung von Daten zustimmt. Die Preisgabe von Daten wird vom Konsumenten häufig per se zunächst als tendenziell risikoreich eingeschätzt. Demgegenüber muss ein positiver Nutzen stehen, der die möglichen Risiken aufwiegt. Das Individuum berücksichtigt bei dieser Entscheidung ein ökonomisches Kalkül, am Ende dessen die Entscheidung für oder gegen die Nutzung eines Dienstes steht.[5] Je mehr Daten ein Anbieter erfragt, umso höher muss der daraus resultierende Nutzen

[1] Kelleher et al. (2015).

[2] Ochs et al. (2019).

[3] Martin et al. (2019).

[4] Bründl et al. (2015).

[5] Dinev und Hart (2006).

für den Konsumenten sein, um diesen zur Preisgabe seiner Daten zu bewegen. „Pokert" ein Anbieter zu hoch und verlangt sehr viele Daten, kann dies zwar durchaus legal sein, aber möglicherweise den Konsumenten von der Nutzung des Dienstes abhalten.

Im Rahmen dieser grundlegenden Austauschbeziehung stellen sich zentrale ökonomische Fragen der Gestaltung und Regulierung in der digitalisierten Welt, welche jeweils im Hinblick auf aktuelle technologische Entwicklungen zu betrachten sind. So hat etwa die zuvor genannte zentrale Abwägung einer Datenpreisgabe in sozialen Netzwerken heutzutage oftmals nicht nur Auswirkungen auf den Teilenden, sondern auch auf andere Personen, etwa wenn diese auf geteilten Bildern ebenfalls zu erkennen sind. Folglich gestaltet sich diese zentrale Entscheidungssituation für Individuen zunehmend komplexer und erfordert einen gewissen kognitiven Aufwand – nicht selten entscheiden hier nicht ausschließlich rationale Faktoren. Gleichzeitig versuchen Anbieter oftmals mittels sogenannter Nudging-Techniken[6] Verbraucher zur Preisgabe von personenbezogenen Daten zu bewegen, was gerade im Kontext von sehr sensitiven – und somit für den Anbieter häufig auch besonders wertvollen – Daten (etwa Gesundheitsdaten) oftmals schwierig ist.

Die personenbezogenen Daten haben somit sowohl für die Konsumenten als auch für die anfragenden Unternehmen einen Wert und einen damit verbundenen Preis. Es zeigt sich somit ein facettenreiches Bild hinsichtlich der zugrunde liegenden Austauschbeziehung zwischen Unternehmen und Konsumenten. Dieser Beitrag verfolgt das Ziel, anhand einzelner exemplarischer Kontexte, das ökonomische Verständnis von Privatheit als Wechselspiel zwischen Anbieter und Nachfrager aufzuzeigen und insbesondere mittels aktueller Erkenntnisse zu erweitern. Der Beitrag ist wie folgt strukturiert: In Abschn. 2 präsentieren wir ein wirtschaftswissenschaftliches Verständnis von Privatheit und stellen die vier relevantesten Forschungsstränge aus Sicht von Unternehmen dar. In Abschn. 3 beschreiben wir zwei unserer Untersuchungen, die sich aus der originären Sicht von Unternehmen mit der Nutzung personenbezogener Daten beschäftigen. Abschn. 4 widmet sich drei von uns durchgeführten Studien, die sich dem Thema aus Sicht der Konsumenten nähern. Wir schließen den Beitrag mit einer Zusammenfassung und dem Ausblick in Abschn. 5 ab.

[6] Schöning et al. (2019).

2 Privatheit aus der Sicht der Wirtschaftswissenschaften

2.1 Grundlegendes Verständnis von Privatheit

Das Konzept der Privatheit wird von unterschiedlichen Disziplinen behandelt, was zu einer Vielzahl von verschiedenen Konzeptualisierungen und Definitionen des Begriffs führt.[7] In Morlok et al.[8] beschreiben wir den zeitlichen Wandel und die disziplinspezifischen Unterschiede des Privatheitskonzepts. Charakteristisch für die Privatheitsforschung ist das hohe Maß an unterschiedlichen Zugängen zum Thema. Anfänglich wurde Privatheit explizit als physische Privatheit verstanden. Diese physische Privatheit bezieht sich auf den körperlichen Zugang zu einem Individuum und dessen räumlicher Umgebung. Im juristischen Kontext wird Privatheit, resultierend aus der physischen Privatheit, definiert als das „Recht, alleine gelassen zu werden"[9]. Weiterhin wird die Privatheit in der Philosophie und der Psychologie beschrieben als der „Zustand des begrenzten Zugangs oder der Isolation".[10] Dagegen wird die Privatheit in den Sozialwissenschaften als ein soziales Problem oder als ein Verhaltenskonzept begriffen.[11]

Im Kontext des vorliegenden Beitrags steht das Konzept der informationellen Privatheit im Fokus, welches den Zugang zu Informationen, die explizit einer Person zuordenbar sind, beschreibt.[12] Im Zentrum der allgemeinen ökonomischen Definition des Begriffs Privatheit steht die Definition von Privatheit als Kontrolle und als Fähigkeit zur Kontrolle.[13] Angewandt auf informationelle Privatheit umfasst dies die Kontrolle über die Preisgabe und die Verwendung von Informationen.[14] Die Wirtschaftswissenschaften adressieren dabei häufig Fragen der Verwendung von *personenbezogen* Daten durch Unternehmen. Unter dem Begriff personenbezogen fallen nicht nur explizit preisgegebene Daten, sondern auch unbewusst geteilte Daten, etwa über das Nutzungsverhalten im Internet.

[7] Smith et al. (2011).

[8] Morlok et al. (2018).

[9] Warren und Brandeis (1890).

[10] Schoeman (1984).

[11] Margulis (2003).

[12] Smith et al. (2011).

[13] ebd, Westin (1967).

[14] Awad und Krishnan (2006), Hann et al. (2007).

Nach Morlok et al.[15] ist es ebenfalls wichtig, beim Umgang mit dem Thema Privatheit auf die unterschiedlichen Akteure und Betrachtungsebenen einzugehen. Wesentliche Akteure sind Unternehmen und Konsumenten und deren Wechselspiel. Auf diese Akteure konzentrieren wir uns nachfolgend. Bei den Unternehmen ist neben der Betrachtung des Unternehmens als Ganzes auch die Betrachtung der in einem Unternehmen agierenden Individuen (Mitarbeiter, Manager) möglich. Konsumenten betrachten wir – etwas vereinfachend – auf Individualebene.

Aus wirtschaftswissenschaftlicher Sicht ebenfalls wichtig sind die Rahmenbedingungen des Zusammenwirkens von Unternehmen und Verbrauchern, sei es in konkreten Marktkonstellationen oder durch Regulationen vorgegeben. Dieses sehr umfassende Themenfeld klammern wir nachfolgend aus.

2.2 Relevante Forschungsstränge

In Morlok et al.[16] geben wir einen Überblick über die wesentlichen Forschungsstränge der Literatur im Bereich der Wirtschaftswissenschaften. Bezüglich des Zusammenspiels von Unternehmen und Verbrauchern findet sich eine beachtliche Zahl von Studien zu den Themen Personalisierung und Preisdifferenzierung.

Unternehmen können ihre Angebote personalisieren, indem sie auf Basis der gesammelten Konsumentendaten die Verhaltensweisen und Präferenzen ihrer Kunden verstehen und sich dementsprechend ausrichten. Forschung über die personalisierte Ansprache durch die Verwendung von personenbezogenen Daten beschäftigt sich mit einer Vielzahl von Themengebieten. Kern der Forschung in diesem Bereich ist, dass Unternehmen möglichst viele personenbezogene Daten auswerten möchten, um ihre Kunden bestmöglich ansprechen zu können. Auf der einen Seite schätzen Kunden die Vorteile der Personalisierung, auf der anderen Seite haben sie häufig Privatheitsbedenken, wenn Angebote durch die Analyse ihrer personenbezogenen Daten entstehen. Dieses Phänomen wird als „Personalization Privacy Paradox“ bezeichnet.[17] Forschung in Bezug auf

[15] Morlok et al. (2018).

[16] Morlok et al. (2017).

[17] z. B. Xu et al. (2011).

die individualisierte Kundenansprache fokussiert sich darauf, unter welchen Bedingungen und zu welchem Grad Unternehmen Systeme zur Personalisierung einsetzen können, ohne dass Konsumenten sich durch die Personalisierung bedroht fühlen. Beispielsweise untersuchen Karwatzki et al.[18], wie digitale Services gestaltet werden sollten, um den Kunden trotz Privatheitsbedenken zum Teilen von personenbezogenen Daten zu bewegen.

Auch zur Preisdifferenzierung finden sich eine Reihe interessanter Studien. Unternehmen können die gesammelten Daten verwenden, um die Zahlungsbereitschaft ihrer Konsumenten präziser als bisher zu bestimmen. Die Vorhersage der Zahlungsbereitschaft von Kunden ermöglicht den Unternehmen die Preisdiskriminierung zumindest bestimmter Kundengruppen, im Einzelfall sogar einzelner Kunden. Im Gegensatz zur Personalisierung geht die Preisdiskriminierung zumeist mit monetären Nachteilen für den Kunden einher.[19]

Personenbezogene Daten können von Unternehmen zudem genutzt werden, um das Verhalten ihrer Mitarbeiter zu steuern. Dies wird in einem dritten, relativ neuen Themenfeld, aufgegriffen. Beispielsweise kann Software zur Überwachung in Unternehmen die Produktivität, das Arbeitsverhalten oder die Bewegungsmuster von Mitarbeitern verfolgen. Unabhängig von der rechtlichen Betrachtungsweise von Überwachung am Arbeitsplatz ergeben sich ökonomische Fragestellungen bezüglich der Privatheit der Mitarbeiter. Literatur in dem unternehmensinternen Kontext beschäftigt sich mit den Auswirkungen von Überwachung auf das Unternehmen und auf dessen Mitarbeiter. So untersuchen Connolly und McParland[20] welchen Einfluss digitale Technologien am Arbeitsplatz auf die Privatheitsbedenken von Arbeitnehmern haben. Des Weiteren beschäftigt sich Literatur zur Privatheit von Jobbewerbern insbesondere mit der Diskriminierung von Bewerbern. In diesem Teilaspekt geht es darum, dass Arbeitgeber auf unterschiedlichen Wegen Zugang zu Informationen von Bewerbern haben, da diese ihre Daten in sozialen Netzwerken teilen.[21] Demnach können im Rahmen der Bewerberauswahl künftige Arbeitgeber gezielt nach Informationen von Bewerbern suchen und diese auswerten. Der öffentliche Zugang zu privaten Informationen wie täglichen Aktivitäten oder privaten Interessen wird durch soziale Netzwerke gefördert.

[18] Karwatzki et al. (2017).

[19] Acquisti et al. (2016).

[20] Connolly und McParland (2012).

[21] Acquisti und Fong (2020).

Jenseits von der unternehmensinternen Nutzung von Daten können Unternehmen von personenbezogenen Daten profitieren, wenn sie diese an Dritte weiterverkaufen. Der vierte ebenfalls noch recht kleine Literaturstrang beschäftigt sich daher mit der ökonomischen Verwertung von Konsumentendaten, die auf internetbasierten Plattformen gesammelt werden. Plattformen können die von ihnen gesammelten Daten an Werbetreibende oder an Datenintermediäre verkaufen, die die Daten anschließend weiterverwerten. Literatur in diesem Bereich beschäftigt sich häufig mit der sekundären Nutzung von personenbezogenen Daten, wenn Informationen von Unternehmen an Drittanbieter oder Datenhändler weitergegeben werden. Hartmann et al.[22] untersuchen Geschäftsmodelle von Startups, die sich auf personenbezogene Daten als Schlüsselressource spezialisieren. Die Hauptaktivität dieser Unternehmen besteht in der Aggregation, Analyse oder Generierung von Daten aus unterschiedlichen Quellen. Welchen Herausforderungen Unternehmen beim Datenhandel gegenüberstehen und welche unternehmensinternen Voraussetzungen sie treffen sollten, wird von Wixom und Ross[23] beschrieben.

3 Personenbezogene Daten als unternehmerische Ressource

Nachfolgend stellen wir zwei Studien vor, die wir in ökonomischen Teilprojekten in den letzten Jahren durchgeführt haben. Die Studien beschäftigen sich mit der unternehmensinternen und -externen Verwendung von Daten.

3.1 Unternehmen als Teil von Datenmärkten und Wertschöpfungsstrukturen für Daten

Im Rahmen einer explorativen Studie haben wir uns in Bründl et al.[24] genauer mit der Struktur von und der Wertschöpfung in Datenmärkten und den damit verbundenen Rollen von Unternehmen auseinandergesetzt. Um tiefere Einblicke in den Markt für personenbezogene Daten zu erhalten, haben wir Experten aus

[22] Hartmann et al. (2016).

[23] Wixom und Ross (2017).

[24] Bründl et al. (2016).

datengetriebenen Unternehmen für echtzeitbasierte Online-Werbung (Real-Time-Advertising) befragt. Mit einem geschätzten Marktvolumen von zum Zeitpunkt der Studie 1,6 Mrd. Euro p. a. ist dies der größte Teilmarkt. Ziel der Experteninterviews war es, zu erfahren, welche Geschäftsmodelle und Anwendungsbeispiele für den Datenhandel vorliegen, welchen monetären Wert Daten auf diesem Markt haben und welche Faktoren den Datenwert beeinflussen. Mit Hilfe der Interviews konnten wir konzeptualisieren, wie Wertschöpfungsstrukturen aussehen, wie der Wert von Daten festgelegt wird und welche Akteure in diesem Prozess beteiligt sind. Im Folgenden fassen wir die Hauptergebnisse der empirischen Studie zusammen.

Akteure

Wir differenzieren sieben Rollen, die sich im Datenmarkt bewegen: *Advertiser, Publisher, Demand-, Supply-Side-Plattformen, Datensammler, Data-Exchange- und Data-Management-Plattformen* (Abb. 1). Wertschöpfungsaktivitäten werden von Datensammlern initiiert. Diese generieren unterschiedliche Arten von Daten und nutzen diese sowohl für eigene Zwecke, als auch für den Verkauf an andere Akteure. Datensammler sind vor allem Anbieter von Online-Plattformen, auf

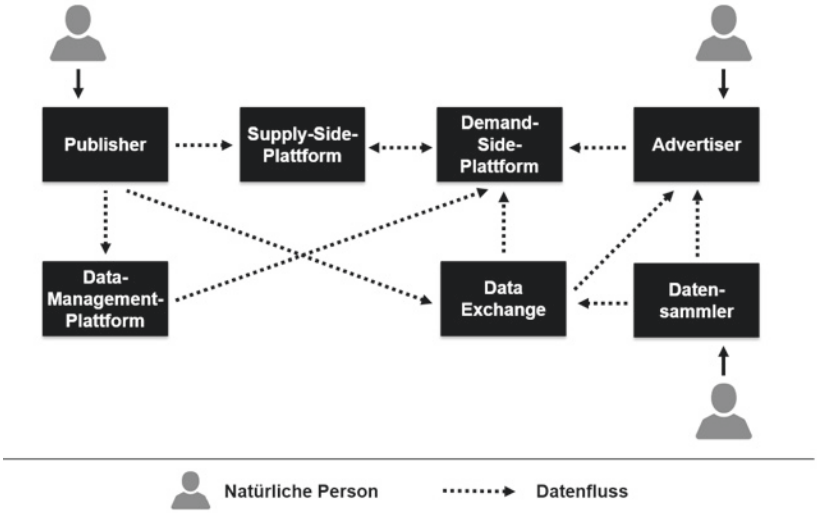

Abb. 1. Wertschöpfungskette für personenbezogene Daten (Quelle: Bründl et al. 2016)

denen kostenfreie Dienste angeboten werden. Diese kostenlosen Dienste werden finanziert durch die Weitergabe der gesammelten Daten an Dritte. Am anderen Ende der Wertschöpfungskette stehen Advertiser (Werbetreibende). Diese wollen ihre Produkte oder Dienste an potentielle Kunden vermarkten. Um auf die digitalen Werbeplätze der Publisher zugreifen zu können, nutzen sie die Dienste von Intermediären (Demand-Side-Plattformen). Damit die Werbung an spezielle Kundensegmente ausgeliefert werden kann, ziehen Demand-Side-Plattformen personenbezogene Daten der Kunden heran. Publisher offerieren auf Webseiten oder in mobilen Applikationen digitale Werbeplätze. An dieser Stelle greifen Publisher auf Intermediäre in Form von Supply-Side-Plattformen zurück, damit sie ihre eigenen Werbeplätze gewinnmaximierend anbieten können. Durch Supply-Side-Plattformen können Publisher ihre Werbeplätze automatisiert in Echtzeit vermarkten (*Real-Time-Bidding*). Supply-Side-Plattformen übermitteln den verfügbaren Werbeplatz und Kontakteigenschaften an Demand-Side-Plattformen. Wenn die übertragenen Eigenschaften vom Werbeplatz mit den vom Advertiser gestellten Anforderungen übereinstimmen, bieten Demand-Side-Plattformen automatisiert einen vordefinierten Preis. Letztendlich erhält den Werbeplatz für den spezifischen Kontakt der höchstbietende Advertiser. So wirken Demand-Side-Plattformen als Intermediäre, durch die Advertiser datengetriebene, zielgruppengerechte Werbekontakte in automatisierter Form erwerben können. Demand-Side-Plattformen aggregieren Daten von Supply-Side-Plattformen, Data-Management-Plattformen und Data Exchanges, um verfügbare Angebote mit den Anforderungen von Advertisern in Einklang zu bringen. Data-Management-Plattformen nutzen Algorithmen des maschinellen Lernens, um Akteure bei Zielgruppenidentifikation zu unterstützen, indem sie die Charakteristika von Kundensegmenten einschätzen. Oftmals eng verknüpft mit Data-Management-Plattformen sind Data Exchanges. Diese wirken als Handelsplätze von Third-Party-Daten von potentiellen Zielgruppen und geben so Auskunft über spezielle Kundensegmente.

Wertschöpfungsstrukturen

Wir beschreiben die Wertschöpfung im Umgang mit Daten auf der Unternehmensebene anhand von vier aufeinanderfolgenden Schritten. Im ersten Schritt werden personenbezogene Daten durch Unternehmen gesammelt. Nachfolgend werden die gesammelten Daten aufbereitet und aggregiert. Im dritten Schritt werden die Daten auf gewisse Muster analysiert. Schließlich können die Daten im letzten Schritt distribuiert und genutzt werden. Der Datenmarkt stellt durch seine Wertschöpfungsprozesse für Unternehmen einen interessanten Anknüpfungspunkt dar. Anhand der Darstellung können Unternehmen geeignete Partner

identifizieren, um ihre vorhandene Datenbasis zu monetarisieren. Die Erhebung von bislang unbeachteten Daten kann sich anbieten, um neue Erlösquellen zu erschließen. Gleichzeitig müssen die Interessen der Kunden und rechtliche Erfordernisse beachtet werden.

In Anbetracht aktueller Entwicklungen des Datenmarkts, wird dieser in Zukunft voraussichtlich an Relevanz gewinnen. Die Menge an verfügbaren Daten wächst durch Trends wie das Internet der Dinge und Big Data weiter an. Auf der einen Seite führt das steigende Angebot an Daten bei gleichbleibender Nachfrage zu sinkenden Preisen. Auf der anderen Seite steigt die Datenqualität wegen zunehmender Möglichkeiten der Vernetzung weiter an. Der zunehmende Preis für personenbezogene Daten stellt ein monetäres Potential für Unternehmen dar. Die zunehmende Generierung von Daten, verbunden mit dem Potential diese Daten gewinnbringend auszuwerten, führt zu einer zunehmenden Bedeutung des Datenhandels und der Rolle von Daten für Unternehmen.

3.2 Daten als Ressource für Unternehmen

Heutzutage sammeln Unternehmen eine zunehmend große Menge an Daten aus unterschiedlichen Quellen. Wenn heterogene Datensets aus unterschiedlichen Quellen miteinander kombiniert werden, kann dies zu vielversprechenden unternehmensinternen Vorteilen führen.[25] Miteinander kombinierte Daten haben einen höheren Wert als Daten, die einzeln betrachtet werden. In Weibl und Hess[26] beschäftigen wir uns mit der Frage, wie Synergieeffekte aus kombinierten Daten konzeptualisiert werden können und wie Synergieeffekte zu unternehmerischen Vorteilen führen.

Ansatz

Die Ergebnisse der Arbeit sind in einem konzeptionellen Framework dargestellt (Abb. 2). Theoretische Basis für das Framework bilden die Systemtheorie und das Konzept von Synergie nach Nevo und Wade.[27] Die Systemtheorie stellt die theoretische Grundlage des Konzepts synergistischer Ressourcen dar[28] und zeigt

[25] Shollo und Galliers (2016).

[26] Weibl und Hess (2020).

[27] Nevo und Wade (2010).

[28] Someh und Shanks (2013).

Abb. 2. Konzeptionelles Modell von Datensynergien (basierend auf Weibl und Hess, 2020)

auf, dass Systeme im Ganzen betrachtet werden sollten.[29] Synergistische Interaktionen zwischen Komponenten eines Systems führen dazu, dass ein System nicht nur aus der Summe seiner Komponenten, sondern auch aus deren Interaktionen besteht.[30] Synergien werden in der Literatur in unterschiedlichen Fachbereichen und aus verschiedenen Perspektiven betrachtet. Nevo und Wade[31] stellen das Konzept von Synergien in der Wirtschaftsinformatik in einem konzeptuellen Framework dar. Dieses beinhaltet in einer ersten Stufe potentielle Synergien aus IT-Ressourcen und organisatorischen Ressourcen. In der zweiten Stufe werden potentielle Synergien mit organisatorischen Voraussetzungen verbunden, damit Synergien praktisch realisiert werden können.

Methodisch verfolgen wir in Weibl und Hess[32] einen zweistufigen Ansatz. In einem ersten Schritt konstruieren wir ein initiales Modell der Datensynergien aus relevanter Literatur. Das Framework der Synergieeffekte nach Nevo und Wade[33] dient an dieser Stelle als Ausgangspunkt. In Kombination mit einer strukturierten Analyse weiterer relevanter Literatur bilden wir ein initiales Framework der Datensynergien. Dieses erste Framework wird in einem zweiten Schritt durch 24

[29] Ackoff (1971).
[30] ebd.
[31] Nevo und Wade (2010).
[32] Weibl und Hess (2020).
[33] Nevo und Wade (2010).

semi-strukturierte Experteninterviews verfeinert. Die ausgewählten Interviewpartner arbeiten als Datenexperten innerhalb von unterschiedlichen Unternehmen und erfüllen verschiedene Positionen. Die Kombination aus Theorie und Empirie führt zu dem konzeptuellen Modell von Datensynergien (Abb. 2). Das Framework stellt dar, welche Voraussetzungen für die Realisierung von Synergien getroffen werden sollten. Außerdem zeigt es auf, welche Arten von Synergieeffekten durch die Kombination von Daten entstehen können.

Voraussetzungen auf Management-Ebene

Die Ergebnisse zeigen fünf Voraussetzungen auf, die das Erschließen von Datensynergien ermöglichen. Diese beziehen sich auf die Managementebene und auf die Eigenschaften der verwendeten Daten. Zwei Bedingungen für die erfolgreiche Synergie von Daten müssen von Seiten des Managements erfüllt werden: Integration und Kontextualisierung.

Obwohl Daten fast augenblicklich über weite Entfernungen transportiert werden können, hat unsere Studie gezeigt, dass Unternehmen spezielle Vorkehrungen zur Integration und Zentralisierung von Daten in ganzheitlichen Data Warehouses (sog. Data Lakes) treffen sollten. Die Sammlung von Daten in Data Lakes bringt mehrere Vorteile mit sich: Auf der einen Seite bietet die zentrale Speicherung von Daten den Vorteil, dass Datenwissenschaftler und Entscheidungsträger einen holistischen Überblick über die vorhandenen Datensätze erhalten und diese so einfacher zu Synergien kombinieren können. Auf der anderen Seite muss gewährleistet sein, dass auf diese Daten von unterschiedlichen Funktionen und Divisionen im Unternehmen zugegriffen werden kann. Dementsprechend ist es die Aufgabe des Managements, die Datenspeicherung in Silos aufzubrechen, um Daten in einem ganzheitlichen System speichern zu können. Dieser Schritt der Datenintegration ermöglicht die (Re-)Kombination von Daten und stellt die Basis für die Erschließung von Datensynergien dar.

Die Kontextualisierung und Verknüpfung von Daten durch das Management eines Unternehmens ist unerlässlich. Um die Verbindung von Daten zu ermöglichen, sollten Unternehmen mit einem geschäftsorientierten Anwendungsfall starten und Daten insofern kombinieren, dass Hypothesen über ihre synergistische Beziehung bestätigt werden können. In dieser Art kann der geschäftsgetriebene Anwendungsfall den Impuls geben, passende Datenquellen zu kombinieren. Ein beispielhafter Anwendungsfall ist die Zusammenführung von Daten, um Erkenntnisse für die Planung einer Marketingkampagne zu erhalten. Die Kombination von bestimmten Datenquellen ist nur dann erfolgreich, wenn Teilinformationen aus unterschiedlichen Kontexten in einer wertstiftenden Form subsumiert werden.

Datenbezogene Voraussetzungen

Zusätzlich zu den managementbezogenen Voraussetzungen müssen drei datenbezogene Voraussetzungen erfüllt werden, um Synergieeffekte zwischen Daten zu fördern: Kompatibilität, Datenqualität und Speicherinfrastruktur.

Wie bereits beschrieben, müssen heterogene Ressourcen miteinander kompatibel sein, um Synergieeffekte zu ermöglichen. So wird sichergestellt, dass Ressourcen nahtlos miteinander verbunden werden können.[34] Die Interviews haben aufgezeigt, dass ein gemeinsamer Schlüssel benötigt wird, damit Daten miteinander verbunden werden können. Dies kann beispielsweise eine zeitliche Dimension sein oder auf Produktebene die Artikelnummer. Darüber hinaus müssen heterogene Datenformate gemeinsame Eigenschaften haben, damit diese in Kombination miteinander genutzt werden können.

Weiterhin wurde in den Interviews eine hohe Qualität der Daten als unerlässlich beschrieben. Dies ist besonders im E-Commerce von hoher Relevanz: Wenn es Datenprobleme im Tracking von Produkten gibt und somit die Verfügbarkeit von Produkten nicht aktualisiert wird, kann dies zu Problemen bei Bestellungen führen. Daher ist eine hohe Datenqualität eine integrale Voraussetzung, um Synergien aus Datenquellen zu schaffen.

Eine weitere entscheidende Voraussetzung ist die Bereitstellung der benötigten Infrastruktur um unterschiedliche Daten aus verschiedenen Quellen in einer einheitlichen Weise zu speichern. Im Gegensatz zu anderen organisatorischen Ressourcen, können Daten schnell und über lange Zeiträume hinweg gespeichert werden und augenblicklich über weite Distanzen transferiert werden. Viele Organisationen verlassen sich im hohem Maße auf externe Cloud-Lösungen (z. B. Microsoft Azure) und zusätzlich verwaltete Services als bevorzugte Speicherform. Auf diese Weise können Datensätze in effizienter Form in Data Lakes gespeichert werden.

Erhöhter Informationswert durch Synergieeffekte

Der erhöhte Informationswert von kombinierten Daten wird durch einen multidimensionalen Blick auf die gesammelten Daten erreicht. Ein einzelner Datensatz hat nur einen begrenzt informativen Charakter. Wenn jedoch mehrere Datensets miteinander kombiniert werden, kann dies den Informationscharakter erhöhen.

Beispielsweise kann die Kombination von historischen Verkaufszahlen mit Standort- und Zeit-Daten zu der Erkenntnis führen, wie viele Produkte

[34] Someh und Shanks (2013).

an bestimmten Tagen zur Verfügung stehen sollten. Eine der befragten Organisationen hat die Verkaufsdaten aus bestimmten Produktkategorien mit Kundendaten kombiniert, um zu sehen, für welche Produktgruppen sich bestimmte Kunden besonders interessieren. Die getrennte Betrachtung von Verkaufszahlen oder Kundenzahlen würde es nicht ermöglichen, etwaige Korrelationen zu erkennen und daraus Segmente zu identifizieren, um neue Erkenntnisse zu gewinnen.

Die synergistische Interaktion zwischen Daten ermöglicht die Betrachtung eines Subjektes aus unterschiedlichen Betrachtungswinkeln. Durch die Aggregation von Daten können bestimmte Muster festgestellt werden, beispielsweise im Online-Kundenverhalten. Unternehmen können neue Erkenntnisse über das Kundenverhalten erlangen, indem sie Transaktionsdaten von Kunden mit personenbezogenen Daten oder dem Online-Surfverhalten verbinden. Die Kombination dieser Daten ermöglicht Einblicke in die Online-Aktivitäten von Kunden und vor allem in die Bedürfnisse von Konsumenten und deren Interessen. Als Folge der gewonnenen Erkenntnisse über den Kunden, können Unternehmen ihre Online-Präsenz optimieren oder Kunden personalisierte Inhalte ausspielen.

Tangible Vorteile in Form von erhöhten Transaktionswerten

Unsere Studie zeigt auf, dass Daten-Synergieeffekte zu tangiblen Vorteilen in Form von individualisierten Marktangeboten und automatisierten Geschäftsprozessen führen können. Die Möglichkeit Daten zu strukturieren und zu segmentieren, erlaubt es Unternehmen, spezielle Kundengruppen mit Angeboten gezielt zu adressieren. Beispielsweise hat einer der Experten angegeben, dass seine Organisation Daten kombiniert mit dem Ziel, Kundenabwanderung zu verhindern. Das Unternehmen erreichte dies, indem es Transaktionsdaten der Kunden mit Informationen über Kunden-Berührungspunkte, den Suchhistorien im Online-Shop und demografischen Daten verbunden hat. Die Kundeninformationen, die so aus mehreren Quellen kombiniert wurden, geben dem Unternehmen ein vervollständigtes Bild über den Kunden.

Laut der befragten Experten kann die Kombination von Daten zu verbesserten und automatisierten Reportingprozessen führen. Daher wird die Datenkombination als typische „quick win“ Aktion in Datenprojekten angesehen. Einer der Datenexperten hat angegeben, dass seine Organisation die managementbezogenen Indikatoren aus unterschiedlichen Quellen effizienzsteigernd zu einem automatisierten Reporting Prozess transformiert hat, indem Rohdaten aus den Data Warehouses verbunden und im Anschluss visuell dargestellt wurden.

Ziel der Studie war es, das synergistische Potential der Wertgenerierung aus Daten zu untersuchen. Daten als Ressource führen durch ihre spezifischen

Eigenschaften auf andere Weise zu synergistischen Interaktionen als andere organisatorische Ressourcen. Die Kernergebnisse aus der Studie von Weibl und Hess[35] führen zu einem konzeptionellen Framework, das im ersten Schritt bestimmte Voraussetzungen beschreibt, die notwendig sind, um synergistische Interaktionen zu ermöglichen. Im zweiten Schritt werden die Ergebnisse der Synergieeffekte beschrieben: Daten in kombinierter Form führen zu einem erhöhten Informations- und Transaktionswert durch automatisierte Entscheidungsfindung und Effizienzsteigerung im Unternehmen.

4 Die Verbraucherperspektive

Verbraucher produzieren Daten als „Nebenprodukt". Für sie stellt sich die Frage, ob sie dieses Nebenprodukt behalten oder weitergeben wollen. Nachfolgend stellen wir drei Studien vor, in denen wir uns diesem Thema aus unterschiedlichen Perspektiven nähern.

4.1 Zahlungsbereitschaft für Privatheit

Dank des interaktiven Charakters digitaler Medien, können Unternehmen große Mengen an personenbezogenen Informationen über Konsumenten und deren Verhaltensweisen erfassen und analysieren. Viele Anbieter haben die resultierenden kommerziellen Möglichkeiten genutzt und neue Geschäftsmodelle entwickelt, die von den gesammelten personenbezogenen Daten profitieren. Doch die Kommerzialisierung personenbezogener Daten löst bei vielen Konsumenten Privatheitsbedenken aus, die zur Beendigung der Nutzung entsprechender Dienste führen können und somit langfristig ein unternehmerisches Risiko für die Anbieter darstellen. Daher ist es ein neuer Ansatz, den Wert personenbezogener Daten zu monetarisieren. Dieser Ansatz basiert auf der Annahme, dass, obwohl es einige Verbraucher bevorzugen Online-Dienste im Austausch gegen die Bereitstellung personenbezogener Informationen kostenlos zu nutzen, andere es vorziehen, für den Schutz ihrer Privatsphäre zu bezahlen. So können Anbieter sozialer Netzwerke den Konsumenten neben einer kostenlosen Version im Austausch gegen ihre personenbezogenen Informationen auch eine Premium-Version mit zusätz-

[35] Weibl und Hess (2020).

lichen Funktionen zur Kontrolle der Privatsphäre anbieten. Dies erlaubt den Verbrauchern zu entscheiden, ob sie für ihre Privatsphäre bezahlen wollen oder nicht. Bisherige Forschung hat aufgezeigt, dass dieses sogenannte Privatheits-Freemium Modell gleich zwei Probleme lösen kann: Einerseits bietet es Anbietern sozialer Netzwerke die Möglichkeit mit nutzergenerierten Inhalten Geld zu verdienen und andererseits können auf diese Weise die Datenschutzbedenken der Konsumenten bei der Verwendung sozialer Netzwerke adressiert werden.[36]

Empirische Untersuchung der Zahlungsbereitschaft für Privatheit

Allerdings hatte die Forschung bis zu diesem Zeitpunkt noch keine theoretische Erklärung für die Zahlungsbereitschaft der Konsumenten für Privatheit gefunden. Vor diesem Hintergrund haben wir uns in Schreiner und Hess[37] mit Höhe und Determinanten der Zahlungsbereitschaft für Privatheit beschäftigt. In dieser Studie haben wir anhand einer Online-Umfrage die Zahlungsbereitschaft der Konsumenten für eine zahlungspflichtige Premium-Version von Facebook untersucht. Mittels der *Theory of Planned Behavior*[38], wollten wir die tatsächliche Zahlungsbereitschaft für Privatheit der Konsumenten bestimmen. Die *Theory of Planned Behavior* wurde bereits in vielen Studien der Wirtschaftswissenschaften als theoretischer Rahmen zur Erklärung des Verhaltens von Individuen angewandt. Die Theorie besagt, dass die Verhaltensweise von Individuen basierend auf ihrer Einstellung gegenüber dem Verhalten, subjektiven Normen und der wahrgenommenen Verhaltenskontrolle vorhergesagt werden kann. In Schreiner und Hess[39] haben wir diesen theoretischen Rahmen auf den Kontext unserer Studie angewandt und um drei Antezedenten der Einstellung erweitert: Wahrgenommenes Risiko der Privatheit, wahrgenommene Nützlichkeit und Vertrauen. Unter dem wahrgenommenen Risiko der Privatheit verstehen wir die Unsicherheit der Konsumenten bezüglich möglicher negativer Konsequenzen, die die Nutzung sozialer Netzwerke mit sich bringen kann. Folglich stellen wir die Hypothese auf, dass das wahrgenommene Risiko der Privatheit im digitalen Kontext die Einstellung der Verbraucher gegenüber einer Premium-Version mit

[36] Schreiner und Hess (2013).

[37] Schreiner und Hess (2015).

[38] Ajzen (1991).

[39] Schreiner und Hess (2015).

zusätzlichen Funktionen zur Kontrolle der Privatsphäre positiv beeinflusst. Des Weiteren vermuten wir, dass die Einstellung gegenüber der Premium-Version positiv beeinflusst wird, wenn Konsumenten einen Mehrwert der angebotenen Funktionen in Bezug auf die Verbesserung des Datenschutzes sehen. Außerdem stellen wir die Hypothese auf, dass Vertrauen in die Premium-Version die Einstellung der Konsumenten gegenüber der Nutzung der Premium-Version positiv beeinflusst.

Das resultierende Forschungsmodell haben wir anhand einer Online-Umfrage getestet.[40] Hierfür haben wir den Teilnehmern der Umfrage eine Premium-Version des sozialen Netzwerks Facebook vorgestellt. Im Vergleich zu der kostenlosen Basisversion, hatte diese Version zusätzliche Funktionen, um die Erfassung, Nutzung, Weitergabe und Speicherung personenbezogener Daten zu kontrollieren. So können Konsumenten der Premiumversion beispielsweise bestimmen, welche ihrer personenbezogenen Daten erfasst und für welche Zwecke diese genutzt wurden. Im Anschluss hatten die Teilnehmer die Möglichkeit, ihren Basis-Facebook-Account zu erweitern, um zusätzliche Kontrollfunktionen für ihre Privatsphäre zu erhalten. Um die tatsächliche Zahlungsbereitschaft der Teilnehmer für die Premiumversion zu erfassen, haben wir eine anreizkompatible Methodik genutzt. Hierfür wurde den Teilnehmern erzählt, dass der Preis für die Premiumversion noch nicht festgelegt worden ist und dass sie entscheiden können, ob und wieviel sie pro Monat für die Premiumversion zahlen wollen. Ist ihr Gebot mindestens so hoch wie ein automatisch generierter Zufallspreis, können sie die Premiumversion zu diesem Preis nutzen. Ist das Gebot dahingegen niedriger als der zufällig generierte Preis, können sie die Premiumversion nicht nutzen und müssen den Preis auch nicht zahlen. Dieses Vorgehen hat es uns ermöglicht, die tatsächliche Zahlungsbereitschaft der Teilnehmer zu erfassen.

Die angegebene Zahlungsbereitschaft der Teilnehmer bewegte sich zwischen 0 und 15 € mit einer durchschnittlichen Zahlungsbereitschaft von 0,63 € für die Premiumversion.

Das resultierende Strukturgleichungsmodel ist in Abb. 3 dargestellt. Die Ergebnisse unserer Studie zeigen, dass die wahrgenommene Nützlichkeit und das Vertrauen die Einstellung der Konsumenten gegenüber einer Premiumversion mit zusätzlichen Funktionen zum Schutz der Privatsphäre signifikant positiv beeinflussen. Das wahrgenommene Risiko der Privatheit hat dahingegen

[40] Ebd.

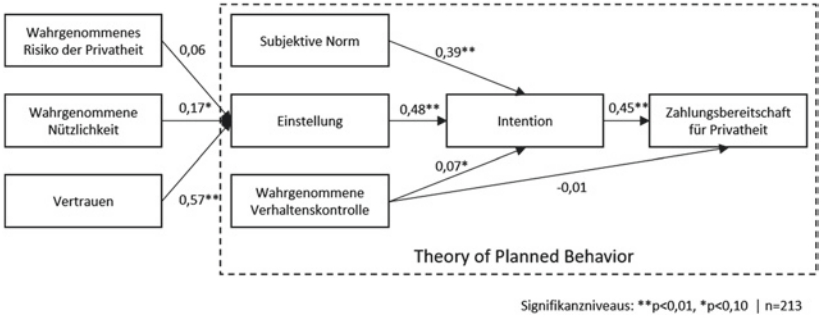

Abb. 3. Determinanten der Zahlungsbereitschaft (basierend auf Schreiner und Hess, 2015)

keinen signifikanten Einfluss auf die Einstellung. In Einklang mit der *Theory of Planned Behavior* zeigt unsere Studie außerdem, dass subjektive Normen, die Einstellung der Verbraucher und die wahrgenommene Verhaltenskontrolle die Nutzungsintention positiv beeinflussen, welche wiederum einen signifikant positiven Einfluss auf die Zahlungsbereitschaft für Privatheit hat. Für Betreiber sozialer Netzwerke bedeutet das, dass das Anbieten einer Premiumversion mit zusätzlichen Funktionen zur Kontrolle der Privatsphäre einen guten Ansatz zur Monetarisierung des Schutzes der Privatheit als Erlösmodel darstellt. Wichtig hierbei ist, dass die angebotene Premiumversion die Möglichkeiten der Konsumenten zum Schutz ihrer personenbezogenen Daten tatsächlich erhöht. Außerdem sollten die Anbieter sozialer Netzwerke sicherstellen, dass die Konsumenten der Premiumversion vertrauen können. Um das Vertrauen der Verbraucher zu stärken, könnten beispielsweise Informationskampagnen gestartet werden, um die Transparenz bezüglich der Unterschiede zwischen der kostenlosen und der Premiumversion zu erhöhen, oder unabhängige Dritte könnten den Schutz der Privatsphäre verifizieren.

Nachfolgende empirische Erkenntnisse

Auch neuere Studien haben sich der Zahlungsbereitschaft für Privatheit gewidmet und zeigen, dass das Entscheidungsverhalten der Individuen sehr komplex ist und die Zahlungsbereitschaft für Privatheit stark vom jeweiligen Kontext abhängt. Zwei kontextspezifische Faktoren scheinen in diesem Hinblick eine besonders zentrale Rolle zu spielen: Die generellen Privatheitsbedenken des Konsumenten

und der Grad der Sensibilität der Daten.[41] Umso sensitiver die Daten und umso höher die generellen Privatheitsbedenken des Einzelnen sind, umso höher ist der Preis, der für die Datenpreisgabe gefordert wird. Nguyen et al.[42] kommen in ihrer Studie zu ähnlichen Ergebnissen wie wir in Schreiner und Hess[43] und zeigen, dass Smartphonenutzer bereit sind, einen Preisaufschlag zu zahlen, um ihre Privatsphäre zu schützen. Außerdem zeigen sie, dass höhere generelle Privatheitsbedenken der Verbraucher zu einer gesteigerten Zahlungsbereitschaft für Privatheit führen. Des Weiteren spielt auch die Sensibilität der offenzulegenden Daten eine wichtige Rolle. Egelman et al.[44] haben eine Studie mit zwei Experimenten durchgeführt, um die Zahlungsbereitschaft der Verbraucher für Privatheit bei der Wahl neuer Apps zu untersuchen. Die Ergebnisse zeigen, dass Konsumenten bei der Wahl zwischen verschiedenen Apps mit ähnlichen Funktionalitäten bereit sind 1,50 US$ für die App zu bezahlen, die am wenigsten Zugriffserlaubnisse fordert. Die Autoren kommen zu dem Schluss, dass viele Smartphonenutzer um ihre Privatheit besorgt sind und daher bereit sind, einen Aufschlag für Apps zu bezahlen, die weniger sensible Daten anfordern. Auch Winegar und Sunstein[45] kommen zu ähnlichen Ergebnissen. In einer Studie mit 2.416 US-amerikanischen Teilnehmern untersuchen sie den Wert, den Individuen ihren personenbezogenen Daten bei der Nutzung digitaler Plattformen beimessen. Die Ergebnisse ihrer Studie zeigen, dass Verbraucher signifikant mehr Geld verlangen, um Daten preiszugeben, die gesundheitsbezogene Informationen beinhalten, im Vergleich zu demographischen Daten. Außerdem belegt die Studie den sogenannten *Superendowment Effect,* der besagt, dass Individuen ihren Daten einen viel größeren Wert beimessen, wenn es darum geht, einen monetären Wert für die Bereitstellung personenbezogener Daten festzulegen verglichen mit der Zahlungsbereitschaft, die Individuen haben, um ihre personenbezogenen Daten zu schützen. Pu und Grossklags[46] haben eine Conjoint Analyse durchgeführt, um den monetären Wert zu quantifizieren, den Individuen sowohl ihren eigenen Informationen als auch denen ihrer Freunde bei der Nutzung einer sozialen App beimessen. Die Ergebnisse zeigen, dass der wahrgenommene Wert

[41] Wagner et al. (2018).

[42] Nguyen et al. (2016).

[43] Schreiner und Hess (2015).

[44] Egelman et al. (2013).

[45] Winegar und Sunstein (2019).

[46] Pu und Grossklags (2016).

personenbezogener Daten der Freunde davon abhängt, ob die gesammelten Informationen für die Funktionalität der App von Bedeutung sind. Ist das der Fall werden die personenbezogenen Informationen der Freunde mit 1,01 US$ bewertet, während ihnen nur ein Wert von 0,68 US$ zugeschrieben wird, wenn sie keinen Mehrwert für die Nutzung der App bieten. Den eigenen Daten wird entsprechend ein Wert von 1,48 bzw. 1,52 US$ beigemessen.

4.2 Bereitschaft zur Offenlegung personenbezogener Daten

Neben dem Wert personenbezogener Daten spielt auch die generelle Bereitschaft der Individuen, personenbezogene Daten offenzulegen, eine zentrale Rolle. im Besonderen gilt dies bei Gesundheitsdaten. Wir haben diese Frage in Verbindung mit sogenannten Health Wearables untersucht und die Ergebnisse in Becker et al.[47] dargelegt. Nachfolgend stellen wir die Ergebnisse und das dahinterliegende Projekt vor.

Personenbezogene Gesundheitsdaten
Besonders im Gesundheitswesen ist die Offenlegung personenbezogener Daten ein zentrales Thema, da es sich bei Gesundheitsdaten um eine sehr sensible Ressource handelt, die es zu schützen gilt. Daher haben viele Individuen Privatheitsbedenken hinsichtlich der Erfassung und Nutzung ihrer Gesundheitsdaten. Vor allem haben sie Bedenken bezüglich möglicher unerwünschter wirtschaftlicher und sozialer Folgen, die der Missbrauch solcher Informationen mit sich bringen kann. Basierend auf dem Privatheitskalkül führen Individuen daher eine Kosten-Nutzen-Analyse durch, um zu entscheiden, welche personenbezogenen Gesundheitsinformationen sie offenlegen. Folglich stellt sich die Frage, auf welche Art und Weise Unternehmen die Bereitschaft ihrer Kunden, personenbezogene Gesundheitsdaten offenzulegen, erhöhen können.

Das Privatheitskalkül als Bezugsrahmen
Ein zentraler Aspekt der Privatheitsforschung in den Wirtschaftswissenschaften und darüber hinaus ist daher das sogenannte Privatheitskalkül, welches einen bewussten kognitiven Prozess zur Entscheidung der Offenlegung

[47] Becker et al. (2020).

personenbezogener Daten beschreibt. Es geht davon aus, dass Individuen sich bewusst entscheiden, welche Informationen sie preisgeben. Der Ansatz des Privatheitskalküls beschreibt, dass Individuen eine Kosten-Nutzen-Analyse durchführen und dabei die Nachteile der Datenpreisgabe gegenüber möglichen Vorteilen abwägen. Das heißt, Individuen wägen einen möglichen Verlust der Privatheit gegen einen potentiellen Nutzen, den die Informationspreisgabe mit sich bringt, ab. Überwiegt der wahrgenommene Nutzen, so entscheidet sich das Individuum, seine personenbezogenen Daten offenzulegen[48] – ggf. unter dem Einfluss von Verzerrungen wie sie aus der Psychologie bekannt sind.

Empirische Untersuchung der Offenlegung personenbezogener Gesundheitsdaten

Um dies genauer zu untersuchen, haben wir in Becker et al.[49] die bereits erwähnte Studie zur Erforschung der Bereitschaft, personenbezogene Gesundheitsdaten zur Nutzung sogenannter Health Wearables preiszugeben, durchgeführt. Health Wearables sind eine spezielle Form der Gesundheitsinformationstechnologie, bei der automatisch individuelle Gesundheitsdaten erfasst werden, um dem Verbraucher darauf basierend medizinischen Rat für seine Gesundheit und sein Wohlbefinden geben zu können. Auch wenn die Offenlegung personenbezogener Gesundheitsdaten sowohl dem Anbieter als auch den Konsumenten von Health Wearables wesentliche Vorteile wie beispielsweise eine verbesserte Personalisierung des Trainingsplans bieten kann, sind Konsumenten oft zögerlich ihre sensiblen Daten preiszugeben. Daher haben wir in Becker et al.[50] untersucht, welchen Einfluss das Framing der Produkteigenschaften und die Informationsqualität der Argumente zur Datenerfassung auf die Bereitschaft zur Offenlegung personenbezogener Gesundheitsdaten haben. Neben den Produkteigenschaften und der Datenschutzerklärung, wird die Bereitschaft personenbezogene Daten offenzulegen meist auch davon beeinflusst, auf welche Art und Weise diese Informationen präsentiert werden. Somit könnten spezielle Kommunikationsstrategien als Teil der Produktpräsentation einen erheblichen Einfluss auf die Einstellung der Verbraucher haben. In diesem Fall könnten die Anbieter von Health Wearables die wahrgenommenen Vorteile ihrer Produkte durch das richtige

[48] Chellappa und Sin (2005), Dinev und Hart (2006).

[49] Becker et al. (2020).

[50] Ebd.

Framing der Produkteigenschaften hervorheben. Außerdem könnte auch die Formulierung der Datenschutzerklärung das wahrgenommene Risiko, das mit der Datenerfassung verbunden ist, minimieren. Anbieter, die die Datenerfassung anhand logischer Argumentationen mit hohem Informationsgehalt rechtfertigen, könnten somit die Bereitschaft der Konsumenten personenbezogene Gesundheitsdaten preiszugeben erhöhen. Um diese Zusammenhänge genauer zu untersuchen, haben wir danach gefragt, welchen Einfluss das Framing der Produkteigenschaften und die Argumentationskraft der Datenschutzerklärung auf die Bereitschaft, personenbezogene Gesundheitsinformationen offenzulegen, haben.[51]

Empirische Einsichten

Zur Beantwortung dieser Frage wurde ein Online-Experiment mit 529 Teilnehmern durchgeführt. Im Rahmen des Experiments haben wir den Teilnehmern die Fitnessarmbanduhr Charge 2 des Anbieters Fitbit vorgestellt. Hierfür wurde die Webseite der originalen Fitbit Charge 2 hinsichtlich der Produkteigenschaften und der Datenschutzerklärung angepasst. Die Produkteigenschaften wurden verlustorientiert, neutral und gewinnorientiert formuliert, um zu untersuchen, ob positiv formulierte Produkteigenschaften die Konsumenten motivieren, personenbezogene Gesundheitsinformationen preiszugeben. Bei der Datenschutzerklärung wurde zwischen logischen, unlogischen und keinen Argumenten für die Datenerhebung unterschieden. Die Hypothese war, dass Konsumenten ihre Daten eher offenlegen, wenn ihnen überzeugendere Datenschutzerklärungen mit hoher Argumentationskraft präsentiert werden. Nach der Erkundung der Webseite sollten die Teilnehmer angeben, in welchem Ausmaß sie dem Anbieter Fitbit personenbezogene Gesundheitsdaten bereitstellen würden.

Die Ergebnisse sind in Abb. 4 dargestellt. Unsere Studie zeigt, dass Konsumenten, denen positiv formulierte Produkteigenschaften präsentiert werden, eher dazu bereit sind personenbezogene Gesundheitsdaten offenzulegen. Dies bedeutet, dass bei diesen Konsumenten die wahrgenommenen positiven Produkteigenschaften gegenüber den wahrgenommenen Risiken überwiegen. Daher sind sie eher dazu geneigt, das Risiko der Datenpreisgabe einzugehen. Des Weiteren zeigen die Ergebnisse der Studie, dass eine Datenschutzerklärung mit starker Argumentationskraft überzeugender auf die Verbraucher wirkt als unlogische oder gar keine Argumente. Interessanterweise zeigen die Ergebnisse aber auch, dass unlogische Argumente zu einer höheren Bereitschaft führen Daten offenzulegen als fehlende

[51] Ebd.

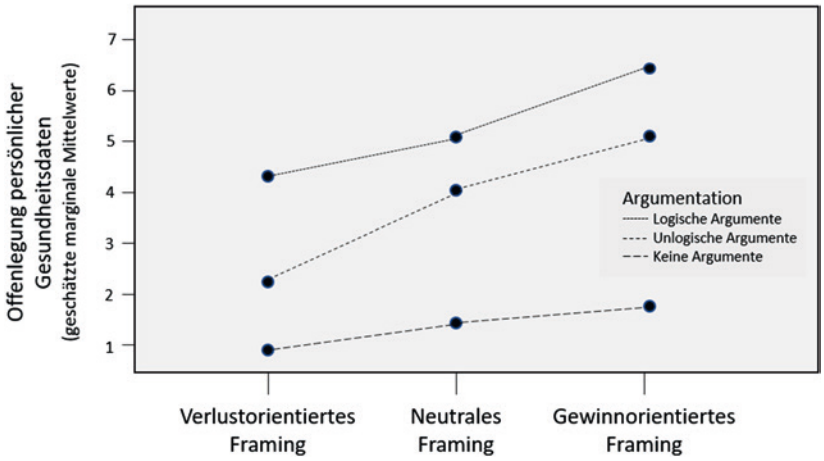

Abb. 4. Offenlegung und Framing (basierend auf Becker et al. 2020)

Argumente. Dieses Phänomen der placebischen Informationen wurde auch schon von früheren Studien nachgewiesen.[52] Mitunter kann der Einsatz unlogischer Argumente effektiver sein als das Fehlen jeglicher Begründung, da Verbraucher die Datenschutzerklärung oft nur gedankenlos überfliegen, anstatt sie aufmerksam zu lesen.

Zusammenfassend lässt sich sagen, dass eine Datenschutzerklärung mit hoher Argumentationskraft die wahrgenommen Risiken der Datenerfassung minimiert, während positiv formulierte Produkteigenschaften die wahrgenommenen Vorteile der Datenerfassung maximieren. Folglich wird die Bereitschaft der Verbraucher, personenbezogene Gesundheitsdaten zur Nutzung von Health Wearables offenzulegen, gesteigert. Die Erkenntnisse unserer Studie zeigen damit auch, dass Anbieter von Health Wearables davon profitieren können, die Argumentationskraft der Datenerfassung und das Framing der Produkteigenschaften anzupassen und somit die Offenlegungsbereitschaft ihrer Kunden zu erhöhen.

[52] z. B. Langer et al. (1978).

4.3 Die Rolle der Privatsphäre Dritter im Entscheidungskalkül eines Konsumenten

Viele Studien gehen implizit davon aus, dass Konsumenten lediglich personenbezogene Daten zu ihrer Person offenlegen (oder eben nicht). Gerade in sozialen Netzwerken sieht man, dass diese Annahme so allgemein nicht mehr stimmt. Somit kann das Offenlegungsverhalten von Verbrauchern nicht nur ihre eigene Privatsphäre (interne Privatsphäre), sondern auch die Privatsphäre von Dritten (externe Privatsphäre) gefährden. Um ihren Erfolg zu sichern, ist es daher für Anbieter sozialer Netzwerke ausschlaggebend zu verstehen, inwieweit Konsumenten die Privatsphäre Dritter in ihrem Entscheidungskalkül zur Offenlegung personenbezogener Daten berücksichtigen.

Kontext

Um dies genauer zu erforschen haben wir in Morlok[53] untersucht, wie die Intention Informationen über andere in sozialen Netzwerken zu teilen durch externe Privatheitsbedenken beeinflusst wird. Außerdem haben wir untersucht, inwiefern Erfahrungen mit Privatsphäreingriffen die externen Privatheitsbedenken und die Intention, Informationen über Dritte zu teilen, beeinflussen.

Ein wichtiger Unterschied sozialer Netzwerke zu anderen Kontexten, in denen personenbezogene Daten preisgegeben werden, ist, dass die Informationen nicht nur gegenüber einer Organisation, sondern auch gegenüber anderen Verbrauchern offengelegt werden. Daher haben Konsumenten nicht nur informationelle Privatheitsbedenken gegenüber der Organisation, wie beispielsweise Facebook, sondern auch soziale Privatheitsbedenken gegenüber anderen Verbrauchern. Folglich kann zwischen *externen informationellen Privatheitsbedenken,* das heißt Bedenken, dass das Verhalten von Organisationen die externe Privatsphäre negativ beeinflusst, und *externen sozialen Privatheitsbedenken,* das heißt Bedenken in Bezug auf die Handhabung der offengelegten Daten durch andere Verbraucher, unterschieden werden. Die *externen sozialen Privatheitsbedenken* setzen sich wiederum aus drei Dimensionen zusammen: Exposition, Eindringen und Identifizierung. Exposition bezieht sich auf die Enthüllung physischer und emotionaler Eigenschaften eines Individuums, wie beispielsweise Kummer oder Nacktheit. Eindringen bezieht sich auf das wahrgenommene Eingreifen in die Privatsphäre

[53] Morlok (2016).

und das personenbezogene Leben eines Individuums wie beispielsweise dessen Komfortzone. Und Identifizierung beschreibt das Bedenken, dass identifizierbare Informationen ermöglichen, dass ein Individuum identifiziert oder lokalisiert werden kann.

Theoretische Grundlagen

Als theoretische Grundlage zur Untersuchung dieses Phänomens eignet sich die *Communication Privacy Management Theory,* da sie ein konzeptionelles Verständnis für den Umgang mit der Privatsphäre anderer Individuen bereitstellt.[54] Die Theorie bezieht sich auf sogenannte metaphorische Grenzen, die aufzeigen, wie Individuen mit ihrer eigenen und der Privatsphäre Dritter umgehen. Hierbei müssen Individuen sowohl personenbezogene als auch kollektive Grenzen gleichzeitig managen. Personenbezogene Grenzen beschreiben die eigene Privatsphäre, während sich kollektive Grenzen auf die Privatsphäre anderer Personen beziehen. Petronio argumentiert, dass Individuen sich auch für die Privatsphäre anderer verantwortlich fühlen.[55]

Basierend auf der *Communication Privacy Management Theory* wurde ein Forschungsmodell entwickelt, das sowohl den Einfluss *externer informationeller Privatheitsbedenken* als auch *externer sozialer Privatheitsbedenken* auf die Bereitschaft, personenbezogene Daten offenzulegen, untersucht. Die *externen sozialen Privatheitsbedenken* setzen sich in dem Modell aus Expositionsbedenken, Eindringungsbedenken und Identifikationsbedenken zusammen. Außerdem vermuten wir, dass Konsumenten, sobald sie einmal eine Verletzung ihrer internen Privatsphäre erlebt haben, eher zögern, Informationen anderer preiszugeben. Folglich stellen wir die Hypothese auf, dass ein vorheriges Eindringen in die personenbezogene Privatsphäre den Einfluss von externen sozialen und informationellen Privatheitsbedenken auf die Offenlegungsbereitschaft moderiert. Des Weiteren stellen wir die Hypothese auf, dass der wahrgenommene Besitz der Informationen von Dritten einen positiven Einfluss auf die Bereitschaft hat, diese Daten offenzulegen. Das Phänomen des wahrgenommenen Besitzes beschreibt, dass Konsumenten die Daten Dritter als ihr Eigentum wahrnehmen, wenn sie Kontrolle über diese haben.

[54] Petronio (2002).

[55] Ebd.

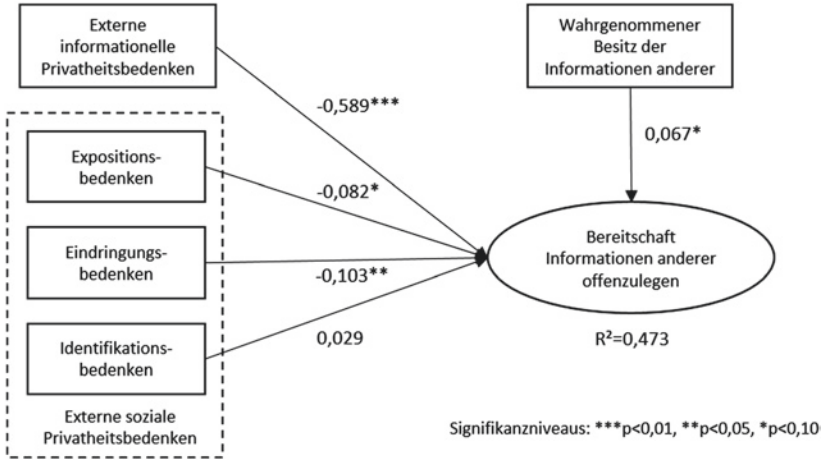

Abb. 5. Determinanten der Bereitschaft zur Offenlegung von Daten Dritter (basierend auf Morlok, 2016)

Empirische Einsichten

Um das Forschungsmodell zu überprüfen, haben wir in Morlok[56] eine Online-Umfrage mit 265 Teilnehmern durchgeführt und anhand eines Strukturgleichungsmodells ausgewertet (Abb. 5).

Die Ergebnisse zeigen, dass sich die Absicht von Konsumenten personenbezogene Daten in sozialen Netzwerken offenzulegen sowohl durch die externen sozialen und informationellen Privatheitsbedenken als auch den wahrgenommenen Besitz der Informationen von Dritten erklären lässt. Der wahrgenommene Besitz der Informationen von Dritten verstärkt die Offenlegungsbereitschaft der Konsumenten. Haben Verbraucher allerdings externe informationelle Privatheitsbedenken, hat dies einen negativen Einfluss auf ihre Bereitschaft personenbezogene Daten offenzulegen. Auch Expositionsbedenken und Eindringungsbedenken verringern die Offenlegungsbereitschaft der Konsumenten, während die dritte Dimension der externen sozialen Privatheitsbedenken, die Identifikationsbedenken, keinen signifikanten Einfluss auf die Offenlegungsabsicht hat. Allerdings zeigt die Studie auch, dass diese Zusammenhänge stark

[56] Morlok (2016).

davon abhängen, ob ein Verbraucher in der Vergangenheit Opfer eines Eingriffs in seine persönliche Privatsphäre geworden ist. Verbraucher, die bereits eine Verletzung ihrer Privatsphäre erfahren haben, machen ihr Offenlegungsverhalten von den Eindringungsbedenken abhängig, nicht aber von Identifikationsbedenken. Konsumenten, die diese Erfahrung noch nicht gemacht haben, sind sich zusätzlich auch der Expositionsbedenken bewusst. Diese Ergebnisse verdeutlichen die bisher kaum untersuchte, aber sehr komplexe Beziehung zwischen externen sozialen Privatheitsbedenken und der Offenlegungsabsicht in sozialen Netzwerken. Wenn Verbraucher einmal einen Eingriff in ihre interne Privatsphäre erlebt haben, werden sie sich auch mehr Sorgen über den Eingriff in die externe Privatsphäre machen, da es für diese Verbraucher einfacher ist, sich in die Lage anderer zu versetzen. Somit hängt das Bewusstsein über die Bedrohungen der externen Privatsphäre von den Erfahrungen der Konsumenten mit eigenen Privatsphäreverletzungen ab.

Die Offenlegung personenbezogener Daten spielt eine wichtige Rolle für Anbieter sozialer Netzwerke, da sie soziale Interaktion, Personalisierung und Ausspielung passender Werbung ermöglicht. Mit dieser Studie zeigen wir in Morlok[57], dass die externen Privatheitsbedenken der Verbraucher eine wichtige Rolle im Zusammenhang mit der Offenlegung personenbezogener Daten in sozialen Netzwerken spielen. Für die Betreiber sozialer Netzwerke bedeutet das, dass nicht nur Kontrollmechanismen zur Gewährleistung der internen, sondern auch der externen Privatsphäre implementiert werden sollten. Außerdem sollten sowohl informationelle als auch soziale Aspekte beim Datenschutz beachtet werden. Die Berücksichtigung dieser beiden Aspekte kann den Betreibern sozialer Netzwerke helfen, die Loyalität ihrer Verbraucher zu stärken und sich so von der Konkurrenz zu differenzieren.

5 Zusammenfassung und Ausblick

Die wirtschaftswissenschaftliche Forschung zur Privatheit um das Zusammenspiel von Unternehmen und Verbrauchern hat sich bisher stark auf die Personalisierung von Angeboten und die verbesserten Möglichkeiten der Differenzierung von Preisen fokussiert. Dies sind wichtige und interessante Perspektiven. Zur vollständigen Erfassung des Phänomens der informationellen

[57] Ebd.

Privatheit, insbesondere vor dem Hintergrund der technischen Entwicklungen bei der Erfassung und der Verarbeitung von Daten, greift dies aber zu kurz. Daher haben wir eine Reihe von Projekten durchgeführt, die bewusst einige wichtige weitere Perspektiven eingenommen haben. Das vorliegende Kapitel gibt einen Überblick über die zentralen Ergebnisse dieser Projekte.

Ein erster Teil der Projekte lässt sich in der unternehmenszentrierten Perspektive verankern. Zwei Szenarien der Verwendung von personenbezogenen Daten durch Unternehmen sind der Datenhandel auf sogenannten Datenmärkten und die unternehmensinterne Verwendung von Daten zwecks Auswertung. In einer ersten Studie wird aus struktureller Perspektive die Wertschöpfung auf Märkten für personenbezogene Daten am Beispiel des Marktes für Online-Werbung untersucht. Die Studie zeigt auf, welche Akteure auf Datenmärkten miteinander agieren und wie personenbezogene Daten zur Wertschöpfung genutzt werden. Die unternehmensinterne Nutzung von Daten zur Schaffung von Synergien wird in einer zweiten Studie thematisiert. Das im Rahmen dieser Studie erarbeitete konzeptionelle Framework zeigt auf, welche unternehmensinternen Voraussetzungen auf Management- und Datenebene gegeben sein müssen, damit Synergieeffekte aus Daten realisiert werden können.

Ein zweiter Teil unserer Projekte bezieht sich auf die verbraucherorientierte Perspektive. Von zentraler Bedeutung sind hier die Offenlegung von Daten sowie die Zahlungsbereitschaft für den Verzicht auf die Weitergabe von Daten. Eine erste Studie hat die Zahlungsbereitschaft von Konsumenten für personenbezogene Daten in sozialen Netzwerken untersucht. Dabei zeigte sich, dass die Zahlungsbereitschaft für eine privatsphäreschützende Premiumversion eines sozialen Netzwerkes signifikant durch den wahrgenommenen Nutzen und das Vertrauen in die Plattform beeinflusst wird. Neben dem Wert, den Verbraucher ihren personenbezogenen Daten beimessen, ist ebenfalls deren Bereitschaft, besagte Daten preiszugeben, relevant. In einer zweiten Studie wurde anhand des Beispiels von Health Wearables dargestellt, dass Konsumenten durch eine aussagekräftige Datenschutzerklärung und positiv formulierte Produkteigenschaften zur Offenlegung ihrer personenbezogenen Gesundheitsdaten bestärkt werden können. Dass Konsumenten nicht nur ihre eigenen personenbezogenen Daten, sondern auch die Daten Dritter in Händen halten, wird von einer dritten Studie herausgearbeitet. In diesem Kontext wird betont, dass Plattformbetreiber nicht nur auf interne Privatheitsbedenken von Konsumenten, sondern auch auf deren externe Privatheitsbedenken eingehen sollten.

Dieses Thema ist keinesfalls erschöpfend behandelt. Schon jetzt bestehen weitere wichtige Lücken. Exemplarisch sei der Umgang mit Privatheit am Arbeitsplatz genannt, hierzu gibt es bisher nur sehr wenige Studien. Darüber

hinaus wird es, aufgrund von technischen Entwicklungen, zu weiteren Lücken kommen. Die zunehmende Verbreitung von mobilen Endgeräten führt zu einer wachsenden Vernetzung der Konsumenten – und das nicht nur untereinander. Man denke daher nur an technologische Trends wie das Internet der Dinge, das physische Objektive mit dem Internet und somit mit dem Konsumenten verbindet. Die zunehmende Entwicklung solcher digitalen Technologien treibt die wachsende Generierung personenbezogener Daten der Verbraucher voran. Dies stellt sowohl die Praxis als auch die Forschung vor immer neue Herausforderungen und fordert neue Gestaltungsansätze. Das Kapitel von Conrad u. a. in diesem Band geht auf jene Gestaltungsansätze ein und beschreibt, wie erhöhte Transparenz über den eigenen digitalen Fußabdruck die informationelle Selbstbestimmung von Konsumenten schützen kann.

Literatur

Ackoff, R. L. (1971). Towards a system of systems concepts. *Management Science, 17(11)*, 661–671.

Acquisti, A., & Fong, C. (2020). An experiment in hiring discrimination via online social networks. *Management Science, 66(3)*, 1005–1024.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature, 54(2)*, 442–492.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50(2)*, 179–211.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly, 30(1)*, 13–28.

Becker, M., Matt, C., & Hess, T. (2020). It's not just about the product: How persuasive communication affects the disclosure of personal health information. *ACM SIGMIS Database: The Database for Advances in Information Systems, 51(1)*, 37–50.

Bründl, S., Matt, C., & Hess, T. (2015). *Wertschöpfung in Datenmärkten – Eine explorative Untersuchung am Beispiel des deutschen Marktes für persönliche Daten*. Ludwig-Maximilans-Universität, Institut für Wirtschaftsinformatik und Neue Medien (WIM).

Bründl, S., Matt, C., & Hess, T. (2016). Daten als Geschäft – Rollen und Wertschöpfungsstrukturen im deutschen Markt für persönliche Daten. *Wirtschaftsinformatik & Management, 8(6)*, 66–71.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6(2)*, 181–202.

Connolly, R., & McParland, C. (2012). Dataveillance: Employee monitoring & information privacy concerns in the workplace. *Journal of Information Technology Research, 5(2)*, 31–45.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17(1)*, 61–80.

Egelman, S., Felt, A. P., & Wagner, D. (2013). Choice architecture and smartphone privacy: There's a price for that. In: R. Böhme (Hrsg.), *The economics of information security and privacy*. Springer, 211-236.

Hann, I.-H., Hui, K.-L., Lee, S.-Y., & Png, I. P. L. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24(2)*, 13–42.

Hartmann, P. M., Zaki, M., Feldmann, N., & Neely, A. (2016). Capturing value from big data – A taxonomy of data-driven business models used by start-up firms. *International Journal of Operations & Production Management, 36(10)*, 1382–1406.

Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization-privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems, 34(2)*, 369–400.

Kelleher, J. D., Namee, M., & Brian und D'arcy, Aoife,. (2015). *Fundamentals of machine learning for predictive data analytics: Algorithms, worked examples, and case studies*. MIT Press.

Langer, E. J, Blank, A., & Chanowitz, B. (1978). The mindlessness of ostensibly thoughtful action: The role of "placebic" information in interpersonal interaction. *Journal of Personality and Social Psychology, 36(6)*, 635-642.

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues, 59(2)*, 243–261.

Martin, N., Matt, C., Niebel, C., & Blind, K. (2019). How data protection regulation affects startup innovation. *Information Systems Frontiers, 21(6)*, 1307–1324.

Morlok, T. (2016). Sharing is (not) caring-the role of external privacy in users' information disclosure behaviors on social network sites. In *Proceedings of the 20th Pacific Asia Conference on Information Systems (PACIS), 2016, Chiayi, Taiwan.*

Morlok, T., Matt, C., & Hess, T. (2017). *Privatheitsforschung in den Wirtschaftswissenschaften: Entwicklung, Stand und Perspektiven*. Ludwig-Maximilians-Universität, Institut für Wirtschaftsinformatik und Neue Medien (WIM).

Morlok, T., Matt, C., & Hess, T. (2018). Perspektiven der Privatheitsforschung in den Wirtschaftswissenschaften.In: M. Friedewald (Hrsg.): *Privatheit und selbstbestimmtes Leben in der digitalen Welt*. Springer, 179-220.

Nevo, S., & Wade, M. R. (2010). The formation and value of IT-enabled resources: Antecedents and consequences of synergistic relationships. *MIS Quarterly, 34(1)*, 163–183.

Nguyen, K. D., Rosoff, H., & John, R. S. (2016). The effects of attacker identity and individual user characteristics on the value of information privacy. *Computers in Human Behavior, 55*, 372–383.

Ochs, C., Friedewald, M., Hess, T., & Lamla, J. (2019). *Die Zukunft der Datenökonomie: Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz*. Springer Fachmedien.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

Pu, Y., & Grossklags, J. (2016). Towards a model on the factors influencing social app users' valuation of interdependent privacy. *Proceedings on Privacy Enhancing Technologies, 2,* 61-81.

Schoeman, F. D. (1984). Privacy: Philosophical dimensions of the literature. In: F.D. Schoeman (Hrsg.), *Philosophical dimensions of privacy: An anthology*. Cambridge University Press.

Schöning, C., Matt, C., & Hess, T. (2019). Personalised nudging for more data disclosure? On the adaption of data usage policies format to cognitive styles. In *Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS), 2019, Hawaii, USA*.

Schreiner, M., & Hess, T. (2013). Published. On the willingness to pay for privacy as a freemium model: First empirical Evidence. In *Proceedings of the 21st European Conference on Information Systems (ECIS), 2013, Utrecht, Niederlande.*

Schreiner, M., & Hess, T. (2015). Why are consumers willing to pay for privacy? An application of the privacy-freemium model to media companies. C*ompleted Research Paper of the 23rd European Conference on Information Systems (ECIS), 2015, Münster, Deutschland.*

Shollo, A., & Galliers, R. D. (2016). Towards an understanding of the role of business intelligence systems in organisational knowing. *Information Systems Journal, 26(4)*, 339–367.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35(4)*, 989–1015.

Someh, I. A., & Shanks, G. (2013). The role of synergy in achieving value from business analytics systems. In *Proceedings of the 34th International Conference on Information Systems (ICIS), 2013, Mailand, Italien.*

Wagner, A., Wessels, N., Buxmann, P., & Krasnova, H. (2018). Putting a Price Tag on Personal Information – A Literature Review. In *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS), 2018, Hawaii, USA*.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4(3)*, 193–220.

Weibl, J., & Hess, T. (2020). Turning data into value – Exploring the role of synergy in leveraging value among data. *Information Systems Management, 37(3)*, 227–239.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum Press.

Winegar, A. G., & Sunstein, C. R. (2019). How much is data privacy worth? A preliminary investigation. *Journal of Consumer Policy, 42(3)*, 425–440.

Wixom, B. H., & Ross, J. W. (2017). How to monetize your data. *MIT Sloan Management Review, 58(3)*, 9–13.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51(1)*, 42–52.

Prof. Dr. Thomas Hess ist Direktor des Instituts für Digitales Management und Neue Medien der Fakultät für Betriebswirtschaft der Ludwig-Maximilians-Universität München.

Prof. Dr. Christian Matt ist Professor und Mitdirektor des Instituts für Wirtschaftsinformatik der Universität Bern.

Verena Thürmel ist wissenschaftliche Mitarbeiterin des Instituts für Digitales Management und Neue Medien der Ludwig-Maximilians-Universität München.

Mena Teebken ist wissenschaftliche Mitarbeiterin des Instituts für Digitales Management und Neue Medien der Ludwig-Maximilians-Universität München.

Privatheit und Digitalität

Zur soziotechnischen Transformation des selbstbestimmten Lebens

Jörn Lamla, Barbara Büttner, Carsten Ochs, Fabian Pittroff und Markus Uhlmann

1 Einleitung

Der vorliegende Beitrag wendet sich dem ambivalenten Zusammenspiel von Privatheit und Digitalität zu, indem er deren Relevanz für Diskurse und Praktiken der Selbstbestimmung ausleuchtet und auf die soziotechnischen Transformationen dieses Zusammenspiels bezieht. Er bedient sich hierfür soziologischer Mittel der theoretischen Perspektivierung ebenso wie der fallbezogenen empirischen Analyse. Das bedeutet zunächst, dass Privatheit und Digitalität nicht als außersoziale Gegenstandsbereiche verstanden werden – etwa als von der Gesellschaft losgelöste Sphäre des Privatlebens bzw. als rein technisch dominierte Interaktivität von Bits and Bytes –, sondern als spezifische Sozialformen, Assemblagen

J. Lamla (✉) · B. Büttner · C. Ochs · F. Pittroff · M. Uhlmann
Universität Kassel, Kassel, Deutschland
E-Mail: lamla@uni-kassel.de

B. Büttner
E-Mail: barbara.buettner@uni-kassel.de

C. Ochs
E-Mail: carsten.ochs@uni-kassel.de

F. Pittroff
E-Mail: pittroff@uni-kassel.de

M. Uhlmann
E-Mail: markus.uhlmann@uni-kassel.de

A. Roßnagel und M. Friedewald (Hrsg.), *Die Zukunft von Privatheit und Selbstbestimmung,* DuD-Fachbeiträge,
https://doi.org/10.1007/978-3-658-35263-9_4

oder Kommunikationsverhältnisse, die gesellschaftlich mitkonstituiert oder konfiguriert, d. h. etwa von historisch sich wandelnden kulturellen Bedeutungsschichten, sozialen, ökonomischen und politischen Machtverhältnissen sowie normativen Regelkomplexen und Konventionen der Gesellschaft durchzogen sind.

In diesem Sinne sollen hier in einem ersten Schritt die umfangreichen Wissensbestände der soziologischen Gesellschaftstheorie konsultiert werden, um nach sozialen Aspekten von Privatheit und Digitalität zu fahnden und diese in die Analyse von Selbstbestimmungspraktiken und -diskursen einzubeziehen. Hierzu wird zunächst im *zweiten Abschnitt* eine kursorische Darstellung gesellschaftstheoretischer Perspektiven auf Privatheit vorgenommen, die nicht auf Vollständigkeit zielt, sondern darauf, die sozialen Aspekte von Privatheit in ihrer Breite und Relevanz vor Augen zu führen (2.1). Im zweiten Schritt ist der mögliche Bias einer solchen Perspektivierung und Konzeptualisierung von Privatheit zu berücksichtigen: Die fachinternen Diskussionen und Revisionen, die das soziologische Denken durch die Hinwendung zu Phänomenen der Digitalität herausfordern und mit neuen An- und Einsichten konfrontieren, lassen auch die Konzeptualisierung von Privatheit nicht unberührt; vielmehr gilt es zu reflektieren, inwiefern das soziologische Bild von Privatheit in dem Maße korrigiert werden muss, in dem soziotechnische Formen und Muster der Digitalität das Soziale insgesamt in neuem Licht erscheinen lassen und klassische Denkwerkzeuge der Soziologie durch Aspekte des Technischen und Materiellen ergänzen. Der Wandel der technisch-medialen Kommunikationssubstrate von ‚oraler' bis ‚digitaler' Vergesellschaftungsweise lässt auch die sozial strukturierte Privatheit nicht unbeeinflusst. Doch ist dieser technisch-materielle Aspekt des Privaten in sozialwissenschaftlichen Konzeptualisierungen von Privatheit hinreichend berücksichtigt worden? Die Behandlung dieser Frage rundet die theoretischen Überlegungen zum Verhältnis von Privatheit und Digitalität ab und mündet in dem Vorschlag, beide mit Theoriemitteln zu konzeptualisieren und aufeinander zu beziehen, die sich Impulsen der *science and technology studies* (STS) verdanken (2.2).

Mit einer solchen theoretischen Voreinstellung der Analyse des Verhältnisses von Privatheit und Digitalität wird eine fundiertere Analyse von Diskursen und Praktiken der Selbstbestimmung unter den veränderten sozio-digitalen Verhältnissen der Gegenwartsgesellschaft möglich. Diese soll exemplarisch an vier zentralen Problemfeldern von Privatheit und Digitalität vorgenommen werden: Vor dem Hintergrund soziologischer Zeitdiagnosen zu den Transformationsdynamiken digitaler Vergesellschaftung und deren Auswirkungen auf den gesellschaftlichen Status und die gesellschaftlichen Strukturbedingungen von Privatheit wird im *dritten Abschnitt* zunächst herausgearbeitet, wie zeitgenössische Vergesellschaftungsformen *Sichtbarkeit* prämieren und dadurch

ein Verhalten evozieren, das die Möglichkeiten datenverarbeitender Erfassung stark erweitert (3.1). Der nachfolgende Abschnitt diskutiert sodann, welche Konsequenzen für Privatheit sich aus den Potentialen der *Verhaltensformung* ergeben, die mit der Gestaltung soziodigitaler Infrastrukturen[1] seitens der Architektinnen komplexer digitaler Dienste, sozialer Netzwerke und Plattformen einhergehen (3.2). Anschließend wird erörtert, inwiefern die gegenwärtigen *Erlösmodelle der Datenökonomie* von datenintensiven Subjektivierungspraktiken abhängig sind. Die Vermutung ist hier, dass durch ökonomischen Verwertungsdruck die Verknüpfungen zwischen datenbasierter Verhaltensbeeinflussung und digitaler Selbstoffenbarung immer feinmaschiger werden und sich selbstverstärkende Feedbackschleifen etablieren (3.3). Der vierte Abschnitt argumentiert dann, dass diese Transformationsdynamiken die *Entscheidungsfreiheiten von Nutzenden* unterminieren und damit hergebrachte Selbstbestimmungskonzepte massiv unter Druck setzen. An dieser degenerativen Transformation der demokratischen Grundidee der Selbstbestimmung soll schließlich die ambivalente Entwicklung von Privatheit und Digitalität zusammengefasst werden (3.4).

Im Fazit des Beitrags werden Konsequenzen für eine soziotechnische Gestaltung von Privatheit, die an demokratischen Grundideen der Selbstbestimmung explizit und umfassend orientiert bleiben will, aufgezeigt (4). Die zentrale Frage ist hierbei, ob und gegebenenfalls wie sich eine digitale Form der Privatheit (er)finden lässt, die eine normativ anspruchsvolle soziotechnische Übersetzung und Erneuerung der demokratischen Selbstbestimmungsidee ermöglicht. Dies betrifft etwa die Frage, wie sich am Back-End digitaler Dienste Bedingungen verankern lassen, die trotz datenintensiver Sozialpraktiken Formen der Privatheit garantieren können. Hier lässt sich teilweise auf ältere soziologische Theorien der Privatheit zurückgreifen, die das Wechselspiel von Privatheit, Vertrauen und Zivilität als Gelingensbedingungen stabiler Sozialbeziehungen bereits an früheren Epochen thematisiert oder kreative Praktiken der Aneignung von technischen oder staatlichen Infrastrukturen fokussiert haben, welche deren Kontrollpotentiale zu unterlaufen vermögen. Im Ergebnis zeigt sich ein erheblicher Bedarf an einer Politik der Gestaltung und Regulierung von

[1] Infrastruktur meint in dieser Betrachtung weit mehr als Glasfaserkabel und andere Technologien des Zugangs zum Digitalen. Der Begriff betont die Verschränkung technisch-materieller und sozialer Formierungskräfte, die das digitale Leben deshalb robust strukturieren, weil sie in der alltagspraktischen kommunikativen Verwendung weitgehend in den Hintergrund treten und nur bei Störungen sichtbar werden (vgl. Star & Ruhleder, 1996).

soziodigitalen Infrastrukturen, die solche Freiräume nicht nur weiterhin erhält, sondern zudem eine andere Datenökonomie ermöglicht und fördert, die sich der demokratischen Kontrolle, Mitbestimmung und vor allem sorgfältiger Kritik konsequent öffnet, anstatt die erkämpften Spielräume der Selbstbestimmung durch neue Finten latenter Verhaltensformung zu unterlaufen.

2 Zur soziologischen Perspektivierung von Privatheit und Digitalität

2.1 Privatheit in der Sozial- und Gesellschaftstheorie

Dass Privatheit keine Privatangelegenheit, sondern durch und durch sozial und gesellschaftsgeschichtlich figuriert ist, ist eine Grundeinsicht soziologischer Perspektivierungen. So sind etwa die Bedeutungszunahme von Individualität als Bezugsgröße für Lebenssinn und -orientierung, die Rätsel und Geheimnisse subjektiver Erlebnis- und Innenwelten, die Abgrenzung von Territorien für verletzliche Körper und ihre intimen Verrichtungen, das Verleihen von liberalen Abwehrrechten gegenüber dem Staat oder das Mischungsverhältnis von Prominenz und Zurückgezogenheit vieler Personen von sozialen Beziehungsgefügen, kulturellem Wandel, geografischer Lage und politisch-rechtlichen Kämpfen abhängig und variieren mit diesen stark. Privatheit bleibt selbst dort noch eine gesellschaftliche Institution, wo sie sich inhaltlich ganz auf das singuläre Individuum bezieht und dessen Unabhängigkeit zu sichern verspricht. Ein solcher radikaler Bezug auf das Individuum ist dabei jedoch weder in normativer Hinsicht noch in geschichtlicher oder kultureller Perspektive notwendig oder plausibel – auch wenn er sowohl in öffentlich-medialen als auch vielen wissenschaftlichen Konzeptualisierungen oft spontan zugrunde gelegt wird (Bennett, 2011, S. 486). Nicht nur finden sich in der Forschungslandschaft wichtige Privatheitskonzepte, die auf die Privatheit von Kollektiven abstellen, etwa Blousteins (Bloustein, 2003) Konzept der „group privacy“; vielmehr erweist sich eine allzu enge definitorische Verknüpfung von Privatheit mit dem Individuum gerade vor dem Hintergrund der seit einigen Jahren beobachtbaren soziotechnischen Vernetzungsprozesse als immer weniger plausibel (Roessler, 2010; Roessler & Mokrosinska, 2013). Ein Verständnis von Privatheit, das Individuen in einem (und sei es auch nur teilweise) „gesellschaftsfreien Raum“ verortet, evoziert folglich grundfalsche Assoziationen (Barth, 2016, S. 484, Nassehi, 2014, S. 33).

Privatheit, bürgerliche Individualität oder subjektive Autonomie sind demnach soziale Konstruktionen – nicht im Sinne bloßer Erfindungen, denen eine soziale Wirklichkeit gegenübersteht, sondern im Sinne realitätsgestaltender sozialer Konzepte und Materialisierungen. Um Aspekte dieser sozialen Konstruktion freizulegen – insbesondere mit Blick auf die durch digitale Technologien herausgeforderte informationelle Privatheit –, werden im Folgenden kursorisch einige wichtige Perspektiven der Sozial- und Gesellschaftstheorie auf Privatheit vorgestellt. Ein Seitenblick gilt dabei der Frage, inwiefern diese Theorien die materiellen und infrastrukturellen Aspekte der Hervorbringung und Institutionalisierung von Privatheit berücksichtigen oder aber theoretische Horizonterweiterungen erforderlich sind, um das soziotechnische Zusammenspiel von Privatheit und Digitalität angemessen untersuchen zu können.

Ein erstes Beispiel für die Verankerung des Privaten in einer gesellschaftlichen Ordnungsstruktur liefert bereits der Blick auf die griechische Antike. So führt Hannah Arendt (2010) die Unterscheidung zwischen Privatem und Öffentlichem auf den Unterschied zwischen *oikos* und *polis* zurück: Ersteres bezeichnet den unveräußerlichen Stammsitz des patriarchal beherrschten Familienklans einschließlich der Sklaven und damit eine gleichzeitig räumlich, eigentumsmäßig und familiär zu verstehende Privat*sphäre*, die als Reich des Notwendigen sowohl der wirtschaftlichen als auch biologischen Reproduktion dient. Wirtschaftlicher Wohlstand wird gleichwohl nicht um seiner selbst willen angestrebt, sondern weil die Befreiung von der Notwendigkeit als Voraussetzung für Freiheit schlechthin gilt, die die Möglichkeit voraussetzt, in der *polis,* der politischen Öffentlichkeit des Stadtstaats, zu agieren. Während Arendt somit die öffentliche Sphäre als maßgeblichen Handlungsbereich der griechischen Stadtkultur der Antike in Anschlag bringt, charakterisiert sie die beiden Sphären doch als sich wechselseitig bedingend (Arendt, 2010, S. 77). Ein solches, auf dichotome Sphärenunterscheidung abstellendes Verständnis von öffentlich und privat hat bereits in der römischen Antike eine weitergehende, rechtliche Verankerung erfahren und sich dann durch die europäische Kulturgeschichte hindurch verstetigt, auch wenn der „römisch-rechtliche Gegensatz von publicus und privatus“ im europäischen Mittelalter zwischenzeitlich „obschon gebräuchlich, ohne Verbindlichkeit“ ist. (Habermas, 1990, S. 58, vgl. auch Weintraub, 1997, S. 1) Wichtig ist hierbei, dass die mit dieser Unterscheidung verbundenen Freiheiten zur Selbstbestimmung, auch wenn sie historisch von der öffentlichen in die private Sphäre wandern und dort zunehmend mit der Individualität der Person in Abgrenzung von Staat und Gemeinschaft verknüpft werden, konzeptionell immer eng mit einer sozialen, infrastrukturellen und materiellen Unterlage verknüpft bleiben. Diese beinhaltet soziale und ökonomische Interdependenzen (etwa der Entlastung durch Sklaven

oder später dann privates Dienstpersonal) ebenso wie Rechte und deren mediale und infrastrukturelle Verankerung (etwa in einer Schriftkultur und weiteren Infrastrukturen der rechtlich-prozeduralen Streitaustragung).

Im Vergleich hierzu setzen sich dann mehr und mehr Perspektiven durch, die Selbstbestimmung mit normativen Idealen des aufkommenden liberalen Denkens und der Menschenrechte verknüpfen und diese zunehmend in der Sphäre des Privaten verorten. Dabei wird die ontologische Verankerung in materialen Praktiken und Strukturen nicht immer konsequent weiterverfolgt, sondern gerät diese bisweilen gegenüber geistesgeschichtlichen Erzählungen zur Durchsetzung von Vernunft, Freiheit und Zivilität ins Hintertreffen. Davon kaum betroffen ist jedoch die soziologische Rekonstruktion der Zivilisationsgeschichte durch Norbert Elias, insofern diese das psychogenetische „Vorrücken der Schamgrenze“ (Elias, 1997, S. 318) eng mit der schrittweisen Soziogenese von bürgerlichen Lebensformen ausgehend vom Mittelalter, den Entwicklungen der höfischen Aristokratie und der großen Staatsapparate im Absolutismus verknüpft. Elias liefert zahlreiche Belege dafür, dass insbesondere körperliche Verrichtungen – Essen, Schlafen, Körperreinigung, natürliche Funktionen – jeweils abgegrenzten und spezialisierten Sozialbereichen zugewiesen wurden. Die „immer stärkere Intimisierung aller körperlichen Funktionen, (…) ihre Einklammerung in bestimmten Enklaven, ihre Verlegung ‚hinter verschlossene Türen‘ hat Konsequenzen verschiedener Art“ (Elias, 1997, S. 354). So wird deren praktische und materiale Abgrenzung vom öffentlich einsehbaren Alltagsleben nach und nach auch auf dessen diskursive Thematisierung übertragen, sodass schließlich auch das öffentliche Erwähnen der fraglichen Inhalte verschwindet. Folge dieser Entwicklung ist eine den „Kult des Individuums“ (Durkheim, 1992, S. 478) hervorbringende und stützende Differenzierung des Sozialen, die nicht nur, aber auch als Vervielfältigung der öffentlich/privat-Unterscheidung auftritt: „Es scheiden sich mit anderen Worten im Leben der Menschen selbst mit der fortschreitenden Zivilisation immer stärker eine intime oder heimliche Sphäre und eine öffentliche Sphäre, ein heimliches Verhalten und ein öffentliches Verhalten voneinander.“ (Elias, 1997, S. 355)

Die Zivilisationstheorie von Elias zeigt, wie in der Sphäre des Privaten allmählich neue Innenwelten des modernen Subjekts emergieren und Vorstellungen individueller Selbstbestimmung hervortreten lassen, die gleichwohl sozial figuriert sind und auf geteilten kulturellen Praktiken basieren. Das gilt auch für die bürgerlichen Ausprägungen von Privatheit, die das kritische Räsonnement als neue Qualität einer „Öffentlichkeit von Privatleuten“ (Habermas, 1990, S. 90)

aus einer Figuration kultureller Praktiken entstehen lassen und zunehmend auf die politische Sphäre der öffentlichen Gewalt des Staates ausdehnen. Literarisch trainiert (d. h. in der Rezeption und Diskussion von Romanen genauso wie in der Produktion extensiven Briefverkehrs geschult) und oftmals kaufmännisch orientiert, ziehen sich die Bürger regelmäßig in die kleinfamiliale Einsamkeit ihrer Schreibstuben zurück, um von dort aus in die Öffentlichkeit der Salons hervorzutreten und kritischen Diskurs zu üben. Dieses viel diskutierte und „weltweit prominenteste" Öffentlichkeitskonzept (Hahn & Langenohl, 2017, S. 19) von Jürgen Habermas lässt nun Privatheit als Quelle der Selbstverwirklichung in neuem Licht erscheinen, insofern die Reiche der Freiheit (Öffentlichkeit) und der Notwendigkeit (Freiheit) nicht nur äußerlich, d. h. ökonomisch und materiell, aneinander hängen, sondern einen inneren Konstitutionszusammenhang moderner Vernunfttätigkeit bilden, für die Aspekte von Privatheit und Öffentlichkeit stets zusammenkommen müssen. Entsprechend heißt es in *Faktizität und Geltung,* dass „sich eine vitale Bürgergesellschaft nur im Kontext einer freiheitlichen politischen Kultur und entsprechender Sozialisationsmuster sowie auf der Basis einer unversehrten Privatsphäre herausbilden [kann] (…). Sonst entstehen populistische Bewegungen, die die verhärteten Traditionsbestände einer von kapitalistischer Modernisierung gefährdeten Lebenswelt blind verteidigen. Diese sind in den Formen ihrer Mobilisierung ebenso modern wie in ihren Zielsetzungen antidemokratisch." (Habermas, 1992, S. 449)

Die mit der bürgerlichen Privatheit verknüpften individualistischen Selbstverwirklichungsideen können die Erfahrungswelten der Innerlichkeit allerdings auch in einer Weise präferieren, dass diese die gesamte Kommunikation mit Erwartungen an die Authentizität von Personen überfrachten. Dominieren die besonderen Erfahrungsbereiche des Privaten auch die Erwartungen in der öffentlichen Sphäre, so kommt es zur „Tyrannei der Intimität" (Sennett, 2008), die jede Regung von der Alltagsinteraktion bis zum politischen Statement auf ihren psychologischen Gehalt hin befragt. Eine solche pathologische Entwicklung, in der die Umgangsformen zunehmend narzisstisch ausgerichtet sind, sieht der Soziologe Richard Sennett – ein Schüler Hannah Arendts – im Übergang von der spätabsolutistischen zur bürgerlichen Strukturierung des öffentlichen und privaten Lebens am Werk. Daran zeigt sich gleichsam ex negativo die Relevanz sozialer Differenzierungen und Begrenzungen von Erfahrungsbereichen, die in dem Maße durch kulturelle Kompetenzen einer auf das unabhängige Individuum zugeschnittenen Kommunikation aufrecht erhalten werden müssen, wie äußere Erwartungssicherheiten versiegen, etwa durch die soziale Maskerade und klare Statussignale

der ständischen Ordnung (z. B. Kleiderordnungen, Verkehrsmittel, Verhaltensstereotype und Ausdrucksformen).[2] Sennett zufolge braucht es Mittel und Fähigkeiten zur Abgrenzung von Erfahrungsfeldern und -qualitäten (Sennett, 2008, S. 35, 41), da ansonsten die Unterscheidung von Privatheit und Öffentlichkeit implodiert. Die im Anschluss an Habermas und Sennett brisante Frage lautet dann, unter welchen Bedingungen entsprechende Fähigkeiten in der Sozialisation ausgebildet werden.

Hierfür ist die Konsultation weiterer Klassiker der Soziologie wie Georg Simmel und Erving Goffman wichtig, die sich grundlegend den sozialen Interaktionsprozessen moderner Individuen zugewandt haben. Insbesondere Simmel hat die Notwendigkeit und Unvermeidlichkeit der Beschränkung von Transparenz als eine Grundbedingung interpersonaler Kommunikation in der Moderne identifiziert. Er geht davon aus, dass die sozialen Akteure zwar ein gewisses Wissen vom anderen haben müssten, gleichzeitig jedoch auch bestimmte „Nichtwissensquanta“ (Simmel, 1992, S. 394) diese Interaktionsgefüge strukturierten. Wer was über wen (legitimerweise) wisse oder nicht wisse, präge die sozialen Verhältnisse, so wie diese umgekehrt auch die wechselseitigen Wissensbestände bestimmten. In diesem Sinne sei das Geheimnis – „eine der größten Errungenschaften der Menschheit“ (Simmel, 1992, S. 406) – ein maßgebliches Strukturelement jeden sozialen Gefüges. Mit der modernen im Unterschied zur vormodernen Vergesellschaftungslogik wird diese Beschränkung wechselseitigen Wissens – die informationelle Privatheit *avant la lettre* – allerdings zunehmend anspruchs- und voraussetzungsvoller, da die zunehmende Differenzierung der sozialen Kreise und die damit einhergehenden Individualisierungsschübe die Anforderungen vervielfältigen. So werde selbst die auf Vertrautheit fußende Einrichtung der Freundschaft hiervon in Mitleidenschaft gezogen, insofern moderne Freundschaft im Unterschied zu antiken nicht mehr die Gesamtperson involviere, sondern lediglich einen bestimmten Persönlichkeitsaspekt. Moderne Individuen müssen folglich stets darauf achten, den Informationsfluss über differenzierte Freundschaftsverhältnisse hinweg einzuschränken, denn differenzierte Freundschaften „fordern, daß die Freunde gegen-

[2] So lässt sich im Anschluss an Elias die Beobachtung einer partiellen Zurücknahme von Scham- und Peinlichkeitsschwellen in der Moderne (öffentliches Küssen, FKK-Strände u. v. m.) als eine Entwicklung einschätzen, die weniger einen historischen Rückschritt im Zivilisationsprozess markiert als vielmehr eine Flexibilisierung anzeigt, die nur durch die lange Einübung und erfolgte Festigung ziviler Kompetenzen möglich wurde (Elias 1997, S. 350 f.).

seitig nicht in die Interessen und Gefühlsgebiete hineinsehen, die nun einmal nicht in die Beziehung eingeschlossen sind und deren Berührung die Grenze des gegenseitigen Sich-Verstehens schmerzlich fühlbar machen würde.“ (Roessler & Mokrosinska, 2013, S. 401 f.)

An diesem Beispiel wird schon deutlich, dass informationelle Privatheit unter modernen Bedingungen schnell zur Überforderung der individuellen Akteure werden kann. Diese benötigen hohe Kompetenzen darin, ihre verschiedenen Interaktionsbeziehungen aktiv zu managen. Wie dies konkret geschieht und welche Mittel ihnen hierfür zur Verfügung stehen, lässt sich mit Erving Goffman weiter vertiefen, der hierzu ein halbes Jahrhundert nach Simmel einflussreiche Forschungen unternommen hat. Auch Goffman geht davon aus, dass Akteursrollen und soziale Situationen unter nach-ständischen Bedingungen nur undeutlich bestimmt sind, insofern Interaktionserwartungen nicht länger umstandslos an soziomateriellen Zeichensystemen (Trachten, Wappen, Material und Farbgebung von Kleidung etc.) abgelesen werden können, sondern im Zuge der Interaktion selbst performativ hergestellt werden müssen. Hierzu müssen die Interaktionspartner im Vollzug der Interaktion zugleich Informationen über die Situation gewinnen und diese gemeinsam aushandeln: „When an individual enters the presence of others, they commonly seek to acquire information about him or to bring into play information about him already possessed. (…) Information about the individual helps to define the situation, enabling others to know in advance what he will expect of them and what they may expect of him. Informed in these ways, the others will know how best to act in order to call forth a desired response for him.“ (Goffman, 1973, S. 1) Sobald solche Informationen aber nicht länger situationsübergreifend verwendet werden können, droht ein Clash normativer Anforderungen, sofern die Kontexte und Rollen keine angemessene Abgrenzung voneinander mehr erfahren: „Behavior may be inconsistent, as in the case of the proverbial office tyrant who is meek before his wife, but it is not noticed if the transactions occur in dissociated contexts. Most people live more or less compartmentalized lives, shifting from one social world to another as they participate in a succession of transactions. In each world their roles are different, their relations to other participants are different, and they reveal a different facet of their personalities.“ (Shibutani, 1955, S. 567) Um die Wahrscheinlichkeit normativer Dissonanzen herabzusetzen, betreiben die Akteure folglich „audience segregation“ (Goffman, 1973, S. 137): Publika werden als Informationsempfänger kontextspezifisch voneinander abgetrennt. Informationelle Privatheit setzt also unter modernen Bedingungen voraus, dass entweder solche interaktiven Techniken der Publikumstrennung und Informationskanalisierung beherrscht werden und greifen können – oder aber funktionale Äquivalente hierfür gefunden werden.

2.2 Zur Verhältnisbestimmung von Privatheit und Digitalität

Aktuelle, auf Herausforderungen der Digitalisierung reflektierende Debatten um informationelle Privatheit (vgl. etwa Nissenbaum, 2010; Roessler, 2010) sind stark von einem solchen Verständnis der Aufrechterhaltung einer in Kontexte differenzierten sozialen und informationellen Ordnung geprägt. Unklar ist dabei allerdings, inwiefern die normativen Bezugspunkte, auf die das Konzept der Privatheit abstellt, weiterhin solche der Ermöglichung von individueller Freiheit und Selbstbestimmung der Person sind oder aber solche der Fortsetzung gesellschaftlicher Ordnungsmuster und damit verknüpfter Erwartungssicherheiten angesichts neuer technologischer Verknüpfungs- und Entdifferenzierungsmöglichkeiten.[3] Was vor der Digitalisierung einen konstitutiven Zusammenhang gebildet hat – die Ausformung der individuellen Persönlichkeit mit einer als authentisch erlebten Innerlichkeit durch das selektive Management pluraler Kommunikationsbeziehungen einerseits und die Kompensation fehlender äußerer Sicherheiten im sozialen Erwartungsgefüge durch die sozialisatorische Herausbildung von Takt, Kontextsensibilität, *impression management* und Rollenkompetenz andererseits – könnte sich unter Bedingungen der Digitalität als trügerisch erweisen, in Konflikt geraten oder sogar Züge eines Nullsummenspiels annehmen.

Beispielsweise geht Helen Nissenbaums (2010) Theorie der kontextuellen Integrität nicht davon aus, dass das Spezifikum von Privatheit in irgendwelchen individuellen Kontrollvorstellungen zu finden sei, sondern in der normativen Angemessenheit von Informationsflüssen: „a right to privacy is neither a right to secrecy nor a right to control but a right to appropriate flow of personal information." (Nissenbaum, 2010, S. 127) Privatheitsverletzungen stellten Verletzungen der informationellen Integrität eines Kontextes dar und würden gerade deshalb als solche beklagt. Wenn etwa eine im Sportkontext verortete Fitness-App Gesundheitsdaten sammelt und an Krankenkassen weitergibt, die dann auf Basis dieser Daten individuelle Beitragssätze kalkuliert, erscheint dies aufgrund der „violation

[3] Solche Entdifferenzierungen können auf Kurzschlüsse unterschiedlicher Funktionssystemkodierungen basieren (Pohle, 2016; Rost 2013), z. B. wenn der Erwerb von Flugtickets nicht nur an Zahlungsfähigkeit, sondern auch an politisches Wohlverhalten geknüpft ist, wie es im chinesischen *Social-Credit-System* der Fall zu sein scheint (vgl. Dölker, 2020). Entdifferenzierungen können aber auch an Akteursrollen ansetzen, etwa wenn das Sammeln und Verarbeiten digitaler Datenspuren zu digitalen Subjektdossiers führt, die eine Abgrenzung funktionsspezifischer Rollen untergraben oder eine vorauseilende Verhaltensanpassung bewirken (Lindemann 2015).

of contextual integrity“ (Nissenbaum, 2010, S. 150) als illegitimer Informationsfluss. Privatheit wird also von vornherein nicht an das Individuum, sondern an kollektiv gültige „context-relative informational norms“ (Nissenbaum, 2010, S. 140) gebunden, die festlegen sollen, welche Akteure in welchen Kontexten welche Informationen über welche Personen und Gegenstände auf welche Art und Weise versenden und empfangen dürfen.

Damit stellt sich allerdings die Frage, wie die nun getrennten Aspekte informationeller Privatheit – also die Begrenzung von Kommunikations- und Informationsflüssen zwischen disparaten gesellschaftlichen Teilbereichen einerseits und die Sozialisation eines differenzierungsfähigen, situationssensiblen und ichstarken bürgerschaftlichen Subjekts andererseits – unter Bedingungen der Digitalität verfolgt und sichergestellt werden können. Denn anders als bei Simmel oder Goffman scheint es nicht länger eine Interaktionsleistung wechselseitiger Situationsdeutung zu sein, einen kontextangemessenen Grad an Privatheit zu gewährleisten, sondern eher eine kollektive Organisations- oder Regulierungsleistung: Die Identifizierung des Kontextes, in dem ein soziotechnisches Informationssystem verortet ist, sowie der kontext-spezifischen informationellen Normen soll es erlauben, die Informationsflüsse einer Gesellschaft kollektiv bindend zu regulieren (Nissenbaum, 2010, S. 140 ff.). Nun war allerdings informationelle Privatheit auch in vordigitalen Gesellschaften keine rein performative Angelegenheit interagierender Subjekte, sondern immer schon mit weiteren gesellschaftlichen Instanzen verbunden, die Beschränkungen und Machtdifferentiale in die Kommunikationsverhältnisse und Informationsflüsse eingezogen haben, man denke etwa an das Briefgeheimnis, Indifferenzen durch binäre Kommunikationscodes (etwa im Zahlungsverkehr) oder Abschreckung durch das Sanktionspotenzial des Staates. Umgekehrt sind technische Vorkehrungen zur Kanalisierung und Begrenzung von Informationsflüssen aber nie ganz von den Instanziierungen durch handelnde Individuen – etwa den Gestaltungsakteuren von IT-Systemen, aber auch kreativ Nutzenden – losgelöst, die demnach wissen und zu beurteilen vermögen müssen, welche Information wann warum verschlüsselt oder gesperrt gehört.

Aus diesem Grund bleibt der Konstitutionszusammenhang von kritikfähigen Subjekten und privatheitssichernden Kontextstrukturen der Kommunikation, der auch als eine Grundbedingung lebendiger Demokratie gesehen wird (Habermas, 1992, S. 429, 449), unter Bedingungen der Digitalität weiter eine Gestaltungsherausforderung, wenngleich sich deren Verbindungslinien nicht mehr so einfach ziehen lassen. Die Verkomplizierungen von Privatheit durch Digitalität sollten nicht durch sozial- oder gesellschaftstheoretische Engführungen weggedeutet werden, indem etwa die Begrenzung von Informationsflüssen als Sache unpersönlicher Kommunikationssysteme oder Technologien dargestellt oder aber naiv an

die Verantwortung und Sensibilität handelnder Individuen appelliert wird. Vielmehr muss auch unter Bedingungen der Digitalität Verschiedenes zusammenkommen, um die Integrität von Kontexten und Personen zu schützen. Dies zu modellieren, bieten Theorien im Anschluss an die *science and technology studies* bessere Ansatzpunkte als etwa die Luhmannsche Systemtheorie oder ein struktur- und technikblinder symbolischer Interaktionismus.[4] Die Akteur-Netzwerk-Theorie (Latour, 2010) nimmt das Digitale als eigenständige Einflussgröße ernst, die in die Kommunikationsgeflechte der Gesellschaft sowie deren Privatheitsverhältnisse sowohl auf der Seite der Subjekte als auch auf der Seite der etablierten institutionellen Ordnungen mit ihren systemisch, technisch oder organisational stabilisierten Informationsschranken interveniert. Dabei trägt sie der Performativität solcher Machtdifferentiale Rechnung, die folglich aktiv hergestellt und gepflegt werden müssen und sich darum nur durch das Nachzeichnen der praktischen Verknüpfungsprozesse erforschen lassen (Latour, 2006, S. 203).

Digitalität kann ebenso Chancen wie Risiken für Privatheit in sich bergen. Um dieses Verhältnis zu durchdringen, sind genauere Kenntnisse darüber erforderlich, wie sie sich konkret situativ auf die Handlungsprogramme jener sozio-technischen Assoziationen auswirkt, in denen informationelle Privatheit als komplexes soziales Arrangement von Schranken und Freiheiten für die unterschiedlichen Beteiligten realisiert werden soll (vgl. Ochs, 2019). Dabei gilt es, digitale Technologien als maßgebliche Elemente in die Analyse einzubeziehen, die aber niemals für sich stehen, sondern ihrerseits nur durch die Verknüpfung mit weiteren Einflussgrößen –ökonomische, politische, wissenschaftliche ebenso wie alltagspraktische und spezifische Kulturen der Wertschätzung von Individualität und Einzigartigkeit – zur Wirkung gebracht werden. Im nachfolgenden dritten Abschnitt werden solche Verknüpfungsprozesse und Wirkungsketten nachzuzeichnen versucht, indem sowohl die soziodigitalen Praktiken, in denen sich heutzutage personale Subjekte formen (3.1 und zusammenführend 3.4), in Augenschein genommen werden als auch die Verbindungen des Digitalen zu Handlungsprogrammen der Ökonomie und Verhaltenswissenschaften sowie

[4] Aus der systemtheoretischen Perspektive lässt sich beispielsweise nicht entscheiden, ob von digitalen Technologien ein weitreichender Transformationsdruck auf die Kommunikationsverhältnisse ausgeht, der den gesellschaftlichen Umbrüchen durch die Erfindungen von schriftlicher Kommunikation oder Buchdruck vergleichbar ist (so etwa die Diagnose von Baecker (2007, 2018), oder aber Digitalität und funktionale Differenzierung immer schon aufeinander verwiesen haben und sich auch in Zukunft stützen können (Nassehi, 2019).

zur Genese neuer komplexer Kommunikationsinfrastrukturen (3.2 und 3.3). Hierfür – das mag irritierend wirken, ist aber nur konsequent – wird unter *Selbstbestimmung* oder *selbstbestimmtem Leben* ein *normatives Handlungsprogramm* verstanden, das sich im Zuge des soziotechnischen Wandels gesellschaftlicher Kommunikationsverhältnisse transformiert. Solche Transformationen hat dieses Programm in der Vergangenheit erfahren und wird es auch unter Bedingungen der Digitalität vollziehen – das ist unvermeidlich. Es bedeutet aber nicht, dass diese Evolution von Privatheit und Selbstbestimmung unkommentiert und unbeeinflusst bleiben muss. Vielmehr ist Privatheit in der hier zugrunde gelegten soziologischen Perspektive immer ein Gegenstand – oder issue (Marres, 2007) – politischer, d. h. umstrittener und vielstimmiger Gestaltung und Konstruktion. Hierbei ist kontingent, welche Problemdeutung sich durchsetzt und ob diese für sich beanspruchen kann, demokratisch inklusive Lösungswege zu forcieren und den normativen Sinn von Selbstbestimmung nicht zu verraten. Solchen politischen Aushandlungsprozessen kann und sollte sich die soziologische Privatheitsforschung nicht entziehen (s. Kapitel von Lamla u. a. in diesem Band), auch wenn ihre Aufgabe vorrangig in der sorgfältigen Beobachtung und Beschreibung dieser soziotechnischen Transformation liegt.

3 Problemfelder des selbstbestimmten Lebens in einer digitalen Datenökonomie

3.1 Sichtbarkeit – datafizierte Subjektivierungspraktiken

Zeitgenössische Praktiken der digitalen Vernetzung, für die insbesondere digitale Medien wie Facebook oder Instagram reichhaltiges Anschauungsmaterial liefern, unterscheiden sich von historisch früheren Ausrichtungen des Privatlebens sehr weitreichend dadurch, dass ein vergleichsweise breites Aussenden von Informationen über sich selbst zu einer wichtigen Grundlage der Bestimmung des eigenen Selbst wird. Dies ist keineswegs einfach ein disruptiver Effekt digitaler Technologien auf Privatheit, sondern beruht auf der Verstärkung älterer gesellschaftlicher Entwicklungen im Bereich privater Lebensführung, die unter Bedingungen der Digitalität erweiterte Ausdrucksmöglichkeiten finden. Zu solchen Entwicklungen gehört die aus der Romantik hervorgegangene Wertschätzung von Einzigartigkeit, Authentizität, Individualität oder auch Singularität (Luhmann, 1993; Reckwitz, 2017, S. 215; Simmel, 1995) ebenso wie das Bedürfnis nach bzw. eine gewisse Abhängigkeit von sozialer Bestätigung durch Peer

Groups (Riesman, 1958). Zwar sind Darstellungen des sozialen Status kein neues gesellschaftliches Phänomen (vgl. etwa Bourdieu, 1987; Veblen, 1958); vergleichsweise jung ist aber die Verbreitung starker Verunsicherungen des Selbstwertgefühls, die zur Suche nach Halt in sozialen Bezugsgruppen antreiben und den dort geltenden Meinungen hohen Orientierungswert verleihen.

Für dieses kulturelle Handlungsprogramm einer Selbstbestimmung, die durch die Suche nach der eigenen Besonderheit und deren soziale Bestätigung und Wertschätzung geprägt ist, bieten die digitalen Plattformen und Netzwerke geeignete Hilfs- und Ausdrucksmittel, deren Nutzung unter Rekurs auf Foucault damit auch als Selbst-Technologie bezeichnet werden kann (Foucault, 2013). Während Tagebücher, Briefe und dergleichen als Selbst-Technologien früherer Epochen gelten, sind Social Network Sites (SNS) paradigmatische Beispiele für deren zeitgenössische Ausformung (Paulitz & Carstensen, 2014). Eine zentrale Rolle spielt hierbei das Anlegen digitaler Profile im Rahmen solcher Sites. Sie ermöglichen zum einen die Demonstration der Vielfältigkeit von Interessen und Formen des Welterlebens und zum anderen eine kuratierende Zusammensetzung der verschiedenen Facetten des Selbst zu einem identifizierbaren Ganzen (Reckwitz, 2017, S. 248; Pittroff, 2017, S. 108 f.). Mit dieser Arbeit am digitalen Abbild oder Spiegel des Selbst einher geht allerdings zwangsläufig dessen Materialisierung in umfangreichen Datenspuren, deren Informationsgehalte und -wirkungen sich nicht mehr ohne Weiteres kontrollieren lassen.

Neben diesem Aspekt einer *datenintensiven Subjektivierungspraxis* ist für die Gegenwartsgesellschaft zugleich eine zunehmende *Datenabhängigkeit der Selbstbestimmung* zu konstatieren. Denn in zunehmendem Maße werden die umfangreichen digitalen Sammlungen und Auswertungen solcher Daten zum eigenen Selbst für dessen Ausformung und Orientierung wichtig. Nicht mehr nur die soziale Peer Group bietet dann den gewünschten Außenhalt des verunsicherten Selbst, sondern maßgeblich auch deren digitale Repräsentationen in Daten und Zahlen. Praktiken des Self-Tracking oder Quantified-Self, welche die Wertschätzung der eigenen Person mittels algorithmisierter Feedbackmechanismen objektivieren und pflegen, sind hierfür exemplarisch (Lupton, 2016; Mau, 2017). Das Sicherheitsproblem der Kontrolle und Verbreitung *personenbezogener Daten,* so ließe sich zuspitzen, wird zunehmend vom Problem der Orientierungsunsicherheiten und -bedarfe *datenbezogener Personen* verdrängt oder doch zumindest überlagert (Lamla & Ochs, 2019, S. 30).

Digitalität setzt damit die herkömmliche Sichtweise auf den Zusammenhang von Privatheit und Selbstbestimmung unter Druck. In dieser Sichtweise war die Herstellung von individueller Autonomie an die Verfügung über Möglichkeiten der individuellen Informationskontrolle sowie an Phasen des Rückzugs in die

Kontemplation gebunden (Roessler, 2001, S. 139; Westin, 1967, S. 31 ff.). Wenn nun aber unter zeitgenössischen Bedingungen dieser Zusammenhang aufgegeben wird, weil Autonomie nicht länger in datensparsamen Praktiken der bürgerlichen Privatheit gewonnen und geschult wird, sondern das breite Aussenden personenbezogener Informationen zum Zwecke der öffentlichen Selbstexploration und der Nutzung digitaler Feedbacktechnologien zwingend erfordert, verändert dies auch den normativen Sinn von Privatheit (Stalder, 2011). Denn ein Festhalten an klassischen Kontroll- und Rückzugstechniken der Privatheit droht nun, die Möglichkeiten der Persönlichkeitsentfaltung durch digitale Unsichtbarkeit und das Kappen potenziell wichtiger Verbindungen und Teilhabemöglichkeiten zu behindern (Stalder, 2019, S. 104). Ein moralischer Appell an datensparsames Verhalten der individuellen Nutzerinnen digitaler Technologien, wie er bis heute von den Institutionen des Datenschutzes wie selbstverständlich vorgebracht wird, findet mithin in den Subjektivierungspraktiken des digitalen Zeitalters keine robuste Verankerung mehr, sondern verweist im Grunde nur noch auf – durchaus erhebliche – Übergangsprobleme einer soziotechnischen Transformation des selbstbestimmten Lebens (Ladeur, 2015; Lamla & Ochs, 2019).[5]

Für die Lösung dieser Übergangsprobleme kann aber die individuelle Informationskontrolle und -zurückhaltung kaum das probate Mittel sein, da der strukturelle Widerspruch zum Erfordernis der digitalen Sichtbarkeit *alltagspraktisch* kaum auszubalancieren ist (Lamla & Ochs, 2019). Gleichwohl setzen sich klassische Praktiken und soziotechnische Muster der Gewährleistung von Privatheit auch unter Bedingungen der Digitalvernetzung zunächst fort. Dies beginnt etwa bei regulativen Maßnahmen zur besseren Informierung über Datenspuren und Sichtbarkeiten und setzt sich fort in Privatsphäreneinstellungen und Verschlüsselungsoptionen, die den Nutzerinnen in Kontexten sozialer Digitalvernetzung erweiterte Möglichkeiten der Informationskontrolle geben sollen (Ochs & Büttner, 2018). Aber auch kreative und subversive Informationspraktiken der Nutzerinnen selbst versuchen den Widerspruch zu überbrücken, indem sie trotz öffentlicher Sichtbarkeit durch Einflussnahme auf die Datenproduktion Grenzen der Teilhabe für unterschiedliche Publika zu installieren versuchen (Barth, 2016; Ochs & Büttner, 2018; Stalder, 2019). Viele wollen in öffentlichen digitalen

[5] Diskutiert wird der Widerspruch zwischen klassischen Privatheitskonzepten und datenintensiven Praktiken der Digitalvernetzung in der Post-Privacy-Debatte (Hagendorff, 2019; Pittroff 2018), die Privatheit unter Bedingungen der Digitalisierung als verloren aufgibt und anschließend daran fragt, wie sich die Schutzgüter der Privatheit (z. B. Schutz vor Diskriminierung) trotzdem bewahren lassen.

Räumen *sichtbar sein,* ohne für ein unbestimmtes Publikum gleichermaßen *öffentlich zugänglich zu sein* (Marwick & boyd, 2014, S. 1052). Sie nutzen dazu weniger technisch-administrativ bereitgestellte Nischen digitaler Plattformen (wie etwa private Chaträume), sondern entwickeln (oder reaktivieren in digitaler Form) Kulturtechniken der Verschleierung von Personenbezügen oder der gezielten Verunreinigung von Daten. Neben der Verfälschung von Profilbildern oder der Vermeidung von Klarnamenangaben sind dies insbesondere Praktiken sozialer Steganographie, d. h. einer kryptischen Kommunikation, deren Botschaften trotz öffentlicher Sichtbarkeit nur von einem begrenzten Adressatenkreis entdeckt und entschlüsselt werden können (boyd, 2014, S. 65). Systematisch erweitert werden solche Verschleierungstaktiken durch digitale Techniken der *Obfuscation.* Damit sind Praktiken bezeichnet, die unter Zuhilfenahme von Anwendungen wie *TrackMeNot* oder durch bewusste Eingabe von Falschinformationen auf eine Produktion irreführender und mehrdeutiger Daten setzen. Diese technisch orientierte und primär gegen die organisierte Sammlung und Auswertung verhaltens- und personenbezogener Daten gerichtete Obfuscation sei „generally useful in relation to a specific type of threat, shaped by necessary visibility" (Brunton & Nissenbaum, 2015, S. 85, Hervorh. i. Orig.).

Diese verschiedenen Praktiken und Techniken der Herstellung von Privatheit unter Bedingungen digitalvernetzer Subjektivierung und Selbstbestimmung stellen Kompromisse dar, die den Widerspruch zwischen Zurückhaltung und Entäußerung nicht auflösen können. Sie weisen allesamt Probleme im Umgang mit den konträren Imperativen auf, die auf das Handlungsprogramm der Selbstbestimmung im Zuge seiner soziotechnischen Transformation einwirken. So bürden sie die Kompromissfindung weiterhin isolierten Individuen auf, die ihre digitalen Erfahrungsmöglichkeiten selbst limitieren müssen und nicht länger ohne Reue den Versprechen digitaler Sichtbarkeit nachgehen dürfen. Damit überlasten sie die digitale Alltagspraxis aber nicht nur mit widersprüchlichen Selbstbestimmungszumutungen. Vielmehr überfordern sie diese auch, weil die datenökonomischen Interventions- und Überwachungsmöglichkeiten, die großen Organisationen durch Big Data und Künstliche Intelligenz zur Verfügung stehen, von einzelnen nicht überblickt und damit kaum durch kulturelle Verschleierungstechniken oder technische Obfuscation adressiert werden können. Letztere könne der Rechenmacht der Datenökonomie nicht annähernd beikommen (Richards & Hartzog, 2017, S. 1204). Womöglich wird mit dem Festhalten an bestimmten Idealen und Praktiken der Privatheit digitale Informationskontrollmacht nur noch simuliert, wo diese gegenüber den Infrastrukturanbietern längst verloren ist.

Daher stellt sich die Frage, ob und ggf. wie die mit Privatheit assoziierte Selbstbestimmungsidee auch unabhängig von individueller Informationskontrolle und trotz prämierter Sichtbarkeit gewährleistet werden kann.

3.2 Digitalität als Treiber des Wandels in sozialen Infrastrukturen der Privatheit

Neue Medien verändern die gesellschaftlichen Kommunikationsverhältnisse, in denen Privatheit einerseits technisch-materiell durch Beschränkung und Ermöglichung von Informationsflüssen und -teilhabe figuriert, andererseits aber auch durch medial vollzogene, kulturelle Praktiken performativ ausgeformt wird (z. B. durch Praktizierung von Kontextsensibilität, Dramaturgie von Selbstdarstellungen oder erworbene Taktiken und Erfahrungen). Es ist kaum zu leugnen, dass die Erfindung der Schrift und private Briefwechsel, neue Aufzeichnungsapparaturen, die räumliche Interaktionsdichte bei Hofe oder Architekturen asymmetrischer Verhaltensüberwachung (Benthams Panopticon) mit den Bedingungen der Herstellung von Privatheit auch das jeweilige Handlungsprogramm der Selbstbestimmung affizieren und verändern. Es ist daher wenig überraschend, dass solche Transformationseffekte auch mit der Digitalität als neuem soziotechnischem Element der Infrastrukturen gesellschaftlicher Kommunikation einhergehen. Unklar ist hingegen zunächst, welcher Art und welchen Ausmaßes diese Effekte genau sind.

Dazu muss näher in den Blick genommen werden, wie sich Digitalität in den technisch-materiellen und sozial-kommunikativen Infrastrukturen der Privatheit einnistet und ausbreitet. So ist das Neue dieser medialen Infrastruktur schon deshalb nicht leicht zu sehen, weil sich viele ältere Kommunikationstechniken darin fortsetzen: Briefverkehr und Freundschaftspflege, aber auch mündliche Kommunikation und Telefonie, Nachrichtenticker und Werbung sowie Radio, Fernsehen und Fotografie etwa. Das spezifisch Neue der Digitalität liegt demgegenüber zunächst in der Fähigkeit zur Vernetzung und Übersetzung unterschiedlichster Elemente gesellschaftlicher Kommunikation in ein einziges und höchst einfaches Medium maschinenlesbaren Codes. Das ist nur auf der Grundlage enormer infrastruktureller Rechenkapazitäten und -leistungen von Computern und Computernetzwerken möglich, in denen Techniken algorithmischer Datenverarbeitung zum Einsatz kommen. Mit der umfassenden Transformation von Informationen in Daten, die dann in ein einziges, scheinbar grenzenloses soziotechnisches Kommunikationsnetz integriert werden können, geht eine enorme Sogwirkung seitens der Digitalität auf sämtliche Bereiche des gesellschaftlichen Lebens einher: Latent versprechen digitale Infrastrukturen

die Verschmelzung der gesamten Gesellschaft mit einer allumfassenden kybernetischen Kommunikationsapparatur (Lanier, 2014, S. 42).

Nicht nur die gewohnten Praktiken der Privatheit geraten damit unter Transformationsdruck, vielmehr muss Privatheit mit der massiven gesellschaftlichen Expansion digitaler Infrastrukturen als Element von Digitalität neu hergestellt, d. h. aktiv und kreativ re-konstruiert werden. Das ist aber unter den besonderen technisch-medialen Bedingungen der Digitalität etwas gänzlich anderes als das analoge Zurückhalten von Geheimnissen oder physische Zurückziehen hinter Schutzmauern und geschlossene Türen. Denn die Form digitaler Daten und deren Speicherung und Zirkulation in umfangreichen Computernetzen schaffen gänzlich neue Voraussetzungen für das Etablieren und Kontrollieren von Beschränkungen des Informationsflusses – und damit auch für eine Kultur des Takts, für Vergessen, *audience segregation* oder andere privatheitsrelevante Kommunikationsmuster. Hier stellen sich nicht nur Fragen nach den technischen Möglichkeiten von privatheitsfreundlichen Infrastrukturen im Medium des Digitalen; vielmehr ist auch ganz entscheidend, wer über die mit der Einrichtung soziodigitaler Infrastrukturen verbundene Definitions- und Gestaltungsmacht hinsichtlich des Verhältnisses von Privatheit, Selbstbestimmung und Digitalität verfügt. Wie lässt sich das Handlungsprogramm eines selbstbestimmten Lebens unter Bedingungen erneuern, unter denen vom gesamten Leben eine digitale Spur oder digitale Repräsentation existiert? Was folgt daraus für die soziale Aushandlung, Beteiligung und Gestaltung im Zuge der Entwicklung von Kommunikationsinfrastrukturen? Und kann der Sinn von Privatheit und Selbstbestimmung überhaupt verlustfrei im Rahmen einer allumfassenden kybernetischen Informationsinfrastruktur eingeholt werden?

Diese Fragen stellen sich in allen Bereichen fortschreitender Digitalität, sei es bei der Transformation der Ökonomie durch digitale Plattformen, Digitalisierung der Arbeit und Industrie 4.0, bei der Pflege von Sozialbeziehungen und öffentlichen Kommunikation mittels Social Media Anwendungen wie Facebook, Instagram, WhatsApp oder Twitter oder bei der Durchdringung des Alltags mit Sprachassistenten, Robotik und smarten Endgeräten aller Art. Die emergierenden soziodigitalen Infrastrukturen verändern die gesellschaftliche Kommunikation und die individuelle Lebensführung so massiv, dass Privatheit und Selbstbestimmung davon grundlegend beeinflusst werden.[6] Dies zeigt sich exemplarisch an den infrastrukturellen Möglichkeiten

[6] Siehe dazu auch das Kapitel von Conrad u. a. in diesem Band, in dem Herausforderungen der Privatheit vor dem Hintergrund aktueller Digitaltechnologieentwicklungen thematisiert werden.

kontinuierlicher Verhaltensüberwachung und intelligenter Feedback-Schleifen, die Mensch und Maschine in Echtzeit verkoppeln. In immer mehr Verhaltensbereichen, vom Schlafen und Musikhören über das Suchverhalten und Einkaufen bis hin zum Autofahren und der körperlichen Bewegung erhält eine adaptive digitale Zwischenschicht in die Strukturen des Alltagslebens Einzug. Diese künstlich intelligenten Infrastrukturen zielen darauf ab, aufgezeichnete Verhaltensäußerungen und -muster als Trainingsdaten zu nutzen, um darüber die eigenen Algorithmen effizienter und lernfähiger zu machen (Engemann, 2018, S. 253 ff.; Mühlhoff, 2019b, S. 579). Zugleich werden aber auch die Erkenntnisse über die Verhaltenslenkungseffekte von infrastrukturellen Situationsrahmungen und Entscheidungsarchitekturen immer feiner, wodurch bestimmte Verhaltensäußerungen und -muster gezielter angeregt oder *genudged* (Mühlhoff, 2019a; Richard, 2011, S. 84) werden können, etwa um ausgeruhter aufzuwachen, musikalisch ermuntert zu arbeiten, ausgewählte kommerzielle Lösungen für individuelle Probleme zu erwägen, mehr Schritte zu Fuß zu laufen oder vorsichtiger und energiesparender Autozufahren. Beide Anpassungspotentiale digitaler Infrastrukturen – die des machine learnings ebenso wie die der gezielten Verhaltensbeeinflussung – erhöhen die Trefferquote und Vorhersagekraft algorithmisch verarbeiteter Verhaltensdaten, sodass es nicht schwerfällt, sich vorzustellen, dass beides zugleich stattfindet und sich wechselseitig stützt, antreibt, verstärkt und verselbstständigt (Yeung, 2017).

Mit einer solchen Verschmelzung oder Hybridisierung von Mensch und kybernetischer Informationsmaschine durch die Allgegenwart digitaler Infrastrukturen wird *Privatheit* potentiell *selbst zu einem Muster algorithmisch modellierbarer Verhaltensdaten.* Informationelle Privatheit erschöpft sich dann nicht mehr in praktischen Entscheidungen darüber, wie sehr das eigene Leben und die eigenen Erfahrungsräume den digitalen Verarbeitungsprozessen überhaupt zugänglich gemacht oder aber verborgen werden. Denn auch das ist etwas, das als Verhaltensmuster sensorisch erfasst, digital verdatet, algorithmisch verarbeitet und probabilistisch vorhergesagt werden kann. Privatheit wird dann eingelesen in die digitale Maschine und darin algorithmisch re-konstruiert und verdoppelt, teilweise aktiv von den Nutzenden unterstützt durch Festlegung von Privatsphäreeinstellungen oder Cookie-Präferenzen, teilweise aber auch durch die Übersetzung rechtlich-normativer Anforderungen in digitalen Code oder die Verwendung künstlich intelligenter Assistenten und Privacy-Nudges. Daraus folgt aber, dass die digitalen Technologien maßgeblich mitgestalten, was Privatheit eigentlich ist und wie diese erlebt wird. Digitalität erzeugt eine *neue, zweite Version von Privatheit,* deren Parameter in durchaus nicht feststehenden, sondern designten,

programmierten, adaptiven und maschinell lernenden IT-Infrastrukturen bestimmt werden, und die faktische Präsenz und empirische Akzeptanz dieser digitalen Muster der Privatheit entfalten normierende Wirkungen auf die Privatheitspraxis der Nutzenden, deren digitale „Repräsentation" sie sein wollen und sollen.

Einmal angenommen, die Feedback-Schleifen zwischen den praktischen – sei es individuellen, kollektiven oder auch rechtlich-normativen – Privatheitsdispositionen der Handelnden und deren digitaler Repräsentation in den Infrastrukturen führten durch maschinelles Lernen und Verhaltensanpassungen tatsächlich zu einer sehr weitgehenden Konvergenz: Ließe die Hybridisierung das *Programm der Selbstbestimmung* damit unberührt, weil die infrastrukturelle Stütze doch lediglich eine digitale Kopie dessen wäre, was die Menschen als Privatheit wollen, sollen oder gewohnt sind? Die Antwort lautet nein, weil es in einer solchen hybriden Welt den Verweis auf ein außerdigitales Subjekt der Selbstbestimmung gar nicht mehr geben kann und fortan das, was als Selbstbestimmung gelebt wird, immer ununterscheidbar auch auf jene Handlungsnormierungen zurückgeht, die in die digitalen Infrastrukturen algorithmisch einprogrammiert sind.[7] Der Unterschied ist dabei nicht, dass es nun ein soziotechnisch materialisiertes Privatheitsdispositiv gebe, wohingegen Privatheit vorher völlig frei von solchen infrastrukturellen Rahmungen gewesen sei. Denn wie eingangs betont wurde, sieht die Soziologie in der gesamten Geschichte der Privatheit solche Dispositive und soziomateriellen Figurationen am Werk. Entscheidend für das Neue des digitalen Wandels von Privatheit ist vielmehr, dass diese Infrastrukturen nun zum *Objekt der IT-Gestaltung* werden und somit die Frage aufwerfen, *wer auf die Verschmelzung von Digitalität und Privatheit mit welchen Mitteln und Verfügungsmöglichkeiten Zugriff hat und Einfluss nimmt.* Die Frage der Selbstbestimmung ist mithin untrennbar mit der Frage verbunden, wer die Pfade auszurichten und vorzuprägen vermag, auf denen die Verhaltensparameter der Praxis mit ihren Re-Präsentationen in den digitalen Kommunikationsnetzen bis zur Ununterscheidbarkeit konvergieren. Denn diese Pfade und Richtungen sind kontingent und können von einseitigen Interessen und Dienstbarmachungen der

[7] Mit „ja" könnten allenfalls jene antworten, die davon ausgehen, dass Gesellschaft, Privatheit und Subjektivität immer schon Teil einer großen kybernetischen Informationsmaschine waren, so dass die digitale Repräsentation und algorithmische Neuprogrammierung von Verhaltensmustern gar keine neue Qualität in die sozialen Kommunikationsverhältnisse hineintragen und diese medial verschieben können.

Technik dominiert sein.[8] Aus diesem Grunde steht auch die digitalisierte Version von Privatheit unvermeidlich vor der Herausforderung, die mit ihr verbundene Idee der Selbstbestimmung auf der Ebene ihrer soziotechnischen Parameter einzig durch demokratische Prozeduren und Beteiligung an der digitalen Infrastrukturgestaltung sicherstellen zu können. Anders ist sie gegenüber der kybernetischen Maschinerie und ihren Programmierern kaum zu retten.

3.3 Verhaltensmodellierung in Geschäftsmodellen der Datenökonomie

Die wichtigsten und treibenden Gestalter und Verwalter soziodigitaler Infrastrukturen sind heute große Privatunternehmen, deren Geschäftsmodelle maßgeblich mitbestimmen, wie Daten über das private Verhalten (einschließlich Privatheits-Verhalten) digital erhoben und verarbeitet werden sowie auf deren Träger über diverse Schnittstellen modifizierend oder stabilisierend zurückwirken.[9] Um zu verstehen, wie genau diese Geschäftsmodelle ihren normierenden Einfluss auf das hybride Handlungsprogramm der Selbstbestimmung entfalten und ausüben, müssen die Strukturprinzipien oder Funktionsweisen der Datenökonomie genauer erfasst werden: Nach welcher Logik erfolgt die ökonomische Verwertung der digital anfallenden Datenmassen, und was folgt daraus für die Praktiken der digitalen Subjektivierung und deren spezifische Ausrichtung?

Der Digitalität ist eine Expansionsdynamik grundlegend eingeschrieben, da die Transformation und Einverleibung von *content* aller Art in das kybernetische Universum binärer Rechenprozesse ihr vielleicht grundlegendstes Strukturprinzip ist. Aber insbesondere zu Beginn, als die Computer noch sehr geringe Kapazitäten hatten, brauchte es sehr selektive Zugriffe auf die Vielfalt möglicher Informationseinheiten, die zunächst über die berühmten Lochkarten oder

[8] Gerade weil die Technikgestaltung verhaltensanpassende Wirkungen entfaltet, „besitzt sie die performative Wirkkraft, genau jene Subjekte hervorzubringen, von denen sie im Hinblick auf die Fähigkeiten, Gewohnheiten und Bedürfnisse des Menschen ausgegangen ist." (Mühlhoff, 2018, S. 572) Vorstellungen von Privatheitswerten und -praktiken, die von den gestaltenden Akteuren bei der Programmierung von IT-Systemen mitgebracht werden, können mithin über den Umweg der Technikgestaltung zu harten Privatheitsnormen werden.

[9] Für eine Analyse datenökonomischer Geschäftsmodelle aus wirtschaftswissenschaftlicher Perspektive unter besonderer Berücksichtigung des Verhältnisses von Privatunternehmen und Nutzenden siehe auch das Kapitel von Hess u. a. in diesem Band.

über Tastaturen händisch einzugeben waren. An das automatisierte Erfassen und die Vorhersage komplexer Verhaltensmuster in Echtzeit war bei den hierfür auszuwählenden Datenarten und Berechnungsvorgängen nicht zu denken (Beniger, 1986). Die Entwicklung hin zur heutigen Datenökonomie, in der die massenhafte Verwertung solcher Verhaltensdaten ins Zentrum einer riesigen Industrie gerückt ist, erklärt sich daher nicht von selbst, sondern stellt eine kontingente Verlaufskurve dieser Expansionsdynamik dar, in der mehrere Faktoren zusammenkamen (Kitchin, 2014). Ab einem bestimmten Punkt übernimmt die Kapitalverwertung in diesem Prozess die Führung und drückt der Ausrichtung des Pfadverlaufs ihren Stempel auf. Zunächst aber mussten die dafür geeigneten datenökonomischen Geschäftsmodelle gefunden werden.

Der kulturelle Trend zur Herstellung von Sichtbarkeit und zur steigenden Abhängigkeit der Persönlichkeitsentfaltung von sozialem Peer-Feedback (s. Abschn. 3.1) kommt einer digitalen Infrastrukturentwicklung, die eine mimetische Verdopplung der Welt verspricht und mit dieser zu einem neuen soziotechnischen Hybrid verschmilzt (s. Abschn. 3.2) ohne Frage entgegen. Die enormen Überschüsse an Verhaltensdaten, die damit generiert und digital verarbeitet werden können, sind aber erst nach und nach zum primären Rohstoff einer ausgreifenden Datenökonomie geworden, die mit dieser Entdeckung auch ein Programm zur systematischen Erschließung dieser neuen Wertquelle aufzulegen beginnt (und so den strukturellen Widerspruch zwischen Sichtbarkeit und Privatheit weiter anheizt). Ein Momentum dieses Programms ist die kapitalistische Landnahme von unerschlossenen Gebieten potenzieller digitaler Verhaltensüberwachung, -vorhersage und -steuerung mittels smarter Technologien und Künstlicher Intelligenz. Diesen Landnahmeprozess hat Shoshana Zuboff vgl. insbesondere Zuboff, 2019, S. 85–121) in ihrem monumentalen Werk zur Datenökonomie nachgezeichnet: Am prototypischen Beispiel von Google zeigt sie auf, dass es sich bei den lukrativen Verhaltensdaten zunächst um Nebenprodukte und Metadaten handelt, die bei der Nutzung des digitalen Suchdienstes angefallen sind. Zu Beginn der Unternehmensgeschichte wurden diese noch zur Verbesserung der Trefferquoten des Suchalgorithmus verwendet. Als profitabel erwiesen sie sich jedoch erst, als die Möglichkeit erkannt wurde, mithilfe dieser Daten präzise Vorhersagen über zukünftiges Verhalten abzuleiten, die sich an Dritte, d. h. an die eigentlichen „Kunden“ datenökonomischer Unternehmen, verkaufen ließen (Zuboff, 2019, S. 70 f., 94). So besteht ein Versprechen ökonomischer Verhaltensvorhersagen darin, personalisierte Werbung genau dann präsentieren zu können, wenn eine hohe Wahrscheinlichkeit besteht, dass Personen tatsächlich aufgrund von

Werbeanzeigen ihr Verhalten ändern (Zuboff, 2019, S. 77 f.). So erreicht „kaum ein anderes Marketinginstrument als die von Google bzw. Facebook gesteuerte Werbung (...) nahezu die gesamte Weltbevölkerung *und* kann den (per Datenanalyse vermuteten) individuellen Wünschen und Bedürfnissen angepasst werden." (Mühlhäuser, 2019, S. 76, Hervorh. i. Orig.)

Mit der ökonomischen Profitabilität solcher Vorhersageprodukte rückt die Produktion von datenförmig verwertbaren Verhaltensüberschüssen zunehmend ins Zentrum digitaler Geschäftsmodelle und -praktiken, wobei das Verhalten damit selbst zweitrangig und zunehmend für andere Zwecke instrumentalisiert wird. So können das Akquirieren von Freundschaften, das Auswählen von Produkten, das Streamen von Musik, körperliche Erregungszustände oder die alltäglichen Bewegungen durch die smarte Stadt, letztlich alles, was statistisch signifikante Verhaltensmuster offenbaren kann, durch Schaffung geeigneter digitaler Plattformen gezielt evoziert und für datenökonomische Unternehmungen erschlossen werden. Dabei greifen dann bestimmte Strukturbedingungen und Mechanismen, die in das Privatleben eingreifen, dieses nicht unerheblich umformen und dabei auch Privatheitsvorstellungen und -erwartungen tangieren. Neben einer hohen Zahl von Nutzerinnen und den sich daraus ergebenden Netzwerk- und Lock-in Effekten, die einen Wechsel zu anderen Anbietern schwierig machen und zu Monopolbildungen auf den Märkten beitragen, benötigen Unternehmen mit der Durchsetzung dieser Geschäftslogik nämlich die möglichst umfassende datenförmige Erfass- und Verarbeitbarkeit von privaten und sozialen Lebensvollzügen, um ökonomisch gegenüber den dominanten Playern mithalten zu können (Schneider, 2019, S. 144 f.; Parker & Marshall, 2017, S. 33). Die resultierenden *Privatheitsrisiken* betreffen hierbei keineswegs nur die missbräuchliche Verwendung personenbezogener Daten. Denn sobald *Verhaltensvorhersagen* die wesentliche Grundlage des Geschäftsmodellerfolgs darstellen, kann auch das Potential zur Beeinflussung von Verhalten durch Nudging und andere soziodigitale Feedbackstrukturen zur zentralen wertschöpfenden Technologie werden, die auf eine zunehmende Hybridisierung von menschlichen und digital-algorithmischen Verhaltensparametern hinauslaufen. In diesem Sinne sind Unternehmen, die sich dem datenökonomischen Extraktionsimperativ verschreiben, auf eine Verankerung und Ausweitung datenbasierter Subjektivierung zunehmend angewiesen (Günter Voß, 2020). Offen bleibt damit nur noch die Frage, welche Konsequenzen die infrastrukturelle Verankerung dieser ökonomischen Imperative durch Unternehmen der Datenindustrie für das moderne Handlungsprogramm der Selbstbestimmung zeitigt.

3.4 Resultierende Paradoxien digitaler Selbstbestimmung

Datenintensive Subjektivierung wird im Rahmen der beschriebenen Konstellationen mit dem Ziel angereizt, einen „Verhaltensüberschuss“ zu generieren und so möglichst gut steuerbares Userverhalten zu erzielen. Die daraus gewonnenen Daten werden in erster Linie nicht zur Verbesserung von Produkten oder Dienstleistungen genutzt, sondern sind Bestandteil eines Vermarktungsapparats. Sie werden somit als mehrwertgenerierende Ressource betrachtet, was schließlich in einen Imperativ des Datensammelns umschlägt (Christl, 2017; Zuboff, 2019). Um Verhaltensdaten erzeugen zu können, muss es Datenökonomien allerdings zunächst gelingen, soziale und kulturelle Prozesse in die eigenen digitalen Infrastrukturen hineinzuziehen und entsprechende Anreizsysteme zu schaffen. Datenökonomische Strukturen docken hierfür an jene soziokulturellen Dispositionen an, die für die Datenproduktion förderlich sind und locken so Nutzerinnen in ihre Netzwerke (Ochs & Büttner, 2019; Ochs et al., 2020).

Ein paradigmatisches Beispiel hierfür liefern Self-Tracking-Apps aus dem Bereich der Health- und Fitnessplattformen. Sie stellen den Nutzerinnen der Plattformen in erster Linie eine Infrastruktur zur Formung datenbasierter Subjektivität bereit. Die mobilen Anwendungen auf dem Smartphone spiegeln das eigene Gesundheitsverhalten in Form aggregierter und modifizierter Daten an die Nutzerinnen zurück und wollen diesen so ermöglichen, auf ihr eigenes Gesundheitsverhalten gezielt einzuwirken, etwa durch Änderung des Lebensstils oder die Nutzung passgenauer Trainingspläne (Lanzing, 2016, S. 10, Mau, 2017, S. 167 ff.). Sie nehmen damit auf das moderne Handlungsprogramm der Selbstbestimmung direkt Bezug, dass allerdings die Nutzung digitaler Datendienste und die Bereitschaft zur Ko-Produktion erforderlicher Datensätze und -schätze nunmehr voraussetzt. Hierbei stellt sich allerdings das Problem ein, dass somit auch das moderne Selbstbestimmungsideal instrumentalisiert und zu einem Mittel wird, Targeting-Objekte für die Werbeindustrie zu erzeugen. Wenn sich in das Handlungsprogramm der Selbstbestimmung über die Verhaltensrelevanz digitaler Daten ökonomische Konzerninteressen mischen, wird „die vordergründig versprochene *selbstbestimmte* Selbst-Bestimmung (...) zur *fremdbestimmten* Bestimmung des Selbst“ (Ochs & Büttner, 2019, S. 210). Die resultierenden Kapazitäten zur Verhaltenssteuerung werden gezielt dafür eingesetzt, die Profitabilität am Markt zu erhöhen. Datenbasierte Selbstbestimmung wird zum bevorzugten und vielversprechenden Zielobjekt all jener Geschäftsmodelle, die unter dem ökonomischen Regime des Überwachungskapitalismus das Potenzial digitaler Infrastrukturen zur Verhaltensformung zu erschließen und einzusetzen trachten.

Damit wird die diagnostizierte Verschmelzung von Privatheit und Digitalität vermittelt über die Gestaltungsmacht datenökonomischer Konzerne an kommerziellen Zwecken ausgerichtet und geraten hergebrachte Vorstellungen von Selbstbestimmung in einem doppelten Sinne unter Druck: Nicht nur wird das Festhalten an einem Konzept von Privatheit fraglich, das die Verantwortung für das Ausbalancieren der ökonomisch induzierten oder gesteigerten Paradoxien datenbasierter Selbstbestimmung in erheblichem Maße beim individuellen Rechtssubjekt verankert sieht; vielmehr wird zugleich die politische Frage aufgeworfen, wie lange diese ökonomische Rahmung und Übersetzung eines mit Privatheit verbundenen Selbstbestimmungsprogramms mit den Normen und Konventionen kollektiver Selbstgesetzgebung in einem demokratischen Gemeinwesen noch vereinbar sind. Denn während aktuell noch an regulatorischen Konzepten informationeller Selbstbestimmung festgehalten wird, die die einzelne Nutzerin adressieren, obgleich beispielsweise ein *Informed Consent* weitere Mitsprache jenseits einer – häufig binären – Eingangswahl weitgehend auszuschalten gestattet, zeigt sich die erheblich folgenreichere Entscheidungsgewalt auf der Ebene jener Gestaltungsakteure, die über das Potenzial digitaler Infrastrukturen zur Verhaltensbeeinflussung und Handlungsnormierung verfügen. Folglich bleibt das Recht auf individuelle Selbstbestimmung halt- und kraftlos, wenn es nicht durch ein Recht auf kollektive Selbstbestimmung abgesichert und gestützt wird, wie es sich in der Idee demokratisch verfasster Gemeinwesen ausdrückt, die wiederum auf kritisch kompetente Bürgerinnen angewiesen bleiben (Habermas, 1992, S. 491).[10] Um diesem Konstitutionszusammenhang auch in Zeiten Geltungskraft zu erhalten oder zu verleihen, in denen digitale Infrastrukturen das selbstbestimmte Leben prägen und formen, wird die Verfügung über datenökonomische Gestaltungsmacht, deren rechtsstaatliche Kontrolle und zivilgesellschaftliche Verankerung, zu einer demokratischen Schlüsselfrage.

4 Fazit: Soziodigitale Privatheit demokratisch gestalten!

In Deutschland und Europa gibt es das breite Bekenntnis, verhindern zu wollen, dass demokratische Selbstbestimmung, demokratische Grundrechte und demokratische Werte und Ordnungsprinzipien durch digitale Überwachung ausgehöhlt werden. Zur Rhetorik dieses Bekenntnisses gehört auf der einen Seite die Abgrenzung gegen-

[10] Siehe dazu auch das Kapitel von Heesen u. a. in diesem Band, das auf die Bedeutung von Privatheit und informationeller Selbstbestimmung für die Absicherung individueller Freiheit und demokratischer Teilhabe fokussiert.

über dem Digitalisierungspfad der USA, wo die Gestaltungsmacht über soziodigitale Infrastrukturen in den Händen weniger privater IT-Konzerne konzentriert ist, die das Geschäftsmodell digitaler Verhaltensbeobachtung und -führung zur Blüte gebracht haben. Auf der anderen Seite wird ebenso kritisch auf autoritäre Regime verwiesen, die diese Gestaltungsmacht unter staatliche Kontrolle bringen und die behavioralen Lenkungseffekte soziodigitaler Infrastrukturen und Überwachungstechniken wie beim chinesischen *Social-Credit*-System an eigenen normativen Standards ausrichten und *top down* diktieren. Beide Entwicklungspfade der Digitalität – verstanden als neue, transformierende Schicht, die in die gesellschaftlichen Kommunikationsverhältnisse Einzug erhält und mit diesen zur ununterscheidbaren Soziodigitalität verschmilzt – gelten hierzulande als privatheitsfeindlich und widersprechen den normativen Prinzipien der Selbstbestimmung, wie sie in der europäischen Tradition angelegt und verstanden werden und die Entfaltung des demokratischen Gedankens maßgeblich geprägt haben (Dijck et al., 2018).

Doch bei all diesem Bekenntnis bleibt unklar, wie eine alternative demokratische Ausgestaltung der soziodigitalen Privatheit eigentlich aussehen müsste und ob der eingeschlagene Pfad europäischer Datenschutzpolitik hierfür geeignete Antworten parat hält. Denn die demokratische Rhetorik kann sich in eine problematische Legitimationsfassade verwandeln, wenn der dritte Weg digitaler Verhaltens- und Privatheitsnormierung seinerseits bloß rechtsgültige Auslegungen der informationellen Selbstbestimmung top down als Parameter einer Infrastrukturgestaltung zu implementieren trachtet, die ansonsten ganz in der Hand privatökonomischer Initiative verbleibt. Denn die eingezogenen Schranken der Verbreitung und Nutzung personenbezogener Daten durch Prinzipien der Datensparsamkeit oder des *Privacy by Designs* könnten sich als – durchaus nicht unwichtige, aber – schwache Elemente einer Infrastruktur erweisen, deren Ausrichtung im Ganzen darauf hinausläuft, der gesellschaftlichen Kommunikation und individuellen Lebensführung ein digitales Skelett einzuziehen, das nach Eingewöhnung als neue, dritte[11] Natur erscheint. Eine digital ausgerichtete Privatheit kann immer noch Teil einseitig kontrollierter datenökonomischer Verhaltensprogramme sein und verhindert solche Machtasymmetrien nicht zwingend. Es gilt etwa in Rechnung zu stellen, dass das digital konfigurierte Privatheitsverhalten, welches sich in der sorgsamen Limitierung von Browser-Cookies, der Einschränkung von Sichtbarkeit oder der Verschlüsselung von Mitteilungen manifestiert, irgendwann nur noch der „Simulation“ (Blühdorn, 2013) eines

[11] „Dritte Natur“ deshalb, weil die Gewöhnlichkeit gesellschaftlicher Lebensverhältnisse, die keineswegs naturgegeben, sondern historisch gewachsen sind, vielfach als „zweite Natur“ bezeichnet werden (vgl. etwa Menke, 2012).

selbstbestimmten Lebens dienen könnte, wodurch die gesellschaftliche Transformation in ein postdemokratisches Regime asymmetrischer Verhaltensüberwachung zwar milder erschiene, dessen Akzeptanz aber gesteigert würde.[12] Privatheitsfreundliche Digitalität könnte sich somit als perfides Mittel erweisen, den Kontrollprogrammen neuer und alter Ordnungsmächte die erforderliche Massenloyalität zu verschaffen und Verhaltenskonformität abzusichern.

Soll ein solcher postdemokratischer Transformationspfad in die neue, soziodigitale Lebenswirklichkeit verhindert oder im Namen der Selbstbestimmung zumindest ernsthaft bekämpft werden, sind weitere demokratische Selbstbestimmungsprinzipien in der soziodigitalen Infrastrukturgestaltung zu verankern. Anstelle einer restriktiven Privatheitskultur wäre – auch vor dem Hintergrund des langen Zivilisationsprozesses, der mit der Geschichte von Privatheit verbunden ist – an die Schaffung und Absicherung einer Vertrauenskultur zu denken, die maßgeblich all jene adressiert, die mit sensiblen Daten hantieren und daraus digitale Verhaltensrepräsentationen und -feedbacks formen (Ari Ezra Waldman, 2018; Richards & Hartzog, 2017; Uhlmann, 2020). Angesichts der Wirkmacht datenökonomischer Imperative ist allerdings nicht anzunehmen, dass sich eine Beschränkung der mit massenhaften Verhaltensdaten verfügbaren Gestaltungsmacht von selbst etabliert. Es braucht dafür schon Gegenkontrollmacht und -mechanismen[13] sowie insbesondere auch einen ehrlichen öffentlichen Streit

[12] So verweisen die oben aufgeführten Beispiele, die auch unter dem Stichwort „Selbstdatenschutz“ diskutiert werden können, vielfach auf eine Illusion von Privatheit und Kontrolle. Wenn Nutzende etwa gerade durch die Anwendung von individuellen Privatheitseinstellungen dazu gebracht werden, mehr Informationen mit datenökonomischen Plattformen zu teilen, dann werden die Nebeneffekte von etablierten Konzepten privatheitsfreundlicher Digitalität offenbar. Für eine Auseinandersetzung mit den Grenzen und Herausforderungen von Selbstdatenschutz aus psychologischer Perspektive siehe auch das Kapitel von Meier u. a. in diesem Band.

[13] Hierzu gehörten etwa angemessene regulative Datenschutznormen, die nicht von Internetunternehmen zu ihren Vorteilen umgedeutet werden können (Clifford et al., 2018; Ladeur, 2015); eine Stärkung von Intermediären wie Datenschutzbehörden oder Verbraucherschutzorganisationen, die unabhängige Kontrollen von unternehmensinternen Risikopräventionsmaßnahmen durchführen, wirksame Zertifikate für vertrauenswürdige Organisationen vergeben und die Öffentlichkeit über Normverstöße in Kenntnis setzen (Mantelero, 2016; Maria Eduarda Gonçalves, 2017); die Entwicklung professionsethischer Selbstverpflichtungen für Personen, die für organisationale Datennutzungspraktiken zuständig sind (Balkin, 2016, Waldman, 2018, S. 88 ff.); ein stärkerer Fokus auf die Regulierung der konkreten Verwendungsweisen von Daten (Mayer-Schönberger & Ramge, 2017, S. 204 f., Mantelero, 2014, Veil, 2018, S. 696) und vieles mehr. Für Vorschläge zur problemangemessenen Fortentwicklung des Datenschutzes siehe auch die Kapitel von Roßnagel u. a. sowie von Hansen u. a. in diesem Band.

über das gesamte normative Gerüst der neuen soziodigitalen Kommunikationsverhältnisse. Eine Konzentration allein auf Privatheit droht den Gehalt von Selbstbestimmungsnormen nicht mehr wirklich ernst zu nehmen und stattdessen allein auf Sicherheit, Stabilität und liberale Ordnung zu setzen. Demokratische Selbstbestimmung ermöglichen die verschiedenen rechtlich-institutionellen Elemente und intermediären Stützen einer soziodigitalen Vertrauenskultur sowie öffentlichen Problematisierungen soziodigitaler Normativität erst dann, wenn sie eine *zentrale Kompetenz individueller ebenso wie kollektiver Selbstbestimmung* nicht unterminieren, sondern stärken, nämlich die *Fähigkeit zur Kritik der normierenden Gehalte und Effekte soziodigitaler Infrastrukturen.* Denn auch Kritik ist nicht unabhängig von soziotechnischen Verhaltenskonfigurationen. Sie kann aber – verglichen mit formal-rechtlicher Privatheit – einen robusteren Widerstand gegen die Tendenzen und ökonomischen Imperative verankern, die auf eine digitale Fremdprogrammierung des Lebens hinauslaufen. Sie ist daher auch unter soziodigitalen Bedingungen der entscheidende Schlüssel für ein selbstbestimmtes Leben.

Die oft angemahnte *Transparenz* von verhaltensnormierenden Algorithmen (Kilovaty, 2019, S. 492), ohne die sich ihre diskriminierenden Effekte gewiss kaum identifizieren ließen, kann hierfür allerdings nur eine notwendige, keine hinreichende Bedingung liefern. Denn sie setzt die Kompetenz zur Kritik bereits voraus, deren Reproduktion unter soziodigitalen Lebensbedingungen jedoch nicht mehr unabhängig von den algorithmischen Rahmungen des Verhaltens gegeben und gesichert ist. Folglich ist es erforderlich, Kritikabilität und Kritikfähigkeit nicht in einem imaginativen Außen der Digitalität zu verorten, etwa in der reinen Innerlichkeit des Privatsubjekts oder der Unparteilichkeit einer technikneutralen Rechtsordnung, sondern als Element der ganz und gar unreinen soziodigitalen Hybridität selbst zu verankern, etwa durch ein „design of our supposedly smart architectures […] based on *agonistic debate, built-in falsifiability and a robust constructive distrust.* This should result in testable and contestable decision systems" (Hildebrandt, 2019, S. 107, Hervorh. i. Orig.; vgl. ebenso Lamla, 2019, S. 54). Wohl hat der öffentliche Diskurs ein gewisses Problembewusstsein für mögliche manipulative Praktiken auf und mittels Plattformen erzeugt und die betreibenden Unternehmen zu korrigierenden Eingriffen gezwungen (Dolata, 2020). Mit der Einrichtung von Kontrollgremien (z. B. Facebooks Oversight Board) und freiwilligen Transparenzmaßnahmen wehren diese die Herausforderungen jedoch nur oberflächlich ab (Burkell & Regan, 2019). Um Kritikfähigkeit in soziodigitalen Umgebungen zu erhalten und systematisch zu fördern, braucht es ein genaueres Verständnis für die *Reproduktionsbedingungen* dieser Kompetenzen: Diese sind auf das Einüben von Urteilsfähigkeit in praktischen

Situationen angewiesen, in denen eindeutige Urteilsalgorithmen nicht zur Verfügung stehen, wie es die ubiquitäre Digitalität fälschlich suggeriert, sondern aus einer Pluralität von Konventionen und Rechtfertigungsordnungen heraus praktisch entschieden und begründet werden muss, was richtig ist und was falsch, was gut ist und was schlecht (Boltanski & Thévenot, 2007). Dazu braucht es aber nicht nur den Zugang zu den Konventionen, d. h. die Sichtbarkeit jener impliziten normativen Ordnungen, mit denen Informationen in soziodigitalen Kommunikationsnetzen erzeugt, prozessiert und bewertet werden (Diaz-Bone, 2019), sondern auch ein öffentliches Bewusstsein von deren Kontingenz, die reflektierende Exploration von Alternativen sowie einen demokratischen Zugriff auf ihre infrastrukturelle Ausgestaltung. Nur wenn die Kommunikationsinfrastrukturen effektiv gewährleisten, dass der Faden zur kritischen Praxis nicht reißt, die die (algorithmischen) Urteilsroutinen immer wieder mit den Unbestimmtheiten und Konflikten des sozialen Lebens konfrontiert und mit einer Pluralität an normativen Registern der Rechtfertigung begründend zu vermitteln sucht, kann Privatheit unter soziodigitalen Bedingungen ein Ort der Selbstbestimmung bleiben.

Literatur

Arendt, H. (2010). *Vita activa oder vom tätigen Leben.* Piper.

Baecker, D. (2007). *Studien zur nächsten Gesellschaft.* Suhrkamp.

Baecker, D. (2018). *4.0 oder Die Lücke die der Rechner lässt.* Merve Verlag.

Balkin, J. M. (2016). „Information Fiduciaries and the First Amendment". *UC Davis Law Review, 49*(4), 1183–1234.

Barth, N. (2016). „Kalte Vertrautheiten. Private Kommunikation auf der Social Network Site Facebook". *Berliner Journal für Soziologie, 25*(4), 459–489.

Beniger, J. (1986). *The control revolution: Technological and economic origins of the information society.* Harvard University Press.

Blühdorn, I. (2013). *Simulative Demokratie. Neue Politik nach der postdemokratischen Wende.* Suhrkamp.

Boltanski, L., & Thévenot, L. (2007). *Über die Rechtfertigung. Eine Soziologie der kritischen Urteilskraft*. Hamburger Edition.

Bourdieu, P. (1987). *Die feinen Unterschiede. Kritik der gesellschaftlichen Urteilskraft.* Suhrkamp.

boyd, d. (2014). *It's complicated. The social lives of networked teens.* Yale University Press.

Brunton, F., & Nissenbaum, H. (2015). *Obfuscation.* MIT Press.

Burkell, J., & Regan, P. M. (2019). „Voter preferences, voter manipulation, voter analytics: Policy options for less surveillance and more autonomy". *Internet Policy Review, 8*(4).

Christl, W. (2017). *Corporate surveillance in everyday life. How companies collect, combine, analyze, trade, and use data on billions.* https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf. Zugegriffen: 19. Juli 2020.

Clifford, D., & Ausloos, J. (2018). Data protection and the role of fairness. *Yearbook of European Law, 37*(1), 130–187.

Colin, Bennett. (2011). „In defence of privacy: The concept and the regime". *Surveillance & Society, 8*(4), S. 485–496.

Diaz-Bone, R. (2019). „Valuation an den Grenzen der Datenwelten". In J. Kropf & S. Laser (Hrsg.), *Digitale Bewertungspraktiken. Für eine Bewertungssoziologie des Digitalen* (S. 71–95). Springer.

Dolata, U. (2020). Plattform-Regulierung. Organisierung von Märkten und Kuratierung von Sozialität im Internet. *Berliner Journal für Soziologie, 29*(3).

Dölker, L. (2020). *Guter Bürger, schlechter Bürger. Das „Sozialkreditsystem" in China.* Phoenix: Das ganze Bild. https://www.phoenix.de/guter-buerger-schlechter-buerger-a-930044.html. Zugegriffen: 16. Juli .2020.

Durkheim, E. 1992[1893]. *Über soziale Arbeitsteilung. Studie über die Organisation höherer Gesellschaften.* Suhrkamp.

Edward, J. (1978). *Bloustein.* Transaction Publishers.

Elias, N. (1997). *Über den Prozeß der Zivilisation. Soziogenetische und psychogenetische Untersuchungen Bd. 1.* Suhrkamp.

Engemann, C. (2018). „Rekursionen über den Körper". In C. Engemann & A. Jahn-Sudmann (Hrsg.), *Machine Learning: Medien, Infrastrukturen und Technologien der künstlichen Intelligenz* (S. 247–268). transcript.

Foucault, M. (2013). „Technologien des Selbst". In D. Defert & F. Ewald (Hrsg.), *Ästhetik der Existenz: Schriften zur Lebenskunst* (S. 287–317). Suhrkamp.

Goffman, E. (1973). *The presentation of self in everyday life.* The Overlook Press.

Gonçalves, M. E. (2017). „The EU data protection reform and the challenges of big data: Remaining uncertainties and ways forward". *Information & Communications Technology Law, 26*(2), 1–26.

Günter Voß, G. (2020). *Der arbeitende Nutzer. Über den Rohstoff des Überwachungskapitalimus.* Campus.

Habermas, J. (1990). *Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft.* Suhrkamp.

Habermas, J. (1992). *Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaates.* Suhrkamp.

Hagendorff, T. (2019). „Post-privacy oder der Verlust der Informationskontrolle". In H. Behrendt et al. (Hrsg.), *Privatsphäre 4.0. Neuverortung des Privaten im Zeitalter der Digitalisierung* (S. 91–106). Springer.

Hahn, K., & Langenohl, A. (2017). „Zur Einführung: Brauchen wir ein neues Öffentlichkeitskonzept für dynamische (Medien-)Gesellschaften?" In K. Hahn & A. Langenohl (Hrsg.), *Kritische Öffentlichkeiten – Öffentlichkeiten in der Kritik* (S. 1–20). Springer VS.

Hildebrandt, M. (2019). „Privacy as protection of the icomputable self: From agnostic to agonistic machine learning". *Theoretical Inquiries in Law, 20*(1), 83–121.

Kilovaty, I. (2019). Legally cognizable manipulation. *Berekeley Technology Law Journal, 34*(2), 449–502.

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures and their consequences.* SAGE.

Ladeur, K.-H. (2015). „Die Gesellschaft der Netzwerke und ihre Wissensordnung. Big data, datenschutz und die relationale Persönlichkeit". In F. Süssenguth (Hrsg.), *Die Gesellschaft der Daten* (S. 225–251). transcript.

Lamla, J. (2019). „Selbstbestimmung und Verbraucherschutz in der Datenökonomie". *Aus Politik und Zeitgeschichte (APuZ), 69*(24–26), 49–54.

Lamla, J., & Ochs, C. (2019). „Selbstbestimmungspraktiken in der Datenökonomie: Gesellschaftlicher Widerspruch oder ‚privates' Paradox?" In B. Blättel-Mink & P. Kenning (Hrsg.), *Paradoxien des Verbraucherverhaltens* (S. 25–39). Springer.

Lanier, J. (2014). *Gadget. Warum die Zukunft uns noch braucht.* Suhrkamp.

Lanzing, M. (2016). „The transparent self". *Ethics and Information Technology, 18*(1), 9–16.

Latour, B. (2006). „Die Macht der Assoziation". In A. Belliger & D. J. Krieger (Hrsg.), *ANThology* (S. 195–212). transcript.

Latour, B. (2010). *Eine neue Soziologie für eine neue Gesellschaft. Einführung in die Akteur-Netzwerk-Theorie.* Suhrkamp.

Lindemann, G. (2015). „Die Verschränkung von Leib und Nexistenz". In F. Süssenguth (Hrsg.), *Die Gesellschaft der Daten. Über die digitale Transformation der sozialen Ordnung* (S. 41–66). transcript.

Luhmann, N. (1993). „Individuum, Individualität, Individualismus". In N. Luhmann (Hrsg.), *Gesellschaftsstruktur und Semantik* (S. 149–258). Suhrkamp.

Lupton, D. (2016). „You are your data: Self-tracking practices and concepts of data". In S. Selke (Hrsg.), *Lifelogging. Digital self-tracking and lifelogging – Between disruptive technology and cultural transformation* (S. 61–80). Springer.

Mantelero, A. (2014). „The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics". *Computer Law & Security Review, 30*(6), 643–660.

Mantelero, A. (2016). „Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection". *Computer Law & Security Review, 32*(2), 238–255.

Marres, N. (2007). „The issues deserve more credit: Pragmatist contributions to the study of public involvement in controversy". *Social Studies of Science, 37*(5), 759–780.

Marwick, A. E., & d. boyd. (2014). „Networked privacy: How teenagers negotiate context in social media". *New Media & Society, 16*(7), 1051–1067.

Mau, S. (2017). *Das metrische Wir. Über die Quantifizierung des Sozialen.* Suhrkamp.

Mayer-Schönberger, V., & Ramge, T. (2017). *Das digital. markt, Wertschöpfung und Gerechtigkeit im Datenkapitalismus.* Econ.

Menke, C. (2012). „Zweite Natur. Kritik und Affirmation". In M. Völk et al. (Hrsg.), *„... wenn die Stunde es zulässt.": zur Traditionalität und Aktualität kritischer Theorie* (S. 154–171). Westfälisches Dampfboot.

Mühlhäuser, M. (2019). „Open metadata: Nutzerzentrierte wettbewerbliche Datenverwertung mit offenen Rahmendaten". In C. Ochs et al. (Hrsg.), *Die Zukunft der Datenökonomie. Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz* (S. 71–102). Springer.

Mühlhoff, R. (2018). „Digitale Entmündigung und user experience design. Wie digitale Geräte uns nudgen, tracken und zur Unwissenheit erziehen“. *Leviathan, 46*(4), 551–574.

Mühlhoff, R. (2019a). „Big data is watching you. Digitale Entmündigung am Beispiel von Facebook und Google“. In Hrsg. R. Mühlhoff, R. Mühlhoff, A. Breljak, & J. Slaby (Hrsg.), *Affekt Macht Netz. Auf dem Weg zu einer Sozialtheorie der Digitalen Gesellschaft.* (S. 81–107). transcript.

Mühlhoff, R. (2019b). „Menschengestützte Künstliche Intelligenz. Über die sozio-technischen Voraussetzungen von deep learning“. *Zeitschrift für Medienwissenschaft, 11*(2), 56–64.

Nassehi, A. (2014). „Die Zurichtung des Privaten. Gibt es analoge Privatheit in einer digitalen Welt?“ In A. Nassehi (Hrsg.), *Kursbuch 177: Privat 2.0.* Murmann.

Nassehi, A. (2019). *Muster. Theorie der digitalen Gesellschaft.* Suhrkamp.

Nissenbaum, H. (2010). *Privacy in context. Technology, policy, and the integrity of social life.* Stanford University Press.

Ochs, C. (2019). „Teilhabebeschränkungen und Erfahrungsspielräume: Eine negative Akteur-Netzwerk-Theorie der Privatheit“. In H. Behrendt et al. (Hrsg.), *Privatsphäre 4.0. Eine Neuverortung des Privaten im Zeitalter der Digitalisierung* (S. 13–31). Springer VS.

Ochs, C., & Büttner, B. (2018). „Das internet als »Sauerstoff« und »Bedrohung«: Privatheitspraktiken zwischen analoger und digital-vernetzter Subjektivierung“. In M. Friedewald (Hrsg.), *Privatheit und selbstbestimmtes Leben in der digitalen Welt. Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes* (S. 33–80). Springer

Ochs, C., & Büttner, B. (2019). „Selbstbestimmte Selbst-Bestimmung? Wie digitale Subjektivierungspraktiken objektivierte Datensubjekte hervorbringen“. In C. Ochs et al. (Hrsg.), *Die Zukunft der Datenökonomie. Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz* (S. 181–214). Springer.

Ochs, C., Büttner, B., & Lamla, J. (2020). “Trading social visibility for economic amenability: Data-based value translation on a ‘Health- and Fitness-Platform’”. *Science, Technology & Human Values, 2*(4), 480–506.

Parker, G. G., & Marshall, W. (2017). Van Alstyne und Sangeet Paul Choudary. *Platform revolution. How networked markets are transforming the economy and how to make them work for you.* W. W. Norton.

Paulitz, T., & Carstensen, T. (2014). *Subjektivierung 2.0: Machtverhältnisse digitaler Öffentlichkeiten.* Springer.

Pittroff, F. (2017). Profile als Labore des Privaten. In I. Beiträge (Hrsg.), *Profile* (S. 101–113). Meson Press.

Pittroff, F. (2018). „Perverse Privatheiten: Die Postprivacy-Kontroverse als Labor der Transformation von Privatheit und Subjektivität“. In J. Kropf & S. Laser (Hrsg.), *Digitale Bewertungspraktiken* (S. 191–214). Springer Fachmedien.

Pohle, J. (2012). “Social networks, functional differentiation of society, and data protection”. arXiv:1206.3027, S. 1–8. https://arxiv.org/abs/1206.3027. Zugegriffen: 16. Juli 2020.

Reckwitz, A. (2017). *Die Gesellschaft der Singularitäten. Zum Strukturwandel der Moderne.* Suhrkamp.

Richards, N., & Hartzog, W. (2017). „Privacy's trust gap: A review". *Yale Law Journal, 126*(4), 1180–1224.

Riesman, D. (1958). *Die einsame Masse.* Rowohlt.

Roessler, B. (2010). „Privatheit und Autonomie. Zum individuellen und gesellschaftlichen Wert des Privaten". In S. Seubert & P. Niesen (Hrsg.), *Die Grenzen des Privaten* (S. 41–59). Nomos.

Roessler, B. (2001). *Der Wert des Privaten.* Suhrkamp.

Roessler, B., & Mokrosinska, D. (2013). „Privacy and social interaction." *Philosophy and Social Criticism, 39*(8), 771–791.

Rost, M. (2013). „Zur Soziologie des Datenschutzes". *DuD – Datenschutz und Datensicherheit, 37*(2), 85–91.

Schneider, I. (2019). „Governance der Datenökonomie – Politökonomische Verfügungsmodelle zwischen Markt, Staat, Gemeinschaft und Treuhand". In C. Ochs et al. (Hrsg.), *Die Zukunft der Datenökonomie. Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz* (S. 144–180). Springer.

Sennett, R. (2008). *Verfall und Ende des öffentlichen Lebens.* Berlin Verlag Taschenbuch.

Shibutani, T. (1955). „Reference groups as perspectives". *American Journal of Sociology, 60(6)*, 562–569.

Simmel, G. (1992). „Das Geheimnis und die geheime Gesellschaft". In O. Rammstedt (Hrsg.), *Soziologie. Untersuchungen über die Formen der Vergesellschaftung* (S. 256–304). Suhrkamp.

Simmel, G. (1995). „Die beiden Formen des Individualismus". In R. Kramme, A. Rammstedt, & O. Rammstedt (Hrsg.), *Aufsätze und Abhandlungen: 1901–1908* (S. 49–65). Suhrkamp.

Stalder, F. (2011). „Autonomy beyond privacy? A rejoinder to Bennett". *Surveillance & Society, 8*(4), 508–512.

Stalder, F. (2019). „Autonomie und Kontrolle nach dem Ende der Privatsphäre". In M. Stempfhuber & E. Wagner (Hrsg.), *Praktiken der Überwachten. Öffentlichkeit und Privatheit im Web 2.0* (S. 97–110). Springer.

Star, S. L., & Ruhleder, K. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information System Research, 1,* 111–134.

Thaler, R. H., & Sunstein, C. R. (2011). *Nudge. Wie man kluge Entscheidungen anstößt.* Econ.

Uhlmann, M. (2020). *Netzgerechte Datenschutzgestaltung: Herausforderungen, Kriterien, Alternativen*. Nomos.

van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world.* Oxford University Press.

Veblen, T. (1958[1899]). *Theorie der feinen Leute. Eine ökonomische Untersuchung der Institutionen.* Kiepenheuer & Witsch.

Veil, W. (2018). Die Datenschutz-Grundverordnung: Des Kaisers neue Kleider. *Neue Zeitschrift für Verwaltungsrecht, 10*, 686–696.

Waldman, AE. (2018). *Privacy as trust Information privacy for an information age.* Cambridge University Press.

Weintraub, J. (1997). „The theory and politics of the public/private distinction". In J. Weintraub & K. Kumar (Hrsg.), *Public and private in thought and practice: Perspectives on a grand dichotomy* (S. 1–42). The University of Chicago Press.

Westin, A. F. (1967). *Privacy and freedom.* Ig Publishing.
Yeung, K. (2017). „Hypernudge": Big data as a mode of regulation by design. *Information, Communication & Society, 20*(1), 118–136.
Zuboff, S. (2019). *The age of surveillance capitalism.* Profile Books.

Prof. Dr. Jörn Lamla ist Professor für Soziologische Theorie am Fachbereich Gesellschaftswissenschaften und Direktor am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel.

Barbara Büttner war wissenschaftliche Mitarbeiterin am Fachgebiet Soziologische Theorie der Universität Kassel.

Dr. Carsten Ochs ist wissenschaftlicher Mitarbeiter am Fachgebiet Soziologische Theorie der Universität Kassel.

Fabian Pittroff ist wissenschaftlicher Mitarbeiter am Fachgebiet Soziologische Theorie der Universität Kassel.

Dr. Markus Uhlmann ist wissenschaftlicher Mitarbeiter am Fachgebiet Soziologische Theorie der Universität Kassel.

Einwirkungen der Digitalisierung auf gesellschaftliche Inklusion und Exklusion

Privatheit, Ethik und demokratische Selbstregulierung in einer digitalen Gesellschaft

Jessica Heesen, Regina Ammicht Quinn, Andreas Baur, Thilo Hagendorff und Ingrid Stapf

1 Persönliche Lebensgestaltung und politisches Handeln

Wenn von Datenschutz und informationeller Selbstbestimmung die Rede ist, dann steht in der Regel vor allem der Bereich der privaten Lebensführung im Zentrum. Im Zusammenhang der Digitalisierung spielen hier die für moderne Informationstechniken charakteristischen individuellen Nutzungsformen – insbesondere in Form von Sozialen Medien und personalisierten Anwendungen – eine hervorgehobene Rolle. Durch diese Nutzugsweisen wird eine umfassende technische Dokumentation des individuellen Verhaltens ermöglicht. Quellen für die massenhafte Datenerhebung sind sowohl die bewusste und unbewusste Interaktion

J. Heesen (✉) · R. Ammicht Quinn · A. Baur · T. Hagendorff · I. Stapf
Internationales Zentrum für Ethik in den Wissenschaften,
Eberhard Karls Universität Tübingen, Tübingen, Deutschland
E-Mail: jessica.heesen@uni-tuebingen.de

R. Ammicht Quinn
E-Mail: regina.ammicht-quinn@uni-tuebingen.de

A. Baur
E-Mail: a.baur@uni-tuebingen.de

T. Hagendorff
E-Mail: thilo.hagendorff@uni-tuebingen.de

I. Stapf
E-Mail: ingrid.stapf@izew.uni-tuebingen.de

A. Roßnagel und M. Friedewald (Hrsg.), *Die Zukunft von Privatheit und Selbstbestimmung,* DuD-Fachbeiträge,
https://doi.org/10.1007/978-3-658-35263-9_5

mit informationstechnischen Systemen als auch die Interaktion von Mensch zu Mensch über die natürliche Sprache in Sozialen Medien, E-Mail und vielen digitalen Fernseh- oder Presseformaten.

Digitale Informationstechniken und insbesondere die Sozialen Medien ermöglichen Informationsverbreitung in zwei Richtungen: durch ihre Nutzer:innen und über ihre Nutzer:innen. Mehr und mehr können durch die Analyse und Auswertung von digitalen Plattformen Informationen über das Verhalten und die Kommunikation der einzelnen Nutzerinnen und Nutzer gewonnen werden (Heesen, 2020, S. 297). Durch die Sammlung und Auswertung von Daten in einer datafizierten Gesellschaft (Cukier et al., 2013, S. 28) werden auf diesem Wege Informationen generiert, die den alltäglichen Handlungsroutinen von Menschen und entsprechenden Datenbanken aus Wissenschaft, Industrie und Verwaltung entstammen. Die Auswertung von Massendaten bzw. die Nutzung von Big Data baut so auf den zahlreichen direkten und indirekten Spuren des individuellen Handelns auf, die durch die Durchdringung der Alltagswelt mit Informationstechniken zu erfassen sind (Kitchin & Revolution, 2014).

Die Möglichkeiten zur Auswertung großer Datenmengen werden immer häufiger im Zusammenhang ihres Nutzens für die Verbesserung politischer Entscheidungen und der gesellschaftlichen Wohlfahrt diskutiert. Kennzeichnend hierfür sind zum Beispiel die Auseinandersetzungen mit den Chancen und Risiken von Datenauswertungen für die politische Entscheidungsfindung, wie dies etwa die US-amerikanische Regierung, die Europäische Union und auf lokaler Ebene mehr und mehr Städte und Kommunen unterschiedlichster Größe praktizieren (The White House, 2015; Zanouda u. a., 2017). Durch die Auswertung von Massendaten ist mit den digitalen Informationstechniken ein Mittel zur Erzeugung vorgeblich gesicherten und unmittelbaren Wissens an die Hand gegeben. Entsprechend werden Algorithmen und moderne Datenindustrie zunehmend für die Entscheidung über „gültige“ Information und „richtige“ Handlungsempfehlungen genutzt.

Gleichzeitig treten mit den Erhebungen über gesellschaftliche Lebens-/Arbeits-/Umgebungssituationen jedoch Prozesse in den Vordergrund, die elementare Grundlagen der demokratischen Selbstorganisation schwächen könnten (Richter, 2015, S. 45; 46; Suárez-Gonzalo, 2019, S. 662). Die Bedrohung liegt hierbei nicht nur in den häufig genannten repressiven Effekten, die das Gefühl überwacht zu werden hervorrufen kann, sondern – und diese These soll im Folgenden im Vordergrund stehen – in einer Aushebelung der Demokratie

durch die Nutzung individueller, privater Datenspuren für die politische Entscheidungsfindung. Dieser Rekurs auf Datenauswertungen für die gesellschaftliche Steuerung wird real in Prozessen für ein „intelligentes", „data driven" Management in der Politik und in Unternehmen oder dem Ruf nach einer *evidence based policy* (Cairney, 2016). Als problematisch zeigt sich dieser Rekurs insbesondere dann, wenn den daten- und softwaregetriebenen Analysen gegenüber politischen, öffentlichen bzw. gemeinschaftlichen Verständigungsprozessen der Vorzug gegeben wird (Heesen, 2020, S. 291).

2 Privates Handeln und öffentliche Meinungsbildung

Was passiert, wenn das private, individuelle Handeln zum Maßstab politischen Handelns wird? Was auf den ersten Blick und angesichts der emanzipatorischen Einbettung des Privatheitsbegriffs (vgl. das Kapitel von Lamla u. a. in diesem Band) als begrüßenswert erscheint, offenbart bei genauerem Hinsehen Fallstricke.

Private Handlungen sind in der Regel individuelle Handlungen und diese sind zu einem guten Teil Alltagshandlungen. Sie beziehen sich z. B. auf die Organisation des Familienlebens oder die Wahl des Verkehrsmittels und entsprechen nicht-öffentlichen Entscheidungen, teils in klassischen privaten Bereichen wie der eigenen Wohnung. Obwohl diese gelebte Handlungspraxis auf individuelle und private Entscheidungen zurückgeht, kann sie durch Datenanalysen erfasst und kategorisiert werden. Datenerhebungen erscheinen anders als Abstimmungsprozesse häufig als evident und neutral. Unter Umständen können Daten sogar eine größere Realitätsnähe beanspruchen und damit ein anscheinend genaueres, „wahreres" empirisches Wissen hervorbringen. So zeigen viele empirische Untersuchungen, dass Menschen bei Selbstauskünften häufig ihr Verhalten ganz anders bewerten und andere Wünsche angeben, als es tatsächlich der Fall ist (z. B. in Bezug auf das Essverhalten oder die Mediennutzung).

Generell ist die Nutzung wissenschaftlicher Erkenntnisse ein anerkanntes Instrument, um zu besseren politischen Entscheidungsgrundlagen zu kommen. Rückt der wissenschaftliche Zugang jedoch stärker ins Zentrum, dann werden Diskussionen über die sogenannte Expertenherrschaft angestoßen, welche die politische Philosophie seit ihren Anfängen begleiten (Platon, 2012) und auch unter dem Begriff Technokratiedebatte bekannt sind (Heesen, 2012a,

S. 256 ff.). Technokratie bezeichnet ursprünglich ein Konzept zur Regulierung der gesellschaftlichen Organisation (Ellul, 1964; Bell, 1991, S. 69). Danach übernehmen „mechanische" Elemente der wissenschaftlichen und technologischen Zivilisation die Rolle von politischen Regelungen. Der Vorteil liegt aus dieser Perspektive in einer effizienten gesellschaftlichen Steuerung, die vor unsachgemäßen ideologischen Strukturen und Entscheidungen geschützt sei. Statt des politischen Souveräns steht in einer Technokratie die optimierte Selbstorganisation des Menschen durch Wissenschaft, Arbeit und Technik im Vordergrund.

Technokratische Regierungsformen werden vor dem Werthorizont und dem Rechtsverständnis demokratischer Rechtsstaaten weitgehend zurückgewiesen (Bell, 1991), insbesondere, weil sie die Rolle des politischen Souveräns und den Grundsatz der demokratischen Selbstorganisation unterlaufen. Darüber hinaus belegen zahlreiche Arbeiten, dass das Wie und Ob des Einsatzes von Techniken als auch die Technologien selbst eben nicht neutral beziehungsweise nicht unideologisch sind, sondern immer auch Ausdruck bestimmter, teils impliziter Wertentscheidungen (Brey & Floridi, 2010, S. 41). Zur Einordnung des Stellenwertes technisch-wissenschaftlicher Verfahren sind stattdessen demokratische, diskursorientierte Prozesse das adäquate Mittel zur Repräsentation des politischen Souveräns (Fisher, 1987). Für das demokratische Modell des liberalen Rechtsstaates steht für die demokratische Selbststeuerung ein normativer Begriff von Öffentlichkeit im Vordergrund, der sich auf die Bedeutung von Öffentlichkeit für die gesellschaftliche Selbstorganisation wie auch die Kritik und Kontrolle staatlicher Einrichtungen konzentriert (Habermas, 1996). Nach dieser normativen Bestimmung dient Öffentlichkeit der Ermöglichung innergesellschaftlicher Verständigung als Bedingung zur Reproduktion einer funktionsfähigen Demokratie. Entsprechend dient Öffentlichkeit auch zur institutionellen Absicherung einer gemeinschaftlichen Handlungsfolgenkontrolle in gesellschaftlicher Verantwortung.

In diesem demokratietheoretisch grundlegenden Konzept von Öffentlichkeit bestimmt die Kommunikation zwischen „natürlichen" Personen oder Personengruppen (mittels Medien) über den politischen Diskurs und Vorstellungen zum Allgemeinwohl. Zum Zustandekommen solcher kommunikativer Öffentlichkeitsformen gehört insbesondere, sich der *Teilhabe an einer öffentlichen Kommunikationssituation bewusst zu sein.* Die individuelle Entscheidung, an Öffentlichkeit teilzuhaben, geht somit einher mit dem Bewusstsein *der Kommunikationspartner:innen zu ihrer Kommunikation als öffentliche und einer entsprechenden Haltung.* Sie drückt sich damit aus im Verhalten der Kommunikationspartner:innen und der Wahl des Kommunikationsgegenstands,

beispielsweise in einer überindividuellen Themenwahl, die in der Regel mit politischer Relevanz verbunden ist.

Aus der Kommunikationssituation als öffentlicher, die zugleich auch immer eine (indirekte, medial vermittelte) Kommunikation zwischen Personen ist, gehen außerdem bestimmte Reziprozitätsannahmen hervor. Die Kommunizierenden haben insofern gegenseitige Erwartungen aneinander, die konzeptionell vor allem in der Diskursethik offengelegt und formuliert werden. Sie betreffen die Wahrheit, die Wahrhaftigkeit und die normative Richtigkeit von verständigungsorientierter Kommunikation (Habermas, 1996), S. 588). Öffentliche Kommunikation unterliegt daher dem Anspruch, in besonderer Weise „wertvolle" Kommunikation in Hinsicht auf Verständigung, Perspektivenübernahme und das Bemühen um gültige und durchdachte Diskursformen zu sein. Zu den Charakteristika normativer Vorstellungen von öffentlicher Kommunikation gehören also die Annahmen, in einem gewissen Maß vernunftgeleitet zu sein, auf gegenseitige Erwartungshaltungen zu rekurrieren und sich auf bestimmte Themen zu fokussieren. Wichtig ist darüber hinaus, dass die jeweiligen Kommunikationsverhältnisse transparent sind, sich die Beteiligten an der Herstellung von Öffentlichkeit ihrer Situation bewusst sind, ihr Handeln danach ausrichten und eine Wahl treffen können.

Eine bloße Verhaltens- und Zustandsanalyse, wie bei Datenauswertungen der Fall, schließt diese kommunikativen Prozesse aus. Bei Datenanalysen stehen nicht Themenwahl und Diskurs, sondern Erhebungen zum Verhalten einer abstrakten Allgemeinheit im Vordergrund. Es handelt sich um eine Allgemeinheit, die bei einer letztlich maschinellen Modellierung dessen, was (vermeintlich) „der Fall ist", verharrt, aber nicht selbstreflexiv ist in dem Sinne, dass sie ihre eigene Funktionsweise und Wirkung kognitiv als Gemeinwohlüberlegung (vgl. „vereinigter Wille aller", Kant, AAV VI, S. 313) einbeziehen würde.

Das wird besonders deutlich, wenn man sich den häufig beobachteten Widerspruch von Einstellung und Handeln vor Augen führt, bekannt zum Beispiel unter Begriffen wie *Attitude-Behavior Gap* oder *Value-Action Gap.* Demnach handeln Menschen privat häufig anders als es ihren Überzeugungen entspricht. Dieser Punkt wurde indirekt bereits angesprochen, als es um die „Wahrheit" von Verhaltensanalysen gegenüber Umfragen ging. Viele Menschen sind zum Beispiel für artgerechte Tierhaltung und Tierwohl, kaufen ihr Grillfleisch jedoch im Sonderangebot beim Discounter; sie lehnen „Trash-TV" ab, sehen sich die entsprechenden Sendungen jedoch an; viele weiße Menschen haben nichts gegen *People of Color,* wollen aber nicht neben ihnen wohnen (Antidiskriminierungsstelle des Bundes, 2014, S. 76; Bonilla-Silva, 2017, S. 120 ff.). Genau dieses Verhalten wird jedoch in Datenauswertungen abgebildet und fließt teils sogar automatisiert

und intransparent durch das maschinelle Lernen in Steuerungssysteme ein, zum Beispiel durch personalisierte Werbung, Wohnwertberechnungen oder die „intelligente“ Regulierung von Verkehrsflüssen (Böschen et al., 2016). Im Unterschied zu diskursiven Öffentlichkeiten entsteht bei einer Entscheidungsfindung über Datenerhebungen und algorithmische Mustererkennung eine statische Form der Allgemeinheit, die weder intersubjektiv verfasst noch für die einzelnen Subjekte bewusst zustande gekommen ist, aber dennoch eine Wirkung in Hinblick auf politische und wirtschaftliche Entscheidungsprozesse entfaltet. *Auf diesem Wege werden individuelle und private Handlungen durch ihre technische Agglomeration und Auswertung zu überindividuellen und öffentlichen Strukturbedingungen.*

Bei dieser Form der *anonymen Strukturpolitik* arbeitet die („intelligente“) Auswertung von Massendaten mit der Identifizierung von Korrelationen. Es geht hier nicht um das Auffinden von Begründungen und die Priorisierung von Bedeutungen, sondern um das Erkennen von Mustern in Datenagglomerationen. Eine konsequente Nutzung von algorithmischen Systemen und Big Data für politisches Handeln schließt insofern die Analyse von kontrafaktischen und ggf. auch moralischen Motiven und Begründungszusammenhängen aus der politischen Reflexion aus. Statt einer bewussten (innovativen oder kritischen) Steuerung der Themen im öffentlichen Diskurs schreiben algorithmische Systeme gesellschaftliche Analysen auf das empirisch Vorhandene fest. Insofern reproduzieren Datenanalysen immer nur das ohnehin Vorhandene und reduzieren die Darstellung der gesellschaftlichen Verhältnisse auf eine *affirmative,* bestätigende Perspektive (Heesen, 2020).

Um diesem Mechanismus zu begegnen, ist die Aufrechterhaltung des Eigensinns der unterschiedlichen gesellschaftlichen Sphären und ihrer spezifischen Funktion für die gesellschaftliche Ordnung essenziell (Walzer, 1983). An dieser Stelle setzen Theorien des Privaten an, die seine Rolle für eine Grenzziehung zwischen unterschiedlichen Gesellschaftsbereichen mit ihren je eigenen Logiken und Normen betonen.

Privatheitstheorien bauen einerseits auf dem überindividuellen Aspekt der Sphärentrennung auf und fokussieren andererseits über den Begriff der informationellen Selbstbestimmung auf den individuellen Zugang zur Kontrolle der persönlichen Daten und dem Schutz der Privatheit. Über die Abgrenzung des Privaten entscheiden somit *überindividuelle* gesellschaftliche und normative *Kontexte* wie auch *Individuen* durch verschiedene *Adressierungen* von Informationen und personenbezogenen Daten.

3 Überindividuelle Konzepte einer privaten Sphäre

In den frühen Theorien (Altman, 1976; Westin, 1967; Parent, 1983) wurde der Wert des Privaten dadurch begründet, dass Privatheit den willkürlichen Zugang von Dritten auf bestimmte Kommunikationsinhalte restringiert. Gleichzeitig sollte Privatheit schützend für bestimmte Räume wirken, in denen eine freie Identitätsbildung und Rolleneinübung möglich wird. Privatheit wird dabei als ein Sozialraum beschrieben, in dem Autonomie, Selbstverwirklichung, körperliche Integrität, Würde sowie freie Meinungs- und Willensbildung ihre Geltung erlangen und bewahren können. Letztlich ist es dieser Strauß an Werten, welcher – zumindest gemäß der liberalen Tradition, aus der das Konzept des Privaten stammt (Cohen, 2012; Solove, 2015) – als konstitutiv für „gesunde" Öffentlichkeiten und Praktiken demokratischer Teilhabe und Mitbestimmung gilt. Aus diesem Grund ist von verschiedenen Seiten immer wieder argumentiert worden, dass Privatheit kein rein individualistischer, sondern ebenso ein kollektiver Wert ist (Regan, 1995; Mantelero, 2016). Im Zuge der Abgrenzung des Begriffs der Privatheit von dem der Öffentlichkeit erhält Privatheit somit eine überindividuelle, gesellschaftsstrukturierende Bedeutung.

Im historischen Kontext und auf der Ebene sozialer und politischer Gesellschaftsverhältnisse stellt sich die Unterscheidung zwischen privat und öffentlich als Trennung von Gesellschaftssphären dar. Wirtschaftsliberale Modelle verstehen die Unterscheidung von privat und öffentlich als solche zwischen Staat und Privatwirtschaft, also als Verfügungsrecht über Privatsachen (Rössler, 2001). Aus sozialgeschichtlicher und verschiedenen feministischen Perspektiven wiederum wird die Trennlinie zwischen privat und öffentlich zwischen dem familiären beziehungsweise häuslichen Bereich auf der einen Seite und dem politischen und ökonomischen auf der anderen beschrieben (ebd.) und kritisiert. Von Seiten des gesellschaftspolitischen Liberalismus wird die Unterscheidung jedoch anders gerahmt und als Gegenüberstellung von politisch-bürgerschaftlicher Zivilgesellschaft einerseits und Markt und Staat andererseits bestimmt. „Administrative Steuerungssysteme", etwa Geld oder Macht, dürfen nicht bis in die Bereiche der privaten Lebenswelt hineinwirken (Habermas, 1987). Habermas nennt diesen Bereich einer in diesem Sinne privatisierten bürgerlichen Gesellschaft auch „nicht-vermachtete Öffentlichkeit", in dem sich private Autonomie und politische Willensbildung als zwei Ausprägungen der bürgerlichen Gesellschaft Geltung verschaffen können (Habermas, 1996, S. 142 ff.). Der Wert der Privatsphäre besteht demnach in der Schaffung eines geschützten Raumes, welcher die Voraussetzung dafür ist, dass Personen angesichts der invasiven

Kräfte einer in die Lebenswelt eindringenden Wirtschaft sowie eines mit weitreichenden Befugnissen ausgestatteten Staates eine selbstbestimmte Persönlichkeit ausbilden und erhalten können (Kahn, 2003, vgl. z. B., Young, 1987; Suárez-Gonzalo, 2019; Nash, 2005).

Ein solcher Begriff einer bürgerschaftlich geprägten Öffentlichkeit von „Privatleuten" (Habermas, 1996) schließt an die emanzipatorischen Erwartungen an, die zu Beginn seines Aufkommens auch mit dem Internet in Bezug auf Pluralismus, Mitbestimmung und Selbstorganisation verbunden waren (Helbing, u. a.). Wichtig für einen solchermaßen verstandenen Begriff einer öffentlichen Privatsphäre ist die Schaffung von Voraussetzungen für die Bildung von sozialen und kulturellen Identitäten, persönlichen Netzwerken und Erfahrungsräumen in Absehung von ökonomischen oder staatlichen Vorgaben. Auf diesem Wege machen die Privatleute den Eigensinn ihrer individuellen Lebensführung für die Teilhabe an Öffentlichkeit als regulatorischem Netzwerk eines demokratischen Gemeinwesens nutzbar.

Privates Handeln bezeichnet somit einen Freiraum persönlicher Lebensgestaltung, aber der Schutz des Privaten und der hiermit verbundene Schutz der informationellen Selbstbestimmung ermöglicht eine überindividuell und politisch relevante Grenzziehung zur Abwehr hegemonialer kommerzieller und administrativer Macht. Privatheit und der Eigensinn privater Lebensführung dienen auf diesem Wege als Ressource für gesellschaftliche Pluralität und unabhängige politische Meinungsbildung. Ein solcher Privatheitsbegriff bezieht sich auf das Handlungspotenzial einer autonomen Privatsphäre. Angesichts dessen ist die Sicherung von Freiheitsrechten durch Datenschutz und Informationelle Selbstbestimmung nicht ausreichend für den nachhaltigen Bestand einer lebendigen Demokratie. Möglichkeiten wie z. B. das Verbergen persönlicher Daten durch Datensparsamkeit oder Verfahren wie Privacy by Design sind zwar eine notwendige, jedoch keine hinreichende Voraussetzung zur Wahrung einer nicht bloß defensiv, datenschutzrechtlich verstandenen Privatsphäre (Heesen, 2012b).

Vor allem jene Privatheitstheorien, die den Begriff des Privaten von einem individualistischen auf einen intersubjektiven Fokus verlagern, argumentieren in diesem Zusammenhang, dass Privatheit nicht mehr individualistisch nur lebensweltliche Autonomie beschützen soll, sondern – im Sinn relationaler Autonomie (Mackenzie & Stoljar, 2000) – intersubjektiv beziehungsweise relational gedacht werden muss. Aus dieser Perspektive verringert sich die vermeintliche Spannung zwischen individueller Freiheit und kollektiver Wohlfahrt sowie sozialer Gerechtigkeit. Privatheit wird somit zum Gemeingut, indem gezeigt wird, dass sämtliche soziale Sphären – jenseits der Dichotomie von Privatheit

und Öffentlichkeit – durchzogen sind von Informationskontexten, die sich über Konventionen des angemessenen Flusses von Informationen und insbesondere personenbezogenen Daten konstituieren (Nissenbaum, 2010).

Vor diesem Hintergrund muss zwischen dem Schutz und der Herstellung von Privatheit unterschieden werden. Das Recht auf informationelle Selbstbestimmung (vgl. das Kapitel von Roßnagel u. a. in diesem Band) sowie der Anspruch auf und der Wunsch nach Privatheit beruhen auf dem Idealbild des autonomen Individuums, das für den Wertekatalog moderner Demokratien und das hiermit verbundene Menschenbild vorherrschend ist. Während der *Schutz* der Privatheit insbesondere für die Wahrung der Integrität der Person von Bedeutung ist, zielt eine Kombination von Schutzansprüchen und Verfahren zur *aktiven Herstellung* eines Privatbereichs auf die gesellschaftspolitische Bedeutung der Privatsphäre als Raum einer lebensweltlichen Ressource zur Kontrolle administrativer und ökonomischer Macht. Diese Funktion kann nur dann bestehen, wenn eine Trennung gesellschaftlicher Sphären intakt ist und verschiedene Norm- und Geltungssysteme miteinander in einen produktiven Widerstreit treten können. Bei dieser Trennung von verschiedenen gesellschaftlichen Handlungssystemen kommt der Privatsphäre für die Wahrung individueller und demokratischer Freiheitsrechte eine besondere Bedeutung zu, denn sie kennzeichnet den Anspruch des Individuums auf einen Bereich, in dem konzeptionell persönliche Unverfügbarkeit, Selbstbestimmung und Zwanglosigkeit im Vordergrund stehen. Aus Perspektive derjenigen, die Privatheit beanspruchen, geht es um den Erhalt von selbstorganisierten, autonomen Handlungsräumen, die sich über die Freiheit von Fremdbestimmung durch eine übergeordnete Struktur (in Staat, Markt, Öffentlichkeit usw.) bestimmt. Privatsphäre konstituiert sich auf gesellschaftlicher Ebene somit durch den Schutz einer Differenz zwischen verschiedenen Handlungsregimen. Bei dieser Bestimmung ist die Bedeutung der Leitdifferenz für den Schutz vor einer vereinheitlichenden, totalitären Ordnung ausschlaggebend. Bei der Wahrung von Privatheit und informationeller Selbstbestimmung geht es also grundlegend um die Abwehr und Einhegung hegemonialer beziehungsweise totalitärer Ansprüche über individuelle und gesellschaftliche Lebens- und Handlungsbereiche (Heesen, 2016, S. 55).

Die Aufteilung der verschiedenen Handlungssphären selbst ist fragil und Gegenstand immer neuer Aushandlungsprozesse, was ja auch die scheinbare Beliebigkeit von „privaten“ und „öffentlichen“ Zuordnungen historisch und in unterschiedlichen sozialen und kulturellen Kontexten zeigt. Zudem herrschen auch in der jeweils als privat titulierten Sphäre teils repressive Ordnungen und nicht zuletzt die feministischen Bewegungen haben verdeutlicht, dass umfassende rechtliche (bzw. öffentliche) Regeln gerade für den häuslichen Bereich ein

befreiendes Potenzial haben können. Trotzdem kommt der Privatsphäre als Ressource und Gegenmodell zu präformierten und fremdbestimmten Möglichkeitsräumen eine elementare Rolle für gesellschaftliche Selbstorganisation und individuelle Freiheit zu. Sie schafft erst die notwendigen Strukturbedingungen für die Auslebung oder Substantiierung von Freiheitsrechten, „weil mit der bloßen Sicherung von *Freiheit* […] noch nicht notwendig und zugleich die *Bedingungen* dafür gesichert sind, dass wir die Freiheiten so leben können, wie wir wirklich wollen“ (Rössler, 2001, S. 138). Während Freiheitsrechte also formal die Bedingungen für ein selbstbestimmtes Leben sichern, steht Privatheit für die Ausgestaltung des Rechts auf eine selbstbestimmte Lebensführung in individueller und demokratischer Perspektive. Vor diesem Hintergrund, der die Bedeutung des Eigensinns und der Trennung verschiedener Gesellschaftssphären vor Augen führt, rückt der Blick auf technische Infrastrukturen in den Vordergrund.

In diesem Zusammenhang werden vor allem drohende oder sich tatsächlich ereignende *context collapses* diskutiert (Wesch, 2009; Marwick & boyd, 2011; Tufekci, 2018). Hierbei geht es um Informationskontexte, welche voneinander getrennt werden sollen, sich faktisch jedoch vermischen, mit dem Resultat des illegitimen informationellen „Eindringens“ von Drittakteuren in eigentlich geschützte Informationsbestände. Problematisiert wird dabei insbesondere die Nichteinhaltung der Anpassung von Informationsflüssen. Diese Angemessenheit wird bestimmt durch kontextspezifische Normen, welche den Verbreitungsradius von personenbezogenen Informationen bestimmen sollen (Nissenbaum, 2010). In diesem Sinne entzündet sich der Protest gegen neue digitale Technologien gerade an deren unkontrollierbaren, kontextübergreifenden Informationsverarbeitungsmöglichkeit (Hagendorff, 2017). Als Treiber dieses Kontrollverlusts sind unter anderem der hohe Vernetzungsgrad digitaler Technologie und deren hohe Speicher- sowie Berechnungskapazitäten zu benennen (Seemann, 2014) wie z. B. beim Cloud-Computing sichtbar.

Beispiel Cloud: Regulierung zentralistischer Infrastrukturen

Infrastrukturen bestimmen über die technischen Grenzen der Kommunikation in und über Gesellschaftssphären hinweg wie auch über die individuellen Eingrenzungen von Informationsflüssen. Für den Schutz und die Ausgestaltung des Privaten spielen nicht nur individuelle Entscheidungen oder staatliche Überwachung eine Rolle, sondern vor allem auch die technische Gestaltung. Die Informationsgesellschaft benötigt sowohl Informationstechnologien wie Computer, Smartphone und andere Endgeräte, aber auch Infrastrukturen und vermehrt auch Plattformen und Netzdienste.

Insbesondere bei IT-Infrastrukturen lässt sich in den letzten Jahren ein Trend hin zu zentralisierten Angeboten und Technologien beobachten. Hier werden zum einen die Effekte der Plattformökonomie diskutiert. Zentralisierungsaspekte liegen dabei vor allem auch im Netzwerkeffekt: Große Plattformen sind attraktiver und haben Wachstumsvorteile, weil die Menschen dahin gehen, wo sie sich mit anderen verbinden können – wie das langjährige Wachstum Facebooks und seiner Dienste trotz harscher Kritik zeigt. Problematisch wird hierbei gesehen, dass diese Plattformen enorme Macht konzentrieren, welche für demokratische Gesellschaften gefährlich sind. Zum anderen hat Shoshana Zuboff einen weitbeachteten Beitrag unter dem Schlagwort „Überwachungskapitalismus" formuliert, in dem sie Plattformanbietern systemische und inhärente Eigenschaften attestiert: Datenextraktion, Verhaltensvorhersage und Verhaltensmodifikation. Dieses Geschäftsmodell bewertet Zuboff als „zutiefst demokratiefeindlich" (Zuboff, 2018, S. 224). Für solche demokratiefeindlichen Geschäftsmodelle stehen insbesondere die Zentralisierungstendenzen in IT Infrastrukturen im Cloud Computing (KPMG, 2019).

Cloud Computing bedeutet, dass IT-Programme und -Dienste nicht auf Computern vor Ort laufen, sondern in großen Rechenzentren, die die Leistung über eine Netzverbindung bereitstellen. Die Vorteile liegen vor allem in den geringeren Investitions- und Wartungskosten sowie ökonomischen Skaleneffekten, aber auch in Sicherheitsüberlegungen. Unternehmen und Nutzer:innen können Serverkapazitäten und Anwendungen nach Bedarf mieten und schnell anpassen – wodurch die Investitionskosten und das nötige Wissen für IT und IT-Sicherheit reduziert werden. Dieser Trend ist sowohl bei Unternehmen und Organisationen als auch bei Konsumenten und Privatpersonen zu beobachten und wird von den großen IT-Plattformen vorangetrieben. Die Dienste werden auf den Nutzeroberflächen der Computer oder Smartphones angezeigt, aber dort werden sie nicht bearbeitet oder die Daten gespeichert – sondern in großen Rechenzentren, die sich viele Organisationen und Nutzer:innen teilen.

Diese Technologien haben auf den Schutz der Privatheit in verschiedenen Aspekten Auswirkungen. Auf grundsätzlicher Ebene ist das Cloud Computing ein zentraler Sammel- und Verarbeitungsraum der Daten aus sämtlichen gesellschaftlichen Teilbereichen. Cloudinfrastrukturen lösen somit die sozialen Grenzen zwischen verschiedenen Informationstypen und verankern zumindest auf technischer Ebene einen permanenten *context collapse* (boyd, 2010). Zum einen fallen bei den sowohl kostenlosen als auch bezahlten Cloud-Anwendungen für Konsument:innen sehr viele Nutzungsdaten an und werden ausgewertet, die bei einer lokalen Installation des Dienstes nicht oder nur in geringerem Maße anfallen würden. Wer Musik über Spotify hört, Filme streamt, seine Dokumente

in der Cloud bearbeitet, wird getrackt. Häufig mit dem Hinweis auf den Beitrag zur Verbesserung des Nutzungserlebnisses. Eine vollständig anonyme Nutzung ist praktisch nicht vorgesehen oder gar möglich.

Zum anderen gibt es Privatheitsprobleme natürlich nicht nur für die Nutzungsvorgänge, sondern auch für die in der Cloud gespeicherten Daten selbst. Cloud-Anbieter haben – außer bei der Verwendung von Ende-zu-Ende-verschlüsselten Lösungen – Einblick in die bei ihnen gespeicherten Daten. Das ist zum einen relevant, wenn man sich als Privatperson dazu entscheidet, Cloud-Dienste statt lokaler Anwendungen und Speichermöglichkeiten zu verwenden. Aber es wird darüber hinaus wichtig, wenn die Unternehmen, Kontaktpersonen und Einrichtungen, die Daten über Privatpersonen speichern und verarbeiten, diese in Cloud-Umgebungen auslagern. Wenn das Krankenhaus, das mich behandelt, Microsofts Cloud-Produkte einsetzt, liegen meine Daten damit auch bei Microsoft – ohne, dass ich davon direkt Kenntnis erlange. Manche Unternehmen lagern ihre komplette IT und ihre Software-Angebote in Cloud-Rechenzentren aus – Tendenz steigend (KPMG, 2019).

Hier gibt es kurz umrissen zwei Bewertungsmöglichkeiten. Die eine folgt der Überzeugung, dass eine Zentralisierung von Datenspeicherung und Anwendungen in Cloud-Rechenzentren die IT-Sicherheit erhöht und damit auch eine spezifische Form der Privatheit verbessert: Expert:innen kümmern sich rund um die Uhr um die Integrität der Systeme, erkennen Sicherheitslücken und Angriffe. Wenn Daten bei kleinen Unternehmen oder im Keller der Psychotherapeutin auf veralteter und nicht gewarteter Konsumentenhardware liegt, sind sie weniger gut geschützt als bei Konzernen, die Millionenbudgets für IT-Sicherheit bereitstellen, Erfahrung haben und durch die zentrale Organisation auch Schwachstellen unter Kontrolle haben, die dezentral unentdeckt blieben oder unerreichbar für eine Lösung sind.

Gleichzeitig haben aber eben diese Cloud-Provider potenziell Einblick in die Daten und ihre Nutzung, können Sie je nach Dienst komplett oder pseudonymisiert auswerten, daraus Wettbewerbsvorteile erreichen und Macht aufbauen. Außerdem ziehen zentrale Datenansammlungen nicht nur Angriffe und Hacking an, sondern wecken auch Begehrlichkeiten von Seiten staatlicher Überwachung. Darüber hinaus ist zu beachten, dass die Cloud-Infrastruktur natürlich in einem anderen Rechtssystem angesiedelt sein kann – mit abweichenden Privatheitsschutzstandards, Sicherheitsanforderungen und staatlichen Zugriffsregelungen.

Aktuell zeigt die Betrachtung und Analyse von Cloud-Projekten in Europa, dass die Antwort auf Privatheitsfragen im Bereich des Cloud-Computings immer häufiger mit territorialen Grenzen verknüpft wird. Die Microsoft Cloud Germany

wollte ihren Erfolg durch die Garantie der Datenspeicherung in deutschen, treuhändisch durch die Deutsche Telekom betreuten, Servern erreichen. Das Projekt GAIA-X setzt auf die Ausgestaltung eines europäischen Cloud-Ökosystems, das „europäische Werte“ und europäische Datenschutzstandards durch Lokalisierung der Cloud-Infrastruktur und damit eine Dezentralisierung und Abkehr von dominanten Cloud-Providern vorsieht. Datenschutz, digitale Souveränität und europäische Werte werden Schlagworte dieser Entwicklungen und es wird versucht, diese in Technik abzubilden und sie so zu gestalten, dass sie den Normen europäischer demokratischer Gesellschaften entspricht oder zumindest nicht zuwider läuft (der wirtschaftliche Konkurrenzkampf mit US-amerikanischen und chinesischen Anbietern ist natürlich ein weiterer Aspekt).

Ein klassischer Ansatz der privatheitsschützenden Technikgestaltung, der auch als Empfehlung seinen Einzug in die europäische Datenschutzgrundverordnung gefunden hat, ist Privacy by Design. Ausgehend von der Beobachtung, dass bestehende Listen über die Religionszugehörigkeit der niederländischen Bevölkerung es den Nazis sehr einfach machte, jüdische Menschen zu verschleppen und umzubringen, präsentierte John Borking 1995 sogenannte Privacy Enhancing Technologies. Technologie sollte niemals mehr dazu verwendet werden können, solche Verbrechen durchzuführen. Er argumentierte dafür, nur notwendige Daten zu speichern und verarbeiten und Technik so zu gestalten, dass sie Menschenrechte und Privatheit schützt. Ann Cavoukian, damals Datenschutzbeauftragte in Kanada, erweiterte diese Idee in den 1990ern durch die Einbeziehung positiver Ziele statt reiner Verbote und veröffentlichte das Konzept Privacy by Design (Cavoukian et al., 2010). Cavoukian argumentiert: „Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks,rather, privacy assurance must ideally become an organization’s default mode of operation“ (Cavoukian, 2011; Altman, 1976).

Gerade in Hinblick einer umgreifenden Technisierung demokratischer Gesellschaften und vor dem Hintergrund einer Konzentration von Daten, Funktionalität und damit Macht nicht nur bei Unternehmen, sondern in der Infrastruktureigenschaft selbst, ist eine bewusste, grundrechtsschützende und demokratiefördernde Technikentwicklung wichtig. Konzepte wie Privacy by Design, aber auch die kritische Begleitung und bei Bedarf der regulatorische Eingriff in Infrastrukturentwicklung und -gestaltung sind Grundlagen heutiger und zukünftiger demokratischer Gesellschaften.

4 Individuelle Privatheit als selbstbestimmter Aushandlungsprozess

Während in Bezug auf IT-Infrastrukturen und die gesellschaftliche Funktion des Privaten überindividuelle Regulierungs- und Ordnungsfragen im Fokus stehen, verbinden komplementäre Ansätze das Recht auf Privatheit mit den Freiheits- und Selbstbestimmungsrechten des Individuums. Insbesondere ausgehend von dem 1983 getroffenen Volkszählungsurteil (Bundesverfassungsgerichturteil vom, 15) wird mit dem Konzept der individuellen informationellen Selbstbestimmung der Wert des Privaten als unverzichtbarer Bestandteil gelingender Demokratien gesehen, der gegen die schleichende Transformation in eine Überwachungs- oder Kontrollgesellschaft (Los, 2006, Deleuze, 1992) verteidigt werden muss. Der Schutz des und der Einzelnen vor der unkontrollierbaren Freigabe von personenbezogener Information ist nach dem Konzept der informationellen Selbstbestimmung eine elementare Voraussetzung für die Ausbildung einer reflektierten Ich-Identität – also einer Identität, die es dem Individuum ermöglicht, sich selbst zu bestimmen und bestimmte Handlungsoptionen zu prüfen beziehungsweise zu verwerfen (Heesen, 2012b).

Allgemein gesprochen soll Privatheit insofern die persönliche Entfaltung sicherstellen sowie vor negativen Einflüssen sowie illegitimen Beobachtungen Dritter beschützen. Diese Einflüsse werden insbesondere an überwachend oder „manipulativ“ wirkenden Technologien festgemacht (Susser et al., 2018), wobei Schlagworte wie „Gesichtserkennung“, „intelligente Videoüberwachung“, „Big Nudging“, „Micro Targeting“ oder andere verwendet werden (Hagendorff et al., 2020). Auch der Umstand der Anwendung computergenerierter probabilistischer Einschätzungen und Prognosen, in der Literatur oft als *algorithmic decision making* (ADM) bezeichnet, auf einzelne Personen wird als Privatheitsproblem gerahmt. Doch trotz zahlreicher Skandale, wie die Aufdeckung von Überwachungspraktiken der NSA, Datenlecks bei Social-Media-Plattformen oder Versuchen der Wahlmanipulation durch Micro Targeting, ist eine effektive Zurückdrängung der Interessen mächtiger wirtschaftlicher oder staatlicher Akteure bislang kaum gelungen (Stanley, 2019; Hagendorff, 2019; O'Neil, 2016; Epstein & Robertson, 2015). Dennoch wird in der Privatheitsliteratur entgegen empirisch feststellbarer Überwachungspraktiken und einer anhaltenden Verdrängung von tradierten Privatheitspraktiken die Wichtigkeit des Schutzes individueller Interessen an Autonomie, Selbstentfaltung, körperlicher Integrität, Würde sowie freier Meinungs- und Willensbildung durch das „Schild“ Privatheit betont (Solove, 2008).

Neuere Theorien verhandeln den Wert des Privaten weniger im „vertikalen" Spannungsfeld zwischen Systemen (Wirtschaft, Politik) und Lebenswelt, sondern mehr im „horizontalen" Verhältnis zwischen einzelnen sozialen Kontexten (Nissenbaum, 2010). In diesem Zusammenhang geht es um die Sicherung der Erwartungen, die Personen gegenseitig in Bezug auf das Wissen voneinander haben. Nur dann, wenn die Beteiligten das Bild kontrollieren können, das andere Personen von ihnen haben (sollen), können Privatheitsansprüche gewahrt bleiben. Darüber hinaus fixiert der Wert des Privaten Normen und Regeln, die einen angepassten, kontextbezogenen Austausch von persönlichen Informationen zwischen verschiedenen sozialen Feldern sichern sollen (Marwick et al., 2011). Die Aufhebung informationeller Kontexttreue kann dabei verschiedene Formen annehmen (Pörksen & Detel, 2012). Zeitliche Kontextverletzungen können dazu führen, dass eventuell vergessene Informationen aus der Vergangenheit in der Gegenwart wieder aufgegriffen werden. Kulturelle Kontextverletzungen hingegen definieren sich darüber, dass Informationen zwischen verschiedenen, miteinander inkompatiblen Bedeutungsräumen ausgetauscht werden. Und publikumsbezogene Kontextverletzungen können auslösen, dass Informationen so verbreitet werden, dass sie verschiedenen, eventuell unerwünschten Kreisen gegenüber verfügbar sind. Gerade letztere Form der Kontextverletzung wird im Zusammenhang mit digitalen Informations- und Kommunikationssystemen mit konstanter Regelmäßigkeit angeprangert, wobei insbesondere Transparenzasymmetrien kritisiert werden, welche sich zwischen staatlichen beziehungsweise wirtschaftlichen Institutionen und Bürger:innen beziehungsweise Kund:innen aufspannen. Problematisch sind solche Transparenzasymmetrien, da mit ihnen ein Machtrespektive Machtmissbrauchspotenzial einhergeht.

Verkompliziert wird das Einhalten von Normen des angemessenen Informationsflusses durch sich weiterentwickelnde Methoden der Datenverarbeitung. Künstliche Intelligenz ermöglicht nicht nur das automatisierte Treffen algorithmengestützter Entscheidungen, welche zur Steuerung und Organisation sozialer Systeme verwendet werden (Krafft & Zweig, 2019), sondern desgleichen die Extraktion „emergenter", privater Informationen aus „unverdächtigen" Datensätzen (Matz et al., 2019, Lambiotte & Kosinski, 2014; Kosinski et al., 2013). In diesem Zusammenhang werden etwa aus Surfgewohnheiten einzelner Individuen auf probabilistische Weise private Informationen gewonnen, welche in der Folge etwa zu Zwecken der Anpassung von personalisierter Werbung oder Newsfeeds eingesetzt werden. Alle diese Technologien können zu einer Gefahr für demokratische Werte werden. So werden beispielsweise Filterblasen für die übermäßige Verbreitung von Falschmeldungen sowie Radikalisierungstendenzen im öffentlichen Diskurs verantwortlich gemacht (Lischka & Stöcker, 2017);

(Tufekci, 2018); (Flaxman et al., 2016); (Pariser, 2011)]. Illegitime Informationsbestände, die jedoch eine besonders hohe Popularität unter den Nutzern sozialer Netzwerke genießen, verbreiten sich stärker als legitime Informationsbestände. Nicht zuletzt die anlasslose Massenüberwachung stützt sich auf Verfahren der künstlichen Intelligenz und ist ihrerseits mit demokratiegefährdenden Tendenzen verbunden (Platon, 2012). Es wird davon ausgegangen, dass staatlich eingesetzte Überwachungstechnologien sich über chilling effects negativ auf das politische Engagement von Bürger:innen auswirken (Lyon, 2001). Wenngleich in der Gesamtschau die kausale Verknüpfung zwischen privatheitsverletzenden digitalen Technologien sowie der Entwicklung politischer Ordnungsformen kaum bis gar nicht valide empirisch untersucht werden kann, so kommen Studien doch zu dem Schluss, dass zumindest der umgekehrte Effekt, also eine Förderung demokratischer Werte und Institutionen nicht gegeben ist (Rød & Weidmann, 2015).

Letztlich verbirgt sich hinter der Betonung der Bedeutung von Privatheit für demokratisch verfasste Gesellschaften die grundlegende Idee, dass Menschen sich zu mündigen, aufgeklärten, freien Individuen entfalten können sollen, um ihr politisches Agieren gegenüber der Gemeinschaft legitimieren zu können [(Gavison, 1980); (Regan, 1995)]. Unter Druck gesetzte, fehlinformierte oder durch Dritte manipulierte Personen können zwar beispielsweise ihr Wahlrecht ausüben oder ihre Meinung öffentlich äußern, allerdings nicht unbedingt im Sinne ihres eigenen Wohls oder des Gemeinwohls.

Beispiel Medienmündigkeit: individuelle Selbstbestimmung in der digitalen Welt
Die grundlegende Idee, dass Menschen sich durch den Schutz ihrer Privatheit zu mündigen, aufgeklärten und freien Individuen entfalten können, impliziert, dass sie über die Form und das Maß ihrer Privatheit selbst entscheiden können. Das demokratische Selbstverständnis ist dadurch geprägt, dass Privatheit individuell, wie auch kollektiv eine wählbare Möglichkeit ist. Das heißt, dass Privatheit ein Wert neben anderen Werten ist, für oder auch gegen den sich Individuen entscheiden können. Genau dieser Akt der Entscheidung ist ein Teil von Autonomieansprüchen, die sich im Grundsatz der informationellen Selbstbestimmung artikulieren. Privatheit ist an den Leitwert der *Autonomie* in Form personaler Selbstbestimmung gekoppelt, die als Grundlage eines gelingenden Lebens des Einzelnen sowie der (auch pluralen) Gesellschaft in freiheitlichen Demokratien gilt.

Damit dies aber möglich wird, bedarf es einer grundlegenden "Mündigkeit" von Bürger:innen, die demokratisches Handeln in Form von politischer Mitbestimmung, gesellschaftlicher Teilhabe und Partizipation im Zuge der Entfaltung der eigenen Persönlichkeit umfasst. Mündigkeit ist in digitalen Gesellschaften

immer auch mediale Mündigkeit. Die Frage der Medienmündigkeit gilt dabei im gesamten Lebensverlauf. Gerade für verletzlichere gesellschaftliche Individuen und Gruppen, wie ältere Menschen, Menschen mit Beeinträchtigungen oder Heranwachsende, wird sie wesentlich. Sie bedarf im Sinne sozialer Gerechtigkeit inklusiver Bedingungen – durch geeignete Infrastrukturen, angemessene Anwendungsformen, aber auch Aufklärung und Maßnahmen zur Ermöglichung von Mündigkeit im gesamten Lebensverlauf.

Fragen einer gelingenden Unterstützung von Medienmündigkeit sind insbesondere für Kinder und Jugendliche von hervorgehobener Bedeutung, wenn man bedenkt, dass laut einer UNICEF-Studie (Livingstone et al., 2019) ein Drittel der weltweiten Internetnutzer:innen Kinder bis 18 Jahre sind. Die Rede von der "mediatisierten Kindheit" (Cavoukian et al., 2010) beschreibt nicht nur die Nutzungszahlen, sondern zusätzlich die Omnipräsenz digitaler Medien als einem „Querschnittsthema" heutiger Kindheit und Jugend. Versteht man Kindheit als besonders vulnerable Entwicklungsphase, so haben Prozesse der Digitalisierung und Medialisierung das Potenzial, die Lebenswelt von Kindern und Jugendlichen maßgeblich zu verändern und ihr Erwachsenenleben elementar zu prägen. Barbies mit Überwachungsfunktion, Video-Plattformen wie YouTube oder TikTok, vernetzte Computerspiele, Lern-Apps und Messenger-Dienste wie WhatsApp stehen exemplarisch für Dienste und Medientechniken, die bereits für Kinder eine bedeutende Rolle spielen und ihr Medienhandeln auch in ihrem Alltag prägen. Heranwachsende unterscheiden dabei nicht mehr, wie frühere Generationen, zwischen „real" und „virtuell" oder zwischen „analog" und „digital". Die Kanäle oder Endgeräte für Kommunikation und sozialen Austausch sind für sie zweitrangig, ohne dass sie gleichzeitig genügend Erfahrungen und Informationen, oder teilweise auch kognitive Fähigkeiten oder gar Kompetenzen haben, die ihnen selbstbestimmte, mündige Entscheidungen in medialen Kontexten ermöglichen.

Bei Kindern geht es um erhöhte Schutzansprüche, die an Fürsorgetragende wie Eltern gestellt werden. Diese sollen eine Zukunft von Kindern überhaupt erst ermöglichen. Je jünger die Kinder sind, desto bedeutsamer ist dieser Schutzbedarf daher auch aufgrund der bestehenden Abhängigkeitsverhältnisse. Dass Kinder noch in Entwicklungsprozessen stecken, in denen sich biologische, psychische und soziale Kompetenzen und Fähigkeiten erst noch ausbilden, ist der Hauptbezugspunkt der Schutzargumentation und Fürsorgepflicht. Sowohl im *Grundgesetz* (Art. 6 GG) als auch in der *UN-Kinderrechtskonvention* (Art. 5 UN-KRK) wird elterlichen Rechten und Pflichten gegenüber ihren Kindern Rechnung getragen (Seemann, 2014). Denn gerade kleinere Kinder können die Folgen ihres Handelns nicht vergleichbar abschätzen wie Erwachsene. Was Kinder von

Erwachsenen unterscheidet, sind sich sukzessive entwickelnde kognitive Fähigkeiten, weniger gelebte Erfahrung und Zugang zu Informationen sowie das erst allmähliche Abwägen möglicher Folgen sowie Nebenfolgen des eigenen Handelns.

Soll Medienmündigkeit ausgesprochenes Ziel heutigen Heranwachsens sein, damit personale Selbstbestimmung in digitalen Umwelten auch mit Blick auf Privatheit möglich wird, dann greift ein alleiniger Fokus auf Schutz zu kurz. Kinder als handelnde Subjekte zu verstehen ermöglicht ein kinderrechtlicher Ansatz, der auf das Zusammenspiel von Partizipation, Befähigung und Schutz fokussiert (Stapf, 2020). Das zentrale Thema einer medienethischen Auseinandersetzung zur Kindheit bleibt dabei die Frage, wieviel paternalistischer Eingriff im Zuge des Schutz- und Fürsorgeprinzips in die Autonomie- und Freiheitsrechte des Kindes trotz des Gleichheitsgrundsatzes rechtfertigbar ist (Stapf, 2018, 2019).

Kinderrechte als „Menschenrechte für Kinder“ (Maywald, 2012) haben dabei die Entwicklungsdimension von Kindheit, d. h. die *evolving capacities* (Lansdown, 2005), von Kindern zu berücksichtigen. Die Wichtigkeit von Befähigung neben Schutz lässt sich an den rechtlichen Vorgaben zur Privatsphäre von Kindern im Kontext des Digitalen veranschaulichen. So verbrieft Artikel 16 der UN-Kinderrechtskonvention, dass „kein Kind (…) willkürlichen oder rechtswidrigen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr oder rechtswidrigen Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden (darf)“ und „Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen“ hat. Es geht also um die Möglichkeit zu entscheiden, welche Informationen in bestimmten Kontexten oder mit bestimmten Personen geteilt werden sollen.

Mit Blick auf Kindheit als Entwicklungsphase geht es folglich auch um die *Ermöglichung von Privatsphäre* als einem grundlegenden demokratischen Freiheitsrecht (Stapf, 2020). Privatheit hat unterschiedliche Bezugsdimensionen (von körperlicher Integrität, mentalen Vorgängen, über persönliche Entscheidungen, lokale Räume, den Schutz privater Daten bis hin zu institutionellen Bereichen), die sich analytisch unterscheiden lassen, die aber – gerade bei Kindern – in der Praxis zutiefst verwoben sind,sie tritt „relational innerhalb sozialer Konstellationen“ auf (Ochs, 2019, S. 15). Die Bildung Heranwachsender hin zur gesellschaftlichen Teilhabe und personalen Selbstbestimmung braucht damit gleichermaßen die konkrete Erfahrung von Privatsphäre in der konkreten Lebenswelt sowie ihre Ermöglichung (Erziehung zur Mündigkeit). Deutlich wird hier die Wichtigkeit von Befähigung im erzieherischen und sozialen Kontext.

Kinder haben dabei ein Recht auf eine offene Zukunft (Feinberg, 1980) und bedürfen besonderer Schutzräume zur freien Entwicklung ihrer Persönlichkeit.

Digitale Medien können hierbei neuartige Formen von Teilhabe und Partizipation sowie Bildung und Unterhaltung ermöglichen, sie können aber auch kindliche Schutzrechte einschränken – ein Spannungsfeld, das sich in der Aushandlung von Autonomie versus Fürsorge immer ergeben kann und was besondere Verantwortlichkeiten bedingt. Dies umfasst eine Verzahnung von Maßnahmen verschiedener Verantwortungsträger:innen, die von der Medienregulierung und dem Jugendmedienschutz, über Elternbildung, bis hin zu medialen Anbietern und Bildungseinrichtungen für Kinder und die Zivilgesellschaft reicht.

5 Zur Ambivalenz des Privaten für die Demokratie

Kritisch gegenüber der liberalen Tradition von Privatheit, wie sie hier in Bezug auf Gesellschaft und Individuum geschildert wurde, kann angemerkt werden, dass Privatheit letztlich keinen politischen Wert an sich darstellt, sondern vielmehr ein Sammelbegriff ist für Werte und Maßnahmen, welche demokratische Teilhabe und politische Entscheidungsfindungsprozesse sicherstellen und optimieren sollen. Privatheit wäre demnach ein instrumenteller Wert, der zur Realisierung anderer Werte dient. Reduktionistisch argumentierende Ansätze gehen davon aus, dass Privatheitskonzepte letztlich Konglomerate anderer grundlegender Rechte, wie etwa des Rechts auf Leben, Freiheit und Eigentum, sind. Diese Ansätze gehen davon aus, dass kein eigenständiges Recht auf Privatheit ausgemacht werden kann (Davis, 1959; Moore, 2008). Kommunitaristische Ansätze kritisieren darüber hinaus, dass Privatheitskonzepte dem Individuum das Primat vor der Gemeinschaft einräumen und damit einen Verfall "öffentlicher" Werte wie Sicherheit, Wohlfahrt, Verantwortungsbewusstsein etc. begünstigen (Etzioni, 1999). Seitens feministischer Positionen wird ferner kritisiert, dass die Privatsphäre der Verschleierung (häuslicher) Gewalt dienen kann und das hierarchische Herrschaftsverhältnis zwischen Männern und Frauen verhärtet (MacKinnon, 1989, Olsen & Smith, 1993). Ebenfalls darf in diesem Zusammenhang nicht in Vergessenheit geraten, dass die Berufung auf Privatheit auch für politisch schädliche Bemäntelungseffekte stehen kann. So kann beispielsweise die Ausübung legitimer journalistischer Recherchearbeit unter Verweis auf das Recht auf Privatheit eingeschränkt werden, sodass wichtige Informationssaufgaben der Presse gegenüber der Öffentlichkeit behindert werden.

Der Ruf nach Privatheit ist demnach möglicherweise in bestimmten Fällen nichts anderes als ein Ruf danach, bestimmte Normverletzungen weiterhin ausführen zu können. Zwischen der sozial akzeptierten Abwehr staatlicher oder unternehmerischer Macht sowie der nicht sozial akzeptierten Begehung und

Verschleierung illegitimer Normverletzungen und Straftaten liegt zwar ein fundamentaler Unterschied, dennoch kommt es in beiden vor, dass Privatheit und Datenschutz als Argumente ins Feld geführt werden. Desgleichen werden möglicherweise dieselben technischen Anwendungen oder *privacy enhancing tools* verwendet (Tavani & Moor, 2001). Wenn beispielsweise gezeigt werden kann, dass sich große Teile des Datenverkehrs im Rahmen von Hidden Services im Tor-Netzwerk auf kinderpornografische Inhalte beziehen (Owen & Savage, 2015), dann erscheint ein solches Werkzeug, welches gemeinhin als wichtiges Hilfsmittel von politischen Aktivistinnen und Aktivisten zur Abwehr von staatlicher Repression angesehen wird, in einer ambivalenten Perspektive. Manchmal kann erst die Aufhebung der schützenden, bemäntelnden Wirkung des Privaten verdrängte, tabuisierte, diskriminierte oder normverletzende Sachverhalte in die Öffentlichkeit, in gesellschaftliche Diskussionsforen und politische Aushandlungsprozesse bringen (Cohen, 2012, Hagendorff, 2018).

Eine solche Verdeutlichung der Ambivalenz des Privaten darf jedoch nicht dazu führen, dass zwischen verschiedenen Werten eine Art Nullsummenspiel eröffnet wird und ein Wert gegen einen anderen ausgespielt wird. Meinungsfreiheit, Pressefreiheit, Sicherheit, Privatheit, das Recht auf den freien Zugang zu Informationen und andere Werte können zwar in einem Spannungsfeld zueinander stehen, die Realisierung von Wert A muss aber nicht zwingend die Verdrängung von Wert B bedeuten (Lever, 2015). Im Gegenteil entspricht die Aushandlung der Gewichtung unterschiedlicher Werte oder Rechtsgüter dem Wesen der Demokratie und spiegelt sich mit dem Prinzip der praktischen Konkordanz auch im Recht wider (Fischer-Lescano, 2008).

6 Zusammenfassung und Ausblick

Die Privatheitsforschung ist mittlerweile eine gut etablierte Disziplin an der Schnittstelle zwischen Technikanalyse, gesellschaftlichen, politischen, psychologischen, ökonomischen und kulturellen Perspektiven. Damit ist Privatheitsforschung ein interdisziplinäres Feld. Ethische Reflexionen sind für dieses Feld essenziell.

Ethik ist die kritische Reflexion und Analyse herrschender gelebter Moral, nicht nur im deskriptiven, sondern auch im präskriptiven Sinn. Dieses Verständnis von Ethik, das bis ins griechische 8. Jahrhundert v. Chr. zurück reicht, beruht auf der Voraussetzung, dass menschliches Leben nicht allein durch Gewohnheiten und Traditionen, aber auch nicht allein durch rechtliche Regelungen gelenkt werden kann. Aristoteles, der „Ethik“ als philosophische Disziplin einführt, geht

davon aus, dass jede menschliche Praxis, auch Gewohnheiten und Traditionen, einer theoretisch fundierten Reflexion zugänglich sind. Gerade deshalb ist es ethisch geboten, die gelebte individuelle Handlungspraxis nicht durch Verhaltensanalysen zum bestimmenden Maßstab für politische bzw. gesellschaftliche Entscheidungen zu machen. Der Einbezug von datengestützten Verhaltensanalysen kann nur dann demokratisch legitim sein, wenn sie Gegenstand eines ethischen, politischen und gesellschaftlichen Verständigungsprozesses bleiben und sich nicht als Steuerungsmittel verselbstständigen.

Wenn Ethik nicht deskriptiv, sondern präskriptiv arbeitet, stellt sie eine doppelte Frage: zum einen die Frage nach richtigem Handeln in Konfliktsituationen, und zum anderen die Frage nach dem „guten Leben" die häufig heißt: In welcher Gesellschaft wollen wir leben? Ethische Analysen sind für das Feld der Privatheit unerlässlich, weil sie die Werthaltigkeit des Konzepts Privatheit diskutieren und die Rolle von Privatheit für eine gute und lebenswerte Gesellschaft reflektieren. Aus dieser Perspektive ist Privatheit ein instrumenteller Wert, der es ermöglicht, dass andere Werte verwirklicht werden können:

Privatheit ist ein individueller Wert, der als Schutz grundlegender Werte wie Autonomie, körperliche Integrität und Würde fungiert, genauso auch Formen des Widerstands gegen repressive Öffentlichkeiten ermöglicht.

Privatheit ist ein Strukturmoment einer Gesellschaft, indem durch Privatheit in unterschiedlichen (räumlichen, zeitlichen, kulturellen Kontexten) ein je angemessener Informationsfluss etabliert und vorausgesetzt werden kann.

Privatheit ist – auf einer Metaebene – auch ein öffentlicher und kollektiver Wert, weil er konstitutiv ist für Praktiken demokratischer Teilhabe und Kritik und damit grundlegend ist für eine demokratische und gerechte Gesellschaft.

In all diesen Bereichen ist Privatheit grundsätzlich in Machtstrukturen eingebunden und bleibt darum ambivalent. Privatheit als individueller Wert ist Voraussetzung für die Entfaltung von Mündigkeit, kann aber genauso der Verschleierung von Hierarchien und Gewalt in „privaten" Bereichen dienen. Privatheit als Strukturmoment einer Gesellschaft, das ungleiche Kontexte unterschiedlich behandelt, schützt Einzelne und Gruppen, die sich in vielfältigen Öffentlichkeiten bewegen; sie kann aber zugleich dort, wo Kontexte zunehmend vielfältig, dynamisch und überlappend werden, falsche Sicherheiten produzieren. Privatheit als kollektiver Wert, der demokratische Teilhabe ermöglicht, kann gleichzeitig das Verdrängte, Tabuisierte, Diskriminierte in die Privatheit abdrängen, genau wie das moralisch Falsche oder Illegale durch den Rückzug ins Private dulden. Aufgrund der hohen Innovationsdichte in diesem Bereich und der raschen Fortschritte hinsichtlich der Leistungsfähigkeit informationstechnischer Systeme bedarf es einer kontinuierlichen Diskussion und Anpassung von Privat-

heitskonzepten und -prinzipien, um unter veränderten Bedingungen ihren Wert für die Demokratie zu sichern.

Wichtig ist an dieser Stelle, Privatheit nicht als ein statisches, sondern als ein dynamisches Konzept zu sehen, welches im Verhältnis zu digitalen Technologien aller Art eine permanente Neuaushandlung erfährt. Dabei bleibt die Frage nach Gerechtigkeit eine unterliegende Konstante. Sie fragt danach, auf welchen Ebenen der Mangel an Privatheit oder der Missbrauch von Privatheit Ungerechtigkeiten hervorbringt. Gerade dort, wo Privatheit kontinuierlich gefährdet ist, kann sie nur gestärkt werden, wenn sie als Privatheit in und für gerechte Kontexte und Ziele gedacht wird. Dafür ist es notwendig, dass Nutzer:innen in der Lage sind, ihr Handeln online zu beurteilen und die beabsichtigten Folgen mit unbeabsichtigten Nebenwirkungen abzuwägen. Es muss trotz immer komplexer werdender technischer Systeme stets ein Ziel sein, (lebenslang) Kompetenzen zu erwerben, anhand derer es möglich wird, unbeabsichtigte Handlungs(neben)folgen bestmöglich zu antizipieren (Heesen, 2020, S. 300). Solche Fragen der Medienmündigkeit oder Data Literacy können jedoch schnell zu Überforderungen privater Anwender:innen, aber auch von Unternehmen oder der öffentlichen Hand führen, wenn eine demokratiekonforme Techniknutzung nicht durch entsprechende Infrastrukturen gerahmt und normativ geprägt wird.

Literatur

Antidiskriminierungsstelle des Bundes. (Hrsg.) (2014). Zwischen Gleichgültigkeit und Ablehnung. Bevölkerungseinstellungen gegenüber Sinti und Roma. Expertise des Zentrums für Antisemitismusforschung und des Instituts für Vorurteils- und Konfliktforschung e.V.

Barlow, J. P. (1996). A declaration of the independence of cyberspace, electronic frontier foundation. https://www.eff.org/de/cyberspace-independence. Zugegriffen: 14. Okt. 2020.

Bell, D. (1991 [1963]). Veblen and the Technocrats: On the Engineers and the Price System. In: Ders.: *The Winding Passage: Sociological Essays and Journeys 1960–1980* (S. 69–90).

Belliger, A., & Krieger, D. J. (2018). *Network public governance. On privacy and the informational self*. Transcript.

Bonilla-Silva, E. (2017). *Racism without racists: Color-blind racism and the persistence of racial inequality in America* (5. Aufl.). Rowman & Littlefield.

Böschen, S., Huber, G., & König, R. (2016). Algorithmische Subpolitik: Big Data als Technologisierung kollektiver Ordnungsbildung? *Berliner Debatte Initial, 27*(4), 66–76.

Boyd, D., & Crawford, K. (2012). Critical questions for big data information: Provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication and Society, 15*(5), 662–679.

Boyd, D. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (Hrsg.), *A networked self: Identity, community, and culture on social network sites* (S. 39–58). Routledge.

Brey, P. (2010). Values in technology and disclosive computer ethics. In L. Floridi (Hrsg.), *The Cambridge handbook of information and computer ethics* (S. 41–58). Cambridge University Press.

Bundesverfassungsgerichturteil vom 15.12.1983, „Volkszählungsurteil".

Cairney, P. (2016). *The politics of evidence-based policy making*. Palgrave Macmillan UK. https://doi.org/10.1057/978-1-137-51781-4

Cavoukian, A. (2011). Privacy by design. The 7 foundational principles. Ontario, https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Zugegriffen: 21. Apr. 2021.

Cavoukian, A., Taylor, S., & Abrams, M. E. (2010). Privacy by design: Essential for organizational accountability and strong business practices. *Identity in the Information Society, 2*(3), 405–413. doi:https://doi.org/10.1007/s12394-010-0053-z.

Cohen, J. E. (2012). What Privacy is fsor. *Harvard Law Eeview, 126*, 1–24.

Cukier, K. N., & Mayer-Schoenberger, V. (2013). The rise of big data: How it's changing the way we think about the world. *Foreign Affairs, 92*(3), 28–40.

Davis, F. (1959). What do we mean by right to privacy. *South Dakota Law Review, 4*, 1–24.

Davis, J. L., & Jurgenson, N. (2014). Context collapse. Theorizing context collusions and collisions. *Information, Communication & Society, 17*(4), 476– 485.

Deleuze, G. (1992). Postscript on the societies of control. October 59, 3–7.

Ellul, J. (1964). *The technological society*. Knopf.

Epstein, R., & Robertson, R. E. (2015). The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. *Proceedings of the National Academy of Sciences, 112*(33), 4512–4521.

Etzioni, A. (1999). *The limits of privacy*. Basic Books.

Feinberg, J. (1980). A child's right to an open future. In: W. Aiken & H. LaFollette (Hrsg.), *Whose child? parental rights, parental authority and state power* (S. 124–153). Littlefield, Adams & Co.

Fischer-Lescano, A. (2008) Kritik der praktischen Konkordanz. *KJ/Kritische Justiz, 41*(2), 166–177. https://www.kj.nomos.de/fileadmin/kj/doc/2008/20082Fischer-Lescano_S_166.pdf. Zugegriffen: 19. Okt. 2020.

Fisher, W. R. (1987). *Human communication as narration: Toward a philosophy of reason, value, and action*. University of South Carolina Press.

Flaxman, S., Goel, S., & Rao, J. M. (2016). Filter bubbles, echo chambers, and online news consumption. *Public Opinion Quarterly 80*(Special Issue), 298–320.

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal, 89*(3), 421–471.

Habermas, J. (1987). *Theorie des kommunikativen Handelns* (Bd. 2). Suhrkamp.

Habermas, J. (1996). *Strukturwandel der Öffentlichkeit: Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft*. Suhrkamp.

Hagendorff, T. (2017). *Das Ende der Informationskontrolle. Zur Nutzung digitaler Medien jenseits von Privatheit und Datenschutz*. Transcript.

Hagendorff, T. (2018). Ambivalenz des Privaten. In: M. Friedewald (Hrsg.), *Privatheit und selbstbestimmtes Leben in der digitalen Welt. Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes* (S. 13–32). Springer.

Hagendorff, T. (2019). Post-privacy oder der Verlust der Informationskontrolle. In: H. Hauke Behrendt, W. Loh, T. Matzner, & C. Misselhorn (Hrsg.), *Privatsphäre 4.0* (S. 91–106). J.B. Metzler.

Hagendorff, T., Geminn, C. L., Lamla, J., Karaboga, M., Krämer, N., Nebel, M., & Uhlmann, M. (2020). Risiken künstlicher Intelligenz für die menschliche Selbstbestimmung. *Policy Paper*, 1–15.

Heesen, J. (2012a). Informationsethik und Technikphilosophie. In: P. Fischer, A. Luckner, & U. Ramming (Hrsg.), *Die Reflexionen des Möglichen. Zur Dialektik von Handeln, Erkennen und Werten* (S. 251–261). LIT-Verlag.

Heesen, J. (2012b). Preisgabe von Information und Konstituierung persönlicher Identität. In: C. R. Bartram, M. Bobbert, D. Dölling, T. Fuchs, G. Schwarzkopf, & K. Tanner (Hrsg.), *Der (un)durchsichtige Mensch. Wie weit reicht der Blick in die Person?* (S. 237–254). Universitätsverlag Winter.

Heesen, J. (2016). Freiheit. In J. Heesen (Hrsg.), *Handbuch Medien- und Informationsethik* (S. 52–58). Metzler.

Heesen, J. (2020). Verantwortlich Forschen mit und zu Big Data und Künstlicher Intelligenz. In: A. Seibert-Fohr (Hrsg.), *Entgrenzte Verantwortung. Zur Reichweite und Regulierung von Verantwortung in Wirtschaft, Medien, Technik und Umwelt* (S. 285–303). Springer.

Heesen, J., & I. Stapf (2021). Digitale Kommunikation: Medienethik, Medienkompetenz. In: M. Bobbert & J. Sautermeister (Hrsg.), *Handbuch Psychologie und Ethik*. Springer (i. Dr.).

Helbing, D. (u. a.) *Digitale Demokratie statt Datendiktatur*. Spektrum.de, 17. 12. 2015.

Helbing, D. (Hrsg.). (2019). *Towards digital enlightenment. Essays on the darf and light sides of the digital revolution*. Springer.

Kahn, J. (2003). Privacy as a legal principle of identity maintenance. *Seton Hall Law Review, 33*(2), 371–410.

Kant, Immanuel: AA VI, Die Metaphysik der Sitten. In: Kants gesammelte Schriften. Hrsg. von der königlich preussischen Akademie der Wissenschaften. Berlin: G. Reimer, 1900 ff.

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures & their consequences*.

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America, 110*(15), 5802–5805.

KPMG. (2019). Cloud-Monitor 2019. Public Cloud und Cloud Security sind kein Widerspruch. With assistance of bitkom research. https://hub.kpmg.de/cloud-monitor-2019.

Krafft, T. D., & Zweig, K. A. (2019). *Transparenz und Nachvollziehbarkeit algorithmenbasierter Entscheidungsprozesse* (S. 1–45). Berlin.

Lambiotte, R., & Kosinski, M. (2014). Tracking the digital footprints of personality. *Proc. IEEE, 102*(12), 1934–1939.

Lansdown, G. (2005). *The evolving capacities of the child*. UNICEF.

Lever, A. (2005). Feminism, democracy and the right to privacy. *Minerva – An Online Journal of Philosophy, 9*, 1–31.

Lever, A. (2012). *On privacy*. Routledge.
Lever, A. (2015). Privacy, democracy and freedom of expression. In: B. Rössler & D. Mokrosinska (Hrsg.), *Social dimensions of privacy. Interdisciplinary perspectives* (S. 162–180). Cambridge University Press.
Lischka, K., & Stöcker, C. (2017). *Digitale Öffentlichkeit. Wie algorithmische Prozesse den gesellschaftlichen Diskurs beeinflussen. Arbeitspapier* (S. 1–88). Bertelsmann Stiftung.
Livingstone, S., Stoilova, M., & Nandagiri, R. (2019). *Children's data and privacy online: Growing up in a digital age. An evidence review*. London School of Economics and Political Science.
Lyon, D. (2001). *Surveillance society. Monitoring everyday life*. Open University Press.
Mackenzie, C., & Stoljar, N. (Hrsg.). (2000). *Relational autonomy: Feminist perspectives on autonomy, agency, and the social self*. Oxford University Press.
MacKinnon, C. A. (1989). *Toward a feminist theory of the state*. Harvard University Press.
Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics. From an individual to a collective dimension of data protection. *Computer Law & Security Review, 32*(2), 238–255. doi:https://doi.org/10.1016/j.clsr.2016.01.014.
Marwick, A., & Boyd, D. (2011). I Tweet honestly, I Tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society, 13*(1), 1–20.
Matz, S. C., Appel, R. E., & Kosinski, M. (2019). Privacy in the age of psychological targeting. *Current Opinion in Psychology, 31*, 116–121.
Maywald, J. (2012). *Kinder haben Rechte! Kinderrechte kennen – umsetzen – wahren*. Beltz/Juventa.
Moore, A. (2008). Defining privacy. *Journal of Social Philosophy, 39*(3), 411–428.
Nash, J. C. (2005). From lavender to purple: Privacy, black women, and feminist legal theory, 11 Cardozo Women's L. J (S. 303–330).
Nissenbaum, H. (2010). *Privacy in context. Technology, policy, and the integrity of social life*. Stanford University Press.
Ochs, C. (2019). *Teilnahmebeschränkungen und Erfahrungsspielräume: Eine negative Akteur-Netzwerk-Theorie der Privatheit*. In: H. Behrendt, W. Loh, T. Matzner, & C. Misselhorn (Hrsg.). *Privatsphäre 4.0. Eine Neuverortung des Privaten im Zeitalter des Digitalen* (S. 13–31). Metzler.
Olsen, F. E. (1993). The family and the market. A study of ideology and legal reform. In P. Smith (Hrsg.), *Feminist Jurisprudence* (S. 65–93). Oxford University Press.
O'Neil, C. (2016). *Weapons of math destruction. How big data increases inequality and threatens democracy*. Crown Publishers.
Owen, G., & Savage, N. (2015). The tor dark net. Global commission on internet governance, Nr. 20. https://www.cigionline.org/sites/default/files/no20_0.pdf. Zugegriffen: 21. Apr. 2021.
Parent, W. A. (1983). Privacy, morality, and the law. *Philosophy & Public Affairs, 12*(4), 269–288.
Pariser, E. (2011). *The filter bubble. What the internet is hiding from you*. The Penguin Press.
Platon. (2012). *Der Staat. Bibliographisch ergänzte Ausgabe von 2000*. Reclam.
Pörksen, B., & Detel, H. (2012). *Der entfesselte Skandal. Das Ende der Kontrolle im digitalen Zeitalter*. Herbert von Halem Verlag.
Regan, P. M. (1995). *Legislating privacy. Technology, social values, and public policy*. University of North Carolina Press.

Regan, P. M. (2015). Privacy and the common good: Revisited. In B. Rössler & D. Mokrosinska (Hrsg.), *Social dimensions of privacy. Interdisciplinary perspectives* (S. 50–70). Cambridge University Press.

Richter, P. (2015). Big data und demokratische Willensbildung aus verfassungsrechtlicher Sicht. In P. Richter (Hrsg.), *Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data* (S. 45–68). Nomos.

Rössler, B. (2001). *Der Wert des Privaten*. Frankfurt a. M.

Rød, E. G., & Weidmann, N. B. (2015). Empowering activists or autocrats? The internet in authoritarian regimes. *Journal of Peace Research, 52*(3), 338–351.

Schneier, B. (2015). Data and goliath. The hidden battles to collect your data and control your world. W. W. Norton & Company.

Seemann, M. (2014). *Das Neue Spiel. Strategien für die Welt nach dem digitalen Kontrollverlust*. orange-press.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Solove, D. J. (2015). The meaning and value of privacy. In B. Rössler, & D. Mokrosinska (Hrsg.), *Social dimensions of privacy. Interdisciplinary perspectives* (S. 71–81). Cambridge University Press.

Stanley, J. (2019). The dawn of robot surveillance; AI, video analytics, and privacy. American Civil Liberties Union. https://www.aclu.org/sites/default/files/field_document/061119-robot_surveillance.pdf. Zugegriffen: 02. Nov. 2020.

Stapf, I. (2020). Kindliche Selbstbestimmung in digitalen Kontexten – medienethische Überlegungen zur Privatsphäre von Heranwachsenden. In F. Buck, J. Drerup, & G. Schweiger (Hrsg.), *Neue Technologien – neue Kindheiten? Ethische und bildungsphilosophische Perspektiven*. Metzler.

Stapf, I. (2016). Freiwillige Medienregulierung. In J. Heesen (Hrsg.), *Handbuch Informations- und Medienethik* (S. 96–104). Metzler.

Stapf, I. (2018). Kindliche Selbstbestimmung in der digital vernetzten Welt: Kinderrechte zwischen Schutz, Befähigung und Partizipation mit Blick auf „evolving capacities". In *merzWissenschaft Kinder\Medien\Rechte – Komplexe Anforderungen an Zugang, Schutz und Teilhabe im Medienalltag Heranwachsen- der. kopaed* (S. 7–18).

Stapf, I. (2019). Zwischen Selbstbestimmung, Fürsorge und Befähigung. Kinderrechte im Zeitalter mediatisierten Heranwachsens. In I. Stapf, M. Prinzing, N. Köberer (Hrsg.), *Aufwachsen mit Medien. Zur Ethik mediatisierter Kindheit und Jugend* (S. 69–84). Nomos.

Susser, D., Roessler, B., & Nissenbaum, H. F. (2018). Online Manipula tion: Hidden Influences in a Digital World. *SSRN Journal*, 1–38.

Tillmann, A., & Hugger, K.-U. (2014). Mediatisierte Kindheit – Aufwachsen in mediatisierten Lebenswelten. In H. Friedrichs, T. Junge, & U. Sander (Hrsg.), *Jugendmedienschutz in Deutschland* (S. 31–45). VS Verlag-Verlag.

Tufekci, Z. (2018). YouTube, the Great Radicalizer. New York Times. https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html. Zugegriffen: 02. Nov. 2020.

Vitak, J. (2012). The impact of context collapse and privacy on social network site disclosures. *Journal of Broadcasting & Electronic Media, 56*(4), 451–470.

Walzer, M. (1983). *Spheres of justice: A defense of pluralism and equality*. Basic Books.

Wesch, M. (2009). YouTube and you. Experiences of self-awareness in the context collapse of the recording Webcam. *Explorations in Media Ecology, 8*(2), 19–34.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Young, I. M. (1987). Impartiality and the civic public. In S. Benhabib & D. Cornell (Hrsg.), *Feminism as critique. On the politics of gender* (S. 56–76). University of Minnesota Press.
Zanouda u. a. (2017). *The quantified city*.
Zuboff, S. (2018). *Das Zeitalter des Überwachungskapitalismus*. Campus.

PD Dr. Jessica Heesen ist Leiterin des Forschungsschwerpunkts Medienethik und Informationstechnik am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen.

Prof. Dr. Regina Ammicht Quinn ist Professorin am und Sprecherin des Internationalen Zentrums für Ethik in den Wissenschaften (IZEW) der Universität Tübingen.

Andreas Baur ist wissenschaftlicher Mitarbeiter am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen und Doktorand an der Universiteit van Amsterdam.

Dr. Thilo Hagendorff ist Post-Doc am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) sowie am Exzellenzcluster „Machine Learning" der Universität Tübingen.

Dr. Ingrid Stapf ist Mitglied im Forum Privatheit und forscht am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen zu Themen der Informations- und Medienethik. Sie habilitiert sich zu einer Kinder-Medien-Ethik im digitalen Zeitalter.

Von Schutzbedürfnissen und Schutzverhalten

Eine medienpsychologische Analyse des individuellen Privatheitsschutzes

Yannic Meier, Judith Meinert und Nicole C. Krämer

Trotz wachsender gesetzlicher Maßnahmen zum Schutz personenbezogener Daten, wie zum Beispiel der Datenschutz Grundverordnung (DSGVO)[1], liegt die Hauptverantwortung zum Schutz der eigenen Daten noch immer bei den Nutzenden. Zwar schreibt die DSGVO vor, dass beispielsweise Gründe für das Erheben, die maximale Dauer der Speicherung, die Verwendung und Weitergabe personenbezogener Daten transparent von Unternehmensseite aus kommuniziert werden müssen, allerdings führen diese Vorschriften bei Internetfirmen wie Facebook, Google oder Amazon nicht dazu, dass weniger Daten über Nutzende gesammelt, verarbeitet und zu den verschiedensten Zwecken genutzt werden[2]. Folglich müssen Nutzerinnen und

[1] Roßnagel u. a. diskutieren in ihrem Kapitel in diesem Band mögliche Modernisierungen des Grundrechtsschutzes im Hinblick auf aktuelle und künftige Herausforderungen der Digitalisierung.

[2] Für eine Diskussion über den Nutzen einer datenschutz- und privatheitskonformen Gestaltung von Systemen vergleiche das Kapitel von Hansen u. a. in diesem Band.

Y. Meier (✉) · J. Meinert · N. C. Krämer
Universität Duisburg-Essen, Duisburg, Deutschland
E-Mail: yannic.meier@uni-due.de

J. Meinert
E-Mail: judith.meinert@uni-due.de

N. C. Krämer
E-Mail: nicole.kraemer@uni-due.de

A. Roßnagel und M. Friedewald (Hrsg.), *Die Zukunft von Privatheit und Selbstbestimmung,* DuD-Fachbeiträge,
https://doi.org/10.1007/978-3-658-35263-9_6

Nutzer noch selbst aktiv werden, wenn sie den Datensammelpraktiken im Internet entkommen wollen. Die Möglichkeiten sind mannigfaltig, jedoch hängt deren Nutzen stark von der jeweilig getroffenen individuellen Schutzmaßnahme ab. So können beispielsweise Werbeblocker vor bestimmten Verfahren der Nutzendenverfolgung (Tracking) schützen, Anonymisierungstools (z. B. Tor-Browser) verschleiern die Identität der Nutzenden beim Browsen und der Umstieg von Google auf datenschutzfreundliche Suchmaschinen hinterlässt weniger Spuren im Netz. Allerdings lassen sich nicht alle Online-Privatheitsrisiken durch die Anwendung von protektiven Maßnahmen verhindern, sondern nur bis zu einem gewissen Grad reduzieren. Einige soziale Netzwerke wie zum Beispiel Facebook sammeln nicht nur Verhaltensdaten ihrer Nutzenden, sondern auch Daten von Nicht-Nutzenden über Drittwebsites. Das hieße, dass beispielsweise die Maßnahme, Facebook nicht zu nutzen, um besser geschützt zu sein, nur eingeschränkt zur Erreichung dieses Ziels beiträgt. Eine zusätzliche Software, die das Tracking durch soziale Medien verhindert, wäre außerdem nötig. Dieses Beispiel dient als Illustration für das sehr komplexe Feld des Selbstdatenschutzes. Der aktuelle Beitrag nähert sich diesem Themengebiet aus psychologischer Perspektive und ist wie folgt gegliedert: zunächst wird anhand verschiedener empirischer Befunde gezeigt, welche protektiven Maßnahmen von Internetnutzenden angewendet werden und welche eher unbeachtet bleiben. Dann werden psychologische Motive und Bedürfnisse als Gründe für den Selbstdatenschutz erörtert. Schließlich wird betrachtet, welche positiven oder eventuell sogar negativen Auswirkungen die Nutzung bestimmter protektiver Maßnahmen haben kann und welche weiteren Interventionen oder Schutzmaßnahmen aus psychologischer Sicht wünschenswert wären, um Nutzende im Rahmen ihres Selbstdatenschutzes besser zu unterstützen. Der Beitrag rekurriert dabei vor allem auf eigene Studien, die wir finanziert durch das Forum Privatheit zwischen 2017 und 2020 durchgeführt haben.

1 Übersicht über empirische Arbeiten

Um einen Überblick über die für diesen Beitrag relevanten empirischen Arbeiten zu erhalten, werden in Tab. 1 alle Studien mit einer kurzen Beschreibung der Methode, zentrale Ergebnisse der Untersuchung sowie die Stichprobengröße dargestellt. Noch nicht alle der Studien sind veröffentlicht und zusätzlich wird zum Teil auf Ergebnisse verwiesen, die nicht Teil der bereits veröffentlichten Manuskripte sind. Um dennoch eine eindeutige Zuordnung der aufgeführten Ergebnisse zu den Studien zu ermöglichen, werden diese in der Tabelle durchnummeriert.

Tab. 1 Übersicht über die im Kapitel verwendeten Studien

Studie	Methode	*N*	Zentrale Ergebnisse zum Thema Privatheitsschutz
I[a]	Kulturvergleich-Fragebogen	1060	Amerikaner:innen wenden mehr schützende Verhaltensweisen an als Deutsche
II[n]	Langzeitstudie mit 3 Messzeitpunkten	1790	Teilnehmende wenden im Schnitt 3 Schutzstrategien an; Zahl über 3 Messzeitpunkte im Abstand von 6 Monaten konstant; am häufigsten werden einfach zu etablierende Maßnahmen angewandt
III[b]	Experimentelle Studie	511	Sehr hoher Wunsch nach besserem Privatheitsschutz in der Stichprobe; Schutzwunsch hängt positiv mit der Intention, ein privatheitsschützendes Tool zu verwenden zusammen; Nutzungsintention hängt positiv mit der Wahrnehmung von Kontrolle über die eigenen Daten während der Nutzung zusammen[z]
IV[c]	Experimentelle Studie	304	Warnmeldungen hatten keinen Einfluss auf Schutzmotivation; wahrgenommene Privatheitsrisiken sowie die wahrgenommene Effektivität des Schutzverhaltens beeinflussen die Schutzmotivation positiv; Privatheitszynismus hatte einen positiven Effekt auf die Schutzmotivation[z]
V[d]	Experimentelle Studie	305	Negativer Zusammenhang zwischen wahrgenommenen Nutzungsvorteilen eines sozialen Netzwerkes und dem Privatheitsschutz
VI[n]	Experimentelle Studie	485	Transparenz über potentielle Privatheitsrisiken des Teilens von Informationen auf verschiedenen Websites senkt die wahrgenommenen Vorteile der Preisgabe und erhöht die wahrgenommenen Risiken; Die Intention, persönliche Informationen preiszugeben, sinkt mit höheren Risiken
VII[e]	Fragebogen	441	Teilnehmende haben ein sehr geringes Wissen über verschiedene Web-Tracking Verfahren; das Informieren der Teilnehmenden über die unterschiedlichen Verfahren führt zu höheren Privatheitssorgen, einer schlechteren Selbsteinschätzung der eigenen Fähigkeiten sowie einer schlechteren Einschätzung des getätigten Schutzverhaltens

[n]nicht veröffentlichte Studie, [z]zusätzliche Rechnung, die nicht im Manuskript erschienen ist/erscheinen wird, [a] (Neubaum et al., 2020), [b] (Meier et al., 2021), [c] (Meier et al., 2020b), [d] (Meier et al., 2020a), [e](Ammicht Quinn et al., 2018)

2 Nutzungs- und Schutzverhalten

Bevor geklärt werden kann, welche Einflussfaktoren dazu führen, dass Personen ihre persönlichen Daten online besser schützen und welche Effekte die Anwendung bestimmter protektiver Maßnahmen haben kann, muss zunächst das grundsätzliche Nutzungsverhalten bekannt sein, das heißt, welche Schutzmaßnahmen in welchem Ausmaß verbreitet sind. Um einen besseren Gesamteindruck zu erhalten, werden sowohl eigene empirische Arbeiten als auch Studien anderer Wissenschaftler:innen herangezogen.

Eine Einteilung von Privatheitsschutzverhalten lässt sich generell an der Unterscheidung einer vertikalen und einer horizontalen Privatheitsdimension treffen (Debatin, 2011; Masur, 2018). Die vertikale Dimension beschreibt dabei den Informationsfluss zwischen einem Individuum und einer höher gestellten Instanz, z. B. einem Unternehmen oder einer Regierungseinrichtung. Verletzungen der Privatheit entstehen, wenn ein Unternehmen oder eine Institution unerlaubt und/oder unbemerkt private Daten einer Person sammelt, speichert und verwendet. Die horizontale Dimension beschreibt den Informationsfluss zwischen Individuen, vor allem gleichgestellter Peers. Dementsprechend gehen Privatheitsrisiken auf der horizontalen Ebene von anderen Individuen aus, zum Beispiel durch das unerlaubte Weiterverbreiten privater Informationen (Masur, 2018). Auf beiden Dimensionen gibt es unterschiedliche Strategien, die angewendet werden können, um die entsprechenden persönlichen Informationen vor unerlaubtem Zugriff zu schützen. Um private Daten vor anderen Personen zu schützen, hilft die Nutzung von Privatsphäreeinstellungen, beispielsweise in sozialen Netzwerken. Privatheitsschutz auf der vertikalen Ebene ist häufig schwieriger, da viele Internetunternehmen Verfahren der Nutzendenverfolgung (Tracking) einsetzen. Hierbei kann man auf die Nutzung verschiedener Tools (z. B. zur Anonymisierung, Verschlüsselung, Anti-Tracking Software) zurückgreifen oder auf die Nutzung bestimmter Dienste verzichten. Diese beiden letztgenannten Strategien werden von Matzner et al. (2016) wiederum eingeteilt in aktive und passive Strategien. Passive Strategien beschreiben dabei solche, die auf Datensparsamkeit oder der Nicht-Nutzung von Services beruhen. Aktiver Privatheitsschutz hingegen ist die Nutzung von Software zum besseren Schutz sowie der Rückgriff auf rechtliche Möglichkeiten (z. B. die Löschung aller personenbezogener Daten, die ein Unternehmen gesammelt hat).

In verschiedenen Studien zeigt sich das Bild, dass die am häufigsten genutzten Schutzmaßnahmen relativ einfach anzuwendende Strategien beinhalten, wohingegen die Nutzungshäufigkeit mit der Komplexität und dem Anwendungsaufwand deutlich

abnimmt (Boerman, 2018; Matzner et al., 2016). In einer noch nicht veröffentlichten Studie mit einer für die deutsche Bevölkerung repräsentativen Stichprobe von 1790 Internetnutzenden mit drei Messzeitpunkten fanden wir heraus, dass die vier am häufigsten genutzten Schutzmaßnahmen Selbstbeschränkung, das Löschen des Browser-Verlaufs, das Löschen von Cookies/des Caches und die Nicht-Nutzung bestimmter Dienste waren (s. Abb. 1). Von knapp einem Viertel der Befragten wurde das Angeben eines falschen Namens sowie der Einsatz von Anti-Tracking Software

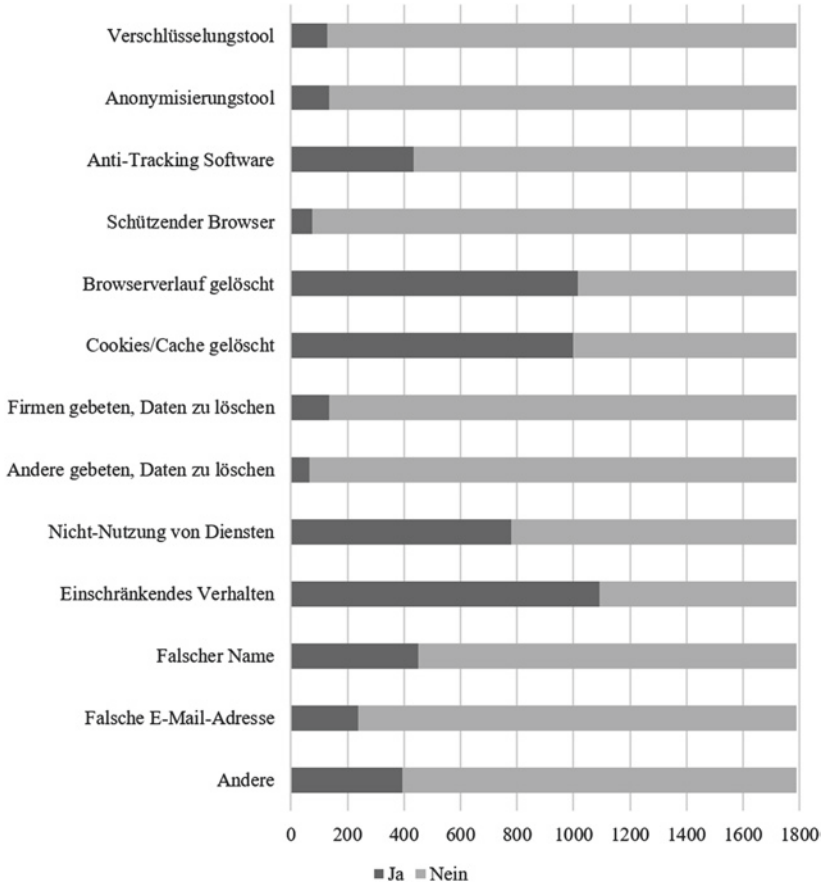

Abb. 1 Absolute Anzahl der Nutzung verschiedener Schutzmaßnahmen von N = 1790 Internetnutzenden. (Durchschnittlicher Wert über drei Erhebungszeitpunkte)

genannt. Tools und Software zur Anonymisierung und Verschlüsselung wurden dagegen nur selten genutzt. Außerdem zeigte sich, dass die Befragten über alle drei Messzeitpunkte hinweg im Schnitt etwa drei verschiedene protektive Maßnahmen nutzten ($M_{t1}=3{,}07$, $SD_{t1}=2{,}07$, $M_{t2}=3{,}08$, $SD_{t2}=2{,}03$, $M_{t3}=3{,}14$, $SD_{t3}=2{,}07$). Diese Ergebnisse decken sich mit einer Studie einer repräsentativen niederländischen Stichprobe (Boerman, 2018) sowie einer weiteren repräsentativen Stichprobe aus Deutschland (Matzner et al., 2016). Die Studien zeigten ebenfalls, dass am häufigsten einfache Methoden genutzt wurden, wie beispielsweise das Löschen von Cookies und des Caches, das Nicht-Nutzen bestimmter Websites oder regelmäßige Updates von Anti-Viren Programmen. Die Nutzung zusätzlicher Software zur Verschleierung der eigenen Anonymität oder von Anti-Tracking Software ist auch in diesen Studien deutlich geringer. Am wenigsten oft wurden Anti-Tracking Software, die Do-Not-Track Funktion des Browsers genutzt oder Internetfirmen gebeten, persönliche Daten zu löschen. Diese Ergebnisse legen den Schluss nahe, dass einfach anzuwendende Schutzmaßnahmen am populärsten sind und die Nutzungsbereitschaft sinkt, je mehr Aufwand betrieben werden muss, um die Maßnahme anzuwenden. Außerdem zeigt sich, dass sowohl passive (z. B. einschränkendes Verhalten) als auch aktive (z. B. Löschung von Cookies) Strategien genutzt werden. Allerdings sollten diese Ergebnisse nicht nur mit dem zu betreibenden Aufwand erklärt werden. Im nachfolgenden Abschnitt gehen wir auf verschiedene Einflussfaktoren ein, die als Erklärung herangezogen werden können.

Soziale Netzwerke wie Facebook und Instagram stellen einen Sonderfall beim Privatheitsschutz dar. Auf diesen Plattformen ist das primäre Ziel der Datenpreisgabe die Kommunikation mit anderen Nutzerinnen und Nutzern. Demnach muss man einerseits darauf bedacht sein, dass man sich so gut wie möglich vor den Datensammelpraktiken sozialer Netzwerke schützt und andererseits darauf, dass man sich nicht Privatheitsrisiken durch andere Personen aussetzt. Wie eingangs bereits erwähnt wird hierbei eine Unterscheidung zwischen einer vertikalen und einer horizontalen Privatheitsdimension getroffen (Debatin, 2011; Masur, 2018). In Studie IV mit 304 Facebook Nutzenden fanden wir heraus, dass der Großteil der Befragten persönliche Informationen auf Facebook preisgegeben, Fotos von sich hochgeladen und auch Beiträge verfasst hat. Auf der anderen Seite gaben aber viele Befragte auch an, dass sie einige Schutzmaßnahmen ergriffen hatten, wie zum Beispiel Facebook untersagt, dass persönliche Informationen für Werbezwecke genutzt werden sollen, dass Facebook den Standort aufzeichnen oder die automatische Gesichtserkennung anwenden darf oder die Funktion, dass das eigene Profil über Suchmaschinen gefunden werden kann, abgestellt (s. Abb. 2). Auffällig war, dass sich die Proband:innen sehr sicher waren, ob sie schon einmal Informationen, Fotos oder Beiträge preisgegeben beziehungsweise verfasst

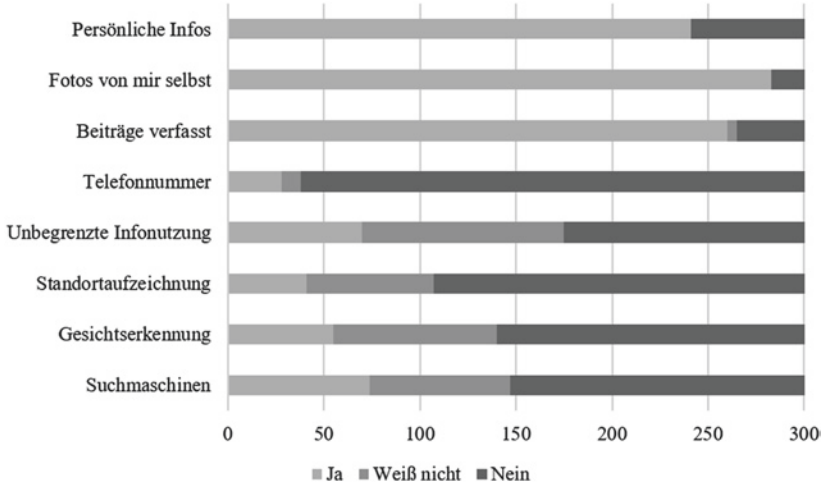

Abb. 2 Privatheitsverhalten auf Facebook (N = 304). Wurden persönliche Informationen, Fotos, Beiträge oder die eigene Telefonnummer auf Facebook preisgegeben/veröffentlicht? Wurde Facebook die unbegrenzte Nutzung der eigenen Informationen, die Standortaufzeichnung, Gesichtserkennung und das Finden durch Suchmaschinen erlaubt?

haben, der Unsicherheitsfaktor (in Form der „ich weiß nicht"-Option) bei den protektiven Maßnahmen jedoch sehr hoch war. Diese Beobachtung lässt den Schluss zu, dass Schutzmaßnahmen nicht in dem Maße salient sind, wie die Preisgabe von Informationen, und dass sich viele befragte Personen nicht gut beim Schutz ihrer Privatsphäre auf Facebook auskennen. Dies kann daran liegen, dass die Privatsphäreeinstellungen auf Facebook regelmäßigen Updates unterliegen, sodass teilweise alte Optionen verschwinden, neue hinzukommen und sich alte Einstellungen per „default" auf die niedrigste Schutzstufe stellen. Daher ist es nicht ausreichend, einmalig eine für sich selbst geeignete Einstellung zu finden. Vielmehr sollte jede Nutzerin und jeder Nutzer in regelmäßigen Abständen die eigenen Schutzeinstellungen überprüfen und gegebenenfalls anpassen. Nur so kann garantiert werden, dass die Facebook-Privatsphäreeinstellungen den eigenen Vorstellungen entsprechen. In Studie V baten wir die Teilnehmenden ($N = 305$), sich auf einer (von uns erstellten) sozialen Netzwerkplattform zu registrieren. Bei der Registrierung konnten die Teilnehmenden die verschiedensten Informationen von sich preisgeben. Nach diesem Registrierungsprozess mussten alle Proband:innen einstellen, für wen die eben preisgegebenen Informationen sichtbar sein sollen. Die Optionen waren, angelehnt an die Optionen auf Facebook,

„nur ich“, „ausgewählte Personen“, „Freunde“, „Freunde von Freunden“ und „alle“. Fast die Hälfte der Befragten (47,5 %) entschied sich dazu, ihre Informationen vollkommen privat zu halten, sodass sie nur für die Person selbst zu sehen sei. Etwa ein Viertel (23 %) wählten „Freunde“ aus und nur 16 % machten ihre Informationen vollständig öffentlich einsehbar. Es zeigte sich außerdem, dass Personen, die die Nutzung der Plattform als besonders vorteilhaft ansahen, dazu tendierten, lockerere Privatsphäreeinstellungen zu wählen. Außerdem bestand ein Zusammenhang mit der Menge an preisgegebenen Informationen: je mehr preisgegeben wurde, desto weniger privat wurden die Einstellungen gewählt. Dieses Ergebnis lässt sich mit dem sogenannten Privacy Calculus Ansatz erklären (Culnan & Armstrong, 1999). Dieser Ansatz geht davon aus, dass die Informationspreisgabe maßgeblich von der Wahrnehmung der Vorteile, die mit der Preisgabe persönlicher Informationen assoziiert werden, und der Wahrnehmung der Privatheitsrisiken, die antizipiert werden, abhängt. Die Restriktion der offenbarten Information durch Privatheitseinstellungen könnte die antizipierten Vorteile folglich gefährden, weshalb weniger strikte Einstellungen gewählt werden.

Die bisher zusammengefassten Daten aus unseren Studien beziehen sich auf eine deutsche Population. Da es aber denkbar und wahrscheinlich ist, dass sich hinsichtlich des Privatheitsverhaltens und spezifischer des Schutzverhaltens Unterschiede zwischen verschiedenen Kulturen finden, haben wir eine Studie durchgeführt, in der das Schutzverhalten von Deutschen ($N = 521$) mit dem von Amerikaner:innen ($N = 539$) verglichen wurde (Neubaum et al., 2020). Basierend auf der Theorie von Petronio (Petronio, 2002) wurden dabei vor allem die kulturell vorherrschenden Normen als Mediatoren erhoben. Überraschenderweise und entgegen der Hypothesen zeigte sich dabei, dass Amerikaner:innen mehr Maßnahmen nutzen, um ihre Privatsphäre zu schützen als Deutsche. Dies ist vor allem vor dem Hintergrund unerwartet, da bisherige Studien überwiegend gezeigt haben, dass Deutsche durchaus besorgter um ihre persönlichen Daten sind als US-Bürger:innen (Krasnova & Veltri, 2010). Erklärbar wird dies aber einerseits dadurch, dass Amerikaner:innen auch wesentlich mehr persönliche Informationen preisgeben (und daher mehr Schutz erforderlich ist) sowie außerdem ausgeprägtere Normen, sich zu schützen, vorherrschen. Zusätzlich sind Nutzende in Deutschland und Europa von vornherein besser durch die DSGVO geschützt. Insgesamt lassen sich somit schon bei der Betrachtung des Verhaltens verschiedene Randbedingungen für ein Zustandekommen von Schutzverhalten identifizieren: So werden komplexere und aufwendigere Schutzmaßnahmen seltener angewendet, eine geringe Salienz der Schutzmaßnahmen kann zu Unsicherheit in Bezug auf den Privatheitsstatus führen, die Wahrnehmung von Gratifikationen im Sinne der Vorteile der Plattform kann zu einer Erhöhung der Kommunikation

und einer Vernachlässigung des Privatheitsschutzes führen und das Vorherrschen gesellschaftlicher Normen kann das Schutzverhalten beeinflussen, ebenso wie der gesetzliche Rahmen.

3 Einflussfaktoren: Motive und Bedürfnisse

Im vorherigen Abschnitt wurde deutlich, dass Internetnutzerinnen und -nutzer dazu tendieren, einfache Schutzstrategien anzuwenden. Außerdem werden nur sehr wenige verschiedene Schutzmaßnahmen angewandt. In einer unserer Studien (II) fanden wir heraus, dass die Teilnehmenden nur etwa drei verschiedene Maßnahmen nutzten. Boerman, Kruikemeier u. a. (Boerman, 2018) stellten in ihrer Untersuchung fest, dass die Proband:innen im Durchschnitt nur zwei bis zweieinhalb Schutzmaßnahmen verwendeten. Aus diesen deskriptiven Beobachtungen lassen sich verschiedene Fragestellungen ableiten. Welche Faktoren können als Erklärung dafür dienen, dass Personen eher einfache als komplexe Schutzstrategien nutzen? Welche Faktoren beeinflussen, ob man viele verschiedene oder aber nur sehr wenige bis gar keine Maßnahmen ergreift? Dieser Abschnitt beschäftigt sich daher mit empirischen Erkenntnissen und theoretischen Überlegungen zu Motiven und Einflussfaktoren, die sich in positiver oder negativer Weise auf das persönliche Schutzverhalten oder die Schutzintention auswirken. Dazu wird, wie im vorherigen Abschnitt auch, sowohl auf eigene aber auch auf Studien von anderen Wissenschaftler:innen zurückgegriffen, um einen umfassenderen Gesamteindruck zu vermitteln.

3.1 Schutzmotivation

Bei der Untersuchung der Einflussfaktoren von Schutzverhalten scheint die Schutzmotivationstheorie (Rogers, 1975, 1983) ein vielversprechender Ansatz zu sein. Diese Theorie, die ihren Ursprung im Gesundheitsbereich findet, geht davon aus, dass Furcht ein guter Motivator ist, schützendes Verhalten zu ergreifen. Dementsprechend beschreibt die Schutzmotivationstheorie, wie Furchtappelle gestaltet sein sollten, damit sich Personen bestmöglich vor schädlichem Verhalten schützen. Die Theorie beschreibt zwei verschiedene kognitive Prozesse, deren Ausgang entscheidend dafür ist, ob man motiviert ist, schützendes Verhalten zu zeigen oder nicht (Rogers, 1983). Der erste Prozess beinhaltet die Bewertung der Gefahr selbst. Hierbei ist es entscheidend, dass sowohl die Schwere der Gefahr (zum Beispiel für die eigene Gesundheit) als auch die eigene Anfälligkeit oder

Verwundbarkeit gegenüber der Gefahr als hoch bewertet werden, damit die Wahrscheinlichkeit für schützendes Verhalten steigt. Demgegenüber steht die positive Bewertung des gefährlichen Verhaltens in Form von Vorteilen oder Belohnungen. Als Beispiel lässt sich das Rauchen aufführen. Personen, die es als sehr wahrscheinlich ansehen durch das Rauchen an Lungenkrebs zu erkranken und Lungenkrebs als gefährlich bewerten, werden wahrscheinlich das schädliche Verhalten unterlassen. Personen, die allerdings primär positive Aspekte wahrnehmen (z. B. Dopaminausschüttung durch Nikotin) und die Gefahr, durch das Rauchen ernsthaft zu erkranken, unterschätzen, werden wenig gewillt sein, ihr gesundheitsschädliches Verhalten zu ändern. Neben der Bewertung der Gefahr muss allerdings auch die Bewältigung des Schutzverhaltens bewertet werden (Rogers, 1983). Hierbei spielen drei verschiedene Komponenten eine Rolle: die Einschätzung der Wirksamkeit des Schutzverhaltens, die Einschätzung, dass man in der Lage ist, das Schutzverhalten auszuführen (Selbstwirksamkeit) und die wahrgenommenen Kosten, die mit dem Schutzverhalten assoziiert werden (z. B. zeitliche Kosten). Bezogen auf das Beispiel des Rauchens, hieße das, dass Personen das Nichtrauchen als wirksamen Schutz vor beispielsweise Lungenkrebs ansehen müssen, dass sie es sich zutrauen müssen, mit dem Rauchen aufzuhören und dass sie die entstehenden Kosten (z. B. Nebenwirkungen, Gewichtszunahme) als nicht zu hoch einschätzen dürfen, damit sie motiviert sind, mit dem Rauchen aufzuhören. Laut Rogers (Rogers, 1983) müssen sowohl die Einschätzung der Gefahr als auch die Einschätzung der Bewältigung der Gefahr hoch sein, damit Menschen schützendes Verhalten zeigen. Diese kognitiven Mechanismen konzeptualisiert Rogers als Grundlage für die Gestaltung von Furchtappellen. Furchtappelle sollten demnach die potentielle Gefahr beschreiben, eine Einschätzung darüber geben, wie wahrscheinlich die Gefahr auftritt und ein geeignetes Schutzverhalten vorschlagen. So konnte bisherige Studien zum Beispiel zeigen, dass Furchtappelle die Intention, Alkohol zu trinken reduzieren können (Stainback & Rogers, 1983) und die Motivation mit dem Rauchen aufzuhören steigern können (Rogers & Deckner, 1975).

Diese Theorie findet mehr und mehr Einzug in Bereiche außerhalb des Gesundheitskontextes, so zum Beispiel ins Gebiet der Online-Privatheit (z.B. Boerman et al., 2018). In Studie IV nutzten wir die verschiedenen Komponenten der Schutzmotivationstheorie, um die Motivation, die eigene Privatsphäre auf Facebook zu schützen, zu untersuchen. Die Ergebnisse der Studie zeigten, dass wahrgenommene Privatheitsrisiken einen positiven Effekt auf die Schutzintention hatten. Darüber hinaus zeigte sich, dass Personen, die die Empfehlung des Tools, die Privatsphäreeinstellungen regelmäßig zu kontrollieren und anzupassen, als wirksame Gegenmaßnahme gegen Privatheitsrisiken ansahen, ebenfalls eine

höhere Schutzmotivation aufwiesen. Somit konnte die Studie Hinweise dafür finden, dass wichtige Komponenten der Schutzmotivationstheorie – die Gefahrenbewertung und die Bewertung der Gegenmaßnahme – mit der Intention, die eigene Privatsphäre auf Facebook in Zukunft besser zu schützen, zusammenhängen.

3.2 Resignation

Rogers (Rogers, 1975) beschreibt in der Schutzmotivationstheorie das Szenario, dass Menschen, die sich nicht in der Lage fühlen, sich vor einem potentiellen Risiko wirksam zu schützen, in einen Zustand der Resignation verfallen und folglich eine sehr geringe Schutzmotivation aufweisen. Aufbauend auf verwandten Überlegungen untersuchten Hoffmann et al. (2016), welchen Einfluss Resignation auf das Privatheitsschutzverhalten hat. Sie erfassten Resignation als eine Subfacette des breiteren Konstruktes des Privatheitszynismus. Die Autor:innen definieren Privatheitszynismus als Einstellung, die Unsicherheit, Machtlosigkeit und Misstrauen gegenüber dem Umgang persönlicher Daten von Online-Firmen umfasst. Resignation beschreibt in diesem Zusammenhang die Einstellung, dass der Schutz persönlicher Daten im Internet sinnlos ist, es also keinen Unterschied mache, ob man Schutzmaßnahmen anwendet oder nicht. In einer repräsentativen Befragung fanden Hoffmann et al. (2016) heraus, dass Privatheitszynismus als generelles Konstrukt nicht mit der Anwendung von Privatheitsschutzmaßnahmen zusammenhängt, dass allerdings die Subfacette Resignation negativ mit dem Ausmaß des Schutzes der eigenen Online-Privatheit zusammenhängt. In Studie IV fanden wir heraus, dass Privatheitszynismus sogar positiv mit der Intention, die eigenen persönlichen Informationen auf Facebook zu schützen, zusammenhängt. Allerdings bestand kein Zusammenhang zwischen Zynismus und bisherigem Schutzverhalten. Diese Ergebnisse lassen vermuten, dass Personen, die sich generell machtlos bezüglich des Umgangs ihrer persönlichen Daten im Internet fühlen und Internetfirmen misstrauen, zwar eine leicht erhöhte Intention aufweisen, sich zu schützen, diese Intention allerdings nicht zwangsweise zu besserem Schutzverhalten führt. Personen, die zusätzlich allerdings der Meinung sind, es sei sinnlos, Schutzmaßnahmen anzuwenden, schützen sich tendenziell eher schlechter. Vorläufige Ergebnisse von Studie VI mit 485 Teilnehmenden deuten darauf hin, dass Personen, die der Meinung sind, es mache keinen Unterschied, sich zu schützen oder nicht, freizügiger bei der Preisgabe persönlicher Daten auf verschiedenen Websites sind. Zusammengefasst deuten die Ergebnisse dieser drei Studien darauf hin, dass eine negative Einstellung gegenüber dem Datenschutz sowie Resignation dazu führen können, dass sich Personen im

Internet schlechter vor Privatheitsrisiken schützen und mehr von sich preisgeben. Folglich ist es von großer Wichtigkeit, die Effektivität von Schutzmaßnahmen zu kommunizieren und zu zeigen, dass protektives Veralten keineswegs sinnlos ist, sondern einen signifikanten Einfluss auf die im Netz hinterlassenen Spuren hat.

3.3 Wunsch nach Privatheitsschutz

Menschen haben ein Bedürfnis nach Privatsphäre (Trepte & Masur, 2017). Obwohl sich die Empfindungen von Privatsphäre offline und online voneinander unterscheiden, gibt es auch online den Wunsch, dass persönliche Informationen geschützt sind. In Studie III fanden wir heraus, dass es in der Stichprobe einen außergewöhnlich hohen Wunsch nach besserem Schutz persönlicher Daten im Netz gab. Das Verlangen nach besserem Privatheitsschutz war dabei definiert als Wunsch, dass Websitebetreibende und Internetfirmen persönliche Daten vertraulich behandeln, nicht für Analyse- oder Werbezwecke nutzen, sie vor Missbrauch schützen und nicht an andere Parteien weitergeben. Empirisch zeigte sich, dass insbesondere die Nutzer:innen, die mit diesen Praktiken hohe Privatheitsrisiken assoziierten, sich wünschten, dass diese Praktiken unterlassen würden. In der Tat konnten wir einen Zusammenhang mit hoher Effektstärke zwischen den beiden Variablen beobachten. Dieses Ergebnis deutet darauf hin, dass die Wahrnehmung hoher Privatheitsrisiken mit dem Wunsch einhergeht, vor diesen Risiken geschützt zu sein. Darüber hinaus untersuchten wir in dieser Studie, ob Personen, die ein hohes Verlangen nach besserem Privatheitsschutz aufwiesen, eine höhere Motivation zeigten, ein hypothetisches privatheitsschützendes Browsertool zu nutzen. Dieses Tool wurde beschrieben als eine Mischung aus einer Privacy Enhancing und einer Transparency Enhancing Technology, also einer Technologie, die automatisch vor bestimmten privatheitsgefährdenden Verfahren schützt und gleichzeitig Nutzenden Informationen über die Verwendung ihrer Daten von besuchten Websites anbietet. Die Ergebnisse zeigten, dass die allgemeine Nutzungsbereitschaft des beschriebenen Tools hoch war und dass ein Zusammenhang zwischen dem Wunsch nach besserem Privatheitsschutz und der Nutzungsbereitschaft bestand. Dieser Zusammenhang war allerdings relativ gering, d. h., dass Personen, die einen hohen Wunsch nach besserem Schutz äußerten, nur leicht höher motiviert waren, das Tool zu nutzen, als Personen, die keinen hohen Wunsch nach besserem Schutz äußerten. Der Hälfte der Proband:innen wurde allerdings geschildert, dass das Tool persönliche Daten sammeln muss, um die persönlichen Daten besser zu schützen und personalisierte Informationen anbieten zu können. Der anderen Hälfte der Proband:innen wurde gesagt, dass

die Software keine persönlichen Informationen der Nutzende sammle. Es zeigte sich, dass der Zusammenhang zwischen dem Wunsch nach Schutz und der Intention, das Tool zu nutzen, nur bestand, wenn das Tool als nicht datensammelnd beschrieben wurde. Da den Proband:innen nicht näher erläutert wurde, wieso es notwendig sein kann, dass datenschutzfreundliche Tools persönliche Informationen von Nutzenden sammeln müssen, wäre hieraus abzuleiten, dass bei der Beschreibung solcher Tools in der Praxis darauf geachtet werden sollte, dass auf vollständige Transparenz gesetzt wird, indem genauestens erläutert wird, weshalb die Erfassung persönlicher Daten von privatheitsschützender Software notwendig und sogar vorteilhaft für Nutzende ist. Zusammengefasst zeigt sich hier, dass Menschen, die sich besseren Schutz ihrer Daten im Internet wünschen, dazu tendieren, Schutzstrategien anzuwenden.

3.4 Weitere Faktoren

Neben der Wahrnehmung von Privatheitsrisiken, der wahrgenommenen Effizienz des Schutzverhaltens sowie dem Wunsch nach besserem Privatheitsschutz gibt es zahlreiche weitere Faktoren, die die Bereitschaft, die eigene Online-Privatsphäre zu schützen, beeinflussen. Viele dieser Faktoren hängen dabei allerdings miteinander zusammen. So korreliert beispielsweise die Wahrnehmung von Privatheitsrisiken stark mit dem Wunsch nach besserem Privatheitsschutz, wie in Studie III deutlich wurde. Daher wird in diesem Abschnitt versucht, die bisher vorgestellten sowie weitere Faktoren in Oberkategorien einzuordnen, um ein besseres Verständnis zu erlangen, durch welche Faktoren Schutzverhalten ausgelöst oder gehemmt wird.

Ein solcher Faktor, der die Wahrscheinlichkeit, sich zu schützen, erhöht, ist das Erleben von negativen Erfahrungen – auch Privatheitsverletzung genannt. Mehrere Studien konnten zeigen, dass Nutzende sozialer Netzwerke ein protektiveres Privatheitsverhalten zeigten, wenn sie negative Privatheitserfahrungen gemacht hatten, wie z. B. das Erhalten feindlicher Nachrichten, Bedauern über das Teilen persönlicher Informationen oder Cyber-Mobbing (Christofides et al., 2012; Trepte et al., 2014). Negative Erfahrungen können zudem die Risikoeinschätzung erhöhen (Trepte et al., 2014). Christofides et al. (2012) fanden heraus, dass Jugendliche, die Privatheitsverletzungen erlebten, ein höheres Schutzverhalten durch Privatsphäreeinstellungen zeigten. Dieser Effekt wurde zudem moderiert durch das Wissen darüber, wie die Privatsphäreeinstellungen anzuwenden sind. Das bedeutet, dass sich Menschen, die negative Erfahrungen machen, insbesondere dann besser schützen, wenn sie

über ein hohes Wissen darüber verfügen, wie man sich besser schützen kann. Diese Beobachtung weist auf eine wichtige Interaktion hin: der Effekt von Faktoren, die generell mit einem höheren Schutzverhalten assoziiert werden, wie zum Beispiel antizipierte Privatheitsrisiken, ist durch das eigene Wissen sowie die eigenen Fähigkeiten begrenzt. Dieses Wissen und die damit einhergehende Fähigkeit zum Schutz der eigenen Daten wird Privatheitskompetenz genannt. Trepte et al. (2015) definieren Online-Privatheitskompetenz als faktisches sowie prozedurales Wissen über Online Privatheit. Die Autor:innen beschreiben Online-Privatheitskompetenz zudem als ein multi-dimensionales Konstrukt, das beispielsweise aus Wissen über institutionale Praktiken, technische Aspekte, Privatheitsrisiken oder Strategien zum Schutz der eigenen Privatheit besteht. Auch in einer Studie von Bartsch und Dienlin (2016) zeigte sich, dass Facebook-Nutzende mit höherer Privatheitskompetenz dazu tendierten, ihre Privatsphäre besser zu schützen. Außerdem fanden die Autor:innen positive Zusammenhänge zwischen der Privatheitskompetenz und der Intensität der Facebook-Nutzung sowie der Erfahrung in Hinblick auf die Regulation. Ähnliche Ergebnisse zeigten sich auch in einer Studie von Park (2011): das Ausmaß des Privatheitsschutzes sowohl auf horizontaler (sozialer) als auch auf vertikaler (institutionaler) Ebene hing positiv mit der Nutzungsintensität und -erfahrung und mit der Online Privatheitskompetenz (unterteilt in technische Fähigkeiten und Bewusstsein für und Verständnis von institutionellen Praktiken) zusammen. Darüber hinaus zeigten sich in dieser Studie Effekte von soziodemographischen Variablen. Ältere Personen und Frauen schienen sich weniger zu schützen, wobei diese Beobachtung für Frauen nur auf der institutionellen, vertikalen Ebene zutrifft. Generell sind die Befunde hinsichtlich soziodemographischer Variablen und dem Ausmaß an Privatheitsschutz widersprüchlich. Boerman et al. (2018) beispielsweise fanden keine Einflüsse von Alter und Geschlecht auf die angewandten Schutzmaßnahmen. Im Gegensatz dazu, zeigte sich in unserer Untersuchung (Studie II), dass bestimmte soziodemographische Variablen mit der Menge an angewandten Schutzmaßnahmen zusammenhingen. Die Analysen ergaben, dass sich jüngere Personen besser schützten (d. h. sie wandten mehr Maßnahmen an) als ältere Personen. Darüber hinaus schienen sich Männer in größerem Umfang zu schützen als Frauen. Letztlich hatte auch die Internetnutzung einen Einfluss auf das Schutzverhalten: je länger die befragten Personen angaben, das Internet pro Tag zu nutzen, desto mehr Schutzmaßnahmen wandten sie an. Keinen Einfluss auf schützendes Verhalten gab es allerdings hinsichtlich der Bildung der Befragten. Der negative Zusammenhang zwischen dem Alter von Befragten und dem protektiven Verhalten kann durch die Nutzungserfahrung erklärt werden: da die Nutzungsintensität generell zu höherem Wissen und höheren Fähigkeiten

führt, liegt der Schluss nahe, dass ältere Personen sich schlechter schützen, da sie weniger Erfahrung haben als jüngere Nutzerinnen und Nutzer. Warum sich Männer mehr zu schützen scheinen als Frauen, ist noch nicht hinreichend erforscht. Doch auch andere Studien deuten auf einen Geschlechtsunterschied beim Privatheitsschutzverhalten hin (z. B. Milne et al., 2009). Schließlich zeigen manche Studien auf, dass Bildung einen negativen Einfluss auf Privatheitsschutz hat (Smit et al., 2014), was nicht in Einklang mit den Ergebnissen aus Studie II steht. Smit und Kolleg:innen erklären diese Beobachtungen damit, dass höhere Bildung mit mehr Wissen einhergeht, was sich negativ auf Privatheitsbedenken auswirkt. Dadurch, dass die Personen weniger besorgt seien, würden sie sich auch weniger schützen. Diese Annahme steht im Allgemeinen zwar in einem Widerspruch zur These, dass sich Privatheitskompetenz (Fähigkeiten und Wissen) generell positiv auf die Anwendung von Schutzmaßnahmen auswirkt, allerdings lassen sich diese Befunde mit unseren Beobachtungen aus Studie IV erklären: in dieser Studie fanden wir heraus, dass Personen, die der Meinung waren, dass sie fähig sind, ihre Privatsphäre auf Facebook schützen zu können, keine gesteigerte Schutzintention aufwiesen. Diese Auffassung führte sogar zu einer höheren Intention, persönliche Informationen preiszugeben. Dieses Ergebnis lässt sich damit erklären, dass sich eine hohe Einschätzung der eigenen Privatheitsfähigkeiten negativ auf tatsächliches Schutzverhalten auswirken kann, da sie zu einem falschen Gefühl von Sicherheit führt (Meier et al., 2020b). In ähnlicher Weise könnte es sich auch mit der Privatheitskompetenz verhalten: Personen, die die Fähigkeiten und das Wissen darüber haben, wie man sich schützt, könnten den tatsächlichen Schutz vernachlässigen, da sie der Auffassung sein könnten, sie seien bereits gut geschützt. Die genauen Hintergründe dieser teils widersprüchlichen Ergebnisse müssen aber in Zukunft noch genauer untersucht werden.

Zusammenfassend lässt sich festhalten, dass der Online-Privatheitsschutz von einer großen Anzahl komplexer und mehrschichtiger Konstrukte, die zum Teil miteinander interagieren, vorhergesagt wird. Grob lassen sich diese Konstrukte in solche einteilen, die die angewandten Schutzmaßnahmen positiv beeinflussen und solche, die Privatheitsschutz mindern. Dies sind zum einen Faktoren wie wahrgenommene Risiken (potenziell beeinflusst durch negative Erfahrungen) und Wissen darüber, wie man sich schützt sowie die entsprechenden Fähigkeiten. Zum anderen kann eine Wahrnehmung von Vorteilen der Datenpreisgabe (z. B. die Auffassung, dass personalisierte Werbung nützlich ist) oder aber Resignation hinsichtlich des Privatheitsschutzes die Anwendung protektiver Maßnahmen behindern. Es scheint allerdings eine dritte Kategorie zu geben: Faktoren, die unter gewissen Umständen positive Effekte und unter anderen Umständen negative Auswirkungen auf das Schutzverhalten haben, wie beispielsweise eine

hohe Einschätzung der eigenen Fähigkeiten. Diese Einschätzung kann entweder dazu führen, dass man sich Privatheitsschutz zutraut und sich besser schützt (Dienlin & Metzger, 2016) oder aber, dass man ein falsches Gefühl von Sicherheit empfindet und sich nicht besser schützt (Meier et al., 2020b).

4 Effekte und Auswirkungen von schützender Software

Auswirkung des Selbstdatenschutzes sollte in erster Linie ein verbesserter Schutz der eigenen Online-Privatsphäre sein. Zum Beispiel sollte die Nutzung eines Anti-Tracking Tools im Browser dazu führen, dass beispielsweise automatisch weniger Daten über das eigene Online-Verhalten durch Websites gesammelt werden. Doch wie wirkt sich ein verbesserter Schutz der Privatsphäre auf die Wahrnehmung und das Verhalten im Netz aus und wie wirkt sich gesteigertes Wissen über Datensammelpraktiken auf das Verhalten aus? Abgeleitet aus den oben beschriebenen Motiven für Schutzverhalten lassen sich zum einen Designvorschläge für bestimmte privatheitsschützende Tools ableiten und zum anderen Vorhersagen über die Auswirkungen auf die Wahrnehmung und das Verhalten der Nutzerinnen und Nutzer treffen. Grundsätzlich lassen sich die Funktionen von privatheitsschützenden Tools zum einen in tatsächlich erhöhten Schutz und zum anderen in gesteigertes Wissen über institutionale Praktiken durch erhöhte Transparenz einteilen[3].

4.1 Erhöhung der Transparenz

Die Schaffung von Transparenz hat das primäre Ziel, über potenziell schädliche Auswirkungen institutioneller Praktiken aufzuklären, damit Nutzende im Sinne der informationellen Selbstbestimmung[4] die bestmöglichen Privatheitsentscheidungen treffen können. In Studie IV simulierten wir die Nutzung eines transparenzsteigernden Tools. Den Teilnehmer:innen (304 Facebook-Nutzer:innen) wurde mitgeteilt, dass sie ein Tool testen würden, das ihre

[3] Eine Diskussion über technische Ansätze, den eigenen digitalen Fußabdruck sichtbar zu machen und dessen Auswirkungen zu verringern, finden Sie im Beitrag von Conrad u.a. in diesem Band.

[4] Die informationelle Selbstbestimmung als Grundlage für individuelle Freiheit und demokratische Teilhabe wird im Beitrag von Heesen u.a. in diesem Band diskutiert.

Privatsphäreeinstellungen auf Unsicherheiten überprüfen kann und eine Warnmeldung anzeigt, sollten die Einstellungen zu durchlässig sein. Die Elemente und das Design des Tools waren dabei an der Beschreibung von Furchtappellen aus der Schutzmotivationstheorie orientiert (Rogers, 1975). Die Proband:innen sahen entweder eine Warnmeldung, dass ihre Privatsphäre auf Facebook nicht gut geschützt ist oder eine neutrale Nachricht darüber, dass keine Probleme mit ihren Einstellungen entdeckt wurden. Außerdem wurden soziale Normen, also Informationen über das Schutzverhalten anderer Facebook-Nutzerinnen, gezeigt und variiert. Es wurde beispielsweise angezeigt, dass 78 % oder 22 % der anderen Nutzerinnen und Nutzer besser geschützt sind als man selbst. Schließlich wurde für alle Bedingungen eine einheitliche Empfehlung gegeben, dass die Facebook-Privatsphäreeinstellungen regelmäßig kontrolliert werden müssen. Die Auswertung der Daten zeigte allerdings keine Effekte der Warnmeldung und der Normen auf die Risikowahrnehmung oder die Intention, sich in Zukunft besser zu schützen. Dies könnte verschiedene Gründe haben. Zum einen wurden die Warnungen zufällig, also unabhängig vom tatsächlichen Privatheitsschutz der Proband:innen, angezeigt, um gleich große Experimentalgruppen zu schaffen. Aus diesem Grund könnten beispielsweise Personen, die sich tatsächlich gut schützen, eine Warnmeldung erhalten haben. Dadurch könnten mögliche Effekte einer Warnung auf die Wahrnehmung von Risiken oder auf die Intention, sich in Zukunft besser zu schützen, nicht wirksam geworden sein. Ein weiterer möglicher Grund für das Fehlen von Effekten des Tools ist, dass in den Medien häufig über Datensammelpraktiken von Facebook berichtet wird. Somit könnte die Warnmeldung wirkungslos bleiben, da ohnehin eine hohe Risikowahrnehmung vorherrscht.

Studie VI, untersuchte ebenfalls den Einfluss eines transparenzerhöhenden Tools, in Form eines Privacy-Scores. Die Proband:innen wurden gebeten, sich verschiedene Szenarien vorzustellen, in denen sie unterschiedliche Websites nutzen. Jede dieser Websites hat eigene Nutzungsvorteile, die lediglich durch die Preisgabe persönlicher Informationen erreicht werden können. Zusätzlich zu der Beschreibung der jeweiligen Website wird ein zufälliger Privacy-Score angezeigt. Dieser Score, abgeleitet vom Nutri-Score für Lebensmittel, zeigt die Buchstaben A, B und C in den Farben Grün, Gelb und Rot. Dabei steht A (grün) für eine privatheitsfreundliche Website und C (rot) für eine privatheitsinvasive Website. Diese Methode soll dazu dienen, Personen, die gerade eine Entscheidung über das Teilen oder Nicht-Teilen persönlicher Informationen treffen, in eben diesem Augenblick mit relevanten Informationen zu versorgen, um sie in ihrer Entscheidung des Teilens oder Nicht-Teilens zu unterstützen. In der Studie sollte untersucht werden, inwiefern der Privacy-Score die Wahrnehmung von

Vorteilen und Privatheitsrisiken und die Intention, Informationen von sich preiszugeben, beeinflussen kann. Erste Zwischenergebnisse mit 485 Teilnehmenden deuten darauf hin, dass der Privacy-Score sowohl die Wahrnehmung von Privatheitsrisiken als auch die Wahrnehmung der Vorteile der Website beeinflusst: während sich die wahrgenommenen Risiken mit steigendem Score erhöhen, verringert sich die Wahrnehmung der Nutzungsvorteile. Zudem sinkt die Bereitschaft, persönliche Informationen von sich auf der Website preiszugeben. Diese Zwischenergebnisse deuten auf die Wichtigkeit einer guten Informiertheit über Privatheitspraktiken in verschiedenen Situationen hin. Je privatheitsinvasiver eine Website wahrgenommen wird, desto weniger ist man offenbar bereit, persönliche Informationen preiszugeben. Fehlt diese Einschätzung, trifft man wohlmöglich eher Entscheidungen, die zu Privatheitsverletzungen führen können. Ähnliche Ergebnisse zeigten sich auch in Studie V. In einem Experiment mit 305 Teilnehmenden untersuchten wir unterschiedlich lange Datenschutzerklärungen als eine potenzielle Möglichkeit, mehr Transparenz zu schaffen (Meier et al., 2020a). Die Proband:innen wurden in der Studie gebeten, sich auf einer sozialen Netzwerkseite anzumelden. Bevor sie ihren persönlichen Account anlegten, hatten sie die Möglichkeit, die Datenschutzerklärung der Netzwerkseite zu lesen. Dabei wurde die Länge der Datenschutzerklärung sowie die Privatheitsfreundlichkeit der Netzwerkseite variiert. Es zeigte sich, dass eine deutlich kürzere Datenschutzerklärung dazu führen kann, dass Personen besser informiert sind und somit ein realistischeres Bild der Privatheitspraktiken der Website haben. Außerdem zeigte sich, dass die Informiertheit mit der wahrgenommenen Privatsphäre auf der Website zusammenhängt, die wiederum mit der Wahrnehmung von Vorteilen und Risiken des Netzwerks in Beziehung stand. Da viele empirische Untersuchungen gezeigt haben, dass die Wahrnehmung von Privatheitsrisiken und Vorteilen der Selbstoffenbarung in Zusammenhang mit der Preisgabe persönlicher Informationen steht (z. B. Culnan und Armstrong, 1999; Dienlin und Metzger, 2016; Meier et al., 2020b) und das Schutzverhalten maßgeblich von den wahrgenommenen Privatheitsrisiken beeinflusst wird (Meier et al., 2020b; Dienlin & Metzger, 2016; Boerman et al., 2018), erhalten die gefundenen Ergebnisse eine wichtige Relevanz. Offenbar scheint durch die transparente Vermittlung von Information über das Ausmaß der Privatheitsschutzes einer Website die Wahrnehmung von Nutzungsvorteilen sowie Privatheitsrisiken beeinflusst zu werden, was wiederum eine direkte Auswirkung auf das Privatheitsverhalten hat. Die Implikation an dieser Stelle ist, dass Nutzende, die auf mehr Wissen über die situativen Gegebenheiten zurückgreifen können, offenbar besser in der Lage sind, Entscheidungen zu treffen, die im eigenen Interesse sind (im Sinne der informationellen Selbstbestimmung) und sich besser vor Gefahren schützen

können, als Personen, denen dieses Wissen fehlt. Auch zeigt sich, dass einfach zu verarbeitende Informationen, wie zum Beispiel kurze Datenschutzerklärungen, Privacy Icons oder ein Privacy-Score, deutlich besser geeignet sind, um Transparenz zu schaffen, als umfangreiche Informationen.

In Studie VII mit 441 Proband:innen wurde analysiert, wie gut die Befragten über Webtracking, also automatisches Nachverfolgen und Aufzeichnen des Nutzendenverhaltens unabhängig von einer Website, informiert sind (Ammicht Quinn et al., 2018). Außerdem fragten wir verschiedene Einschätzungen ab, zum Beispiel die Selbsteinschätzung der eigenen Schutzfähigkeiten, getroffene Schutzmaßnahmen oder Sorgen bezüglich der Online-Privatheit. Zum einen zeigte sich, dass die Teilnehmer:innen der Studie nur sehr schlecht über Web-Tracking informiert waren. Die Kenntnisse von verschiedenen Web-Tracking Verfahren rangierten zwischen 14 und 41 %. Zum anderen zeigte sich, dass sich die Einschätzung über die eigenen Fähigkeiten und das Wissen, wie man sich im Internet ausreichend vor Privatheitsrisiken schützen kann, signifikant verschlechterte, wenn die Befragten über die bislang nicht bekannten Praktiken informiert wurden. Auch die Selbsteinschätzung über das Ausmaß getroffener Schutzmaßnahmen wurde am Ende der Studie deutlich schlechter bewertet als zu Beginn. Letztlich hatte das Informieren über verschiedene Web-Tracking Verfahren einen Einfluss auf die Besorgtheit der Befragten: am Ende der Untersuchung waren die Teilnehmenden besorgter als am Anfang. Auch diese Untersuchung zeigt, dass Transparenz einen Einfluss auf die Wahrnehmung und die Einschätzung der eigenen Fähigkeiten oder des eigenen Privatheitsschutzes hat. Auf Basis von fehlender Informiertheit könnten Internetnutzende die Meinung vertreten, sie seien ausreichend geschützt, obwohl dies nicht der Fall ist. Nur Personen, die über eine hinreichende Informiertheit verfügen, können sich ihren optimalen Vorstellungen entsprechend schützen und ein selbstbestimmtes[5] Privatheitsverhalten an den Tag legen.

4.2 Kontroll-Paradoxon

Obwohl auf der einen Seite positive Effekte von transparenz- und privatheitserhöhenden Technologien zu erwarten sind, kann es allerdings unter Umständen auch zu negativen Auswirkungen kommen. Brandimarte et al. (2013)

[5] Für eine ausführliche Diskussion, wie die individuelle Selbstbestimmung trotz des sozio-technischen Wandels aufrechterhalten werden kann, vergleiche den Beitrag von Lamla u. a. in diesem Band.

untersuchten den Effekt wahrgenommener Kontrolle, über die eigenen Daten verfügen zu können, auf die Bereitschaft persönliche Informationen von sich preiszugeben. Die Wissenschaftler:innen fanden heraus, dass Personen, denen der Eindruck von mehr Kontrolle über die eigenen Informationen vermittelt wurde, tatsächlich mehr von sich preisgaben, obwohl die Privatheitsrisiken de facto höher waren als in der Bedingung mit weniger implizierter Kontrolle. Diese Ergebnisse deuten darauf hin, dass das Gefühl der Kontrolle über die persönlichen Daten mit einem weniger vorsichtigen Privatheitsverhalten einhergehen kann, dass Personen folglich unvorsichtiger im Umgang mit ihren Informationen werden. Dieser Effekt lässt sich auch auf den Bereich der privatheitsschützenden Technologien übertragen: Personen, die glauben, sie seien durch die Nutzung bestimmter Software gut geschützt und hätten Kontrolle darüber, wer persönliche Informationen erhält und wer nicht, könnten zu unvorsichtigerem Verhalten tendieren, was schlussendlich dazu führen kann, dass die Risiken für Verletzungen der Privatheit trotz der Nutzung entsprechender Tools höher sind, als ohne die Nutzung solcher Tools. In diesem Zusammenhang fanden wir in Studie III heraus, dass es einen positiven Zusammenhang zwischen der Nutzungsbereitschaft eines privatheitsschützenden Tools und der mit der Nutzung assoziierten Kontrolle über persönliche Informationen gab. Außerdem zeigte sich, dass die mit der Nutzung assoziierte Kontrolle positiv mit der Intention, Informationen von sich während der Nutzung preiszugeben, zusammenhängt. Diese Ergebnisse deuten auf ähnliche Effekte wie die des Kontroll-Paradoxons hin, obwohl in dieser Untersuchung kein tatsächliches Verhalten gemessen wurde. Das sogenannte Paradoxon lässt sich mit den Ergebnissen aus unseren Studien V und VI erklären. Diese beiden Untersuchungen zeigten, dass Websites, die als privater wahrgenommen werden als andere Websites, positiver bewertet werden (im Sinne, dass mehr Nutzungsvorteile mit den Websites assoziiert werden) und gleichzeitig weniger Privatheitsrisiken antizipiert werden. Da in der Literatur häufig das Ausmaß an möglicher Kontrolle synonym mit dem Ausmaß an Privatsphäre verwendet wird, könnte in der Studie von Brandimarte et al. (2013) das Ausmaß der Kontrolle eng mit dem Ausmaß an Privatheit zusammenhängen[6].

[6] Für die Beleuchtung eines rational-ökonomischen Einsatzes von Daten als Zahlungsmittel und dessen Einfluss auf Kontrolle und Intentionalität sei an dieser Stelle auf den Beitrag von Hess u. a. in diesem Band verwiesen.

5 Zusammenfassung und Implikationen

Die vorgestellten Studien ergeben ein breites Bild, welche unterschiedlichen Faktoren beeinflussen, dass Personen privatheitsschützendes Verhalten zeigen. Die Daten erlauben auch Schlussfolgerungen über die Wirksamkeit von technischen Interventionen wie beispielsweise Warnhinweisen. Abb. 3 gibt einen Überblick über die Einflussfaktoren.

Zunächst lassen sich Aspekte aufführen, die die Evaluation der Situation durch die individuellen Nutzer:innen (d. h. deren Wahrnehmung und Einstellungen) betreffen. Zentral und in zahlreichen Studien bestätigt ist dabei die Wahrnehmung von Gratifikationen: Je vorteilhafter die Plattform empfunden wird, desto mehr wird preisgegeben und desto weniger schützt man sich. Auch eine negative Einstellung zum Datenschutz führt zur geringeren Anwendung von Schutzmaßnahmen. Auf der anderen Seite führen sowohl der Wunsch nach Schutz im Internet als auch vorangegangene negative Erfahrungen bzw. erlebte Privatheitsverletzungen zu mehr Schutzverhalten.

Des Weiteren nimmt auch die soziale Umwelt Einfluss. So kann das Vorherrschen von privatheitsfreundlichen Normen (zum Beispiel die in einer Gesellschaft und/oder über Medien vermittelte Annahme, dass man sich schützen sollte) zu mehr Schutzverhalten führen.

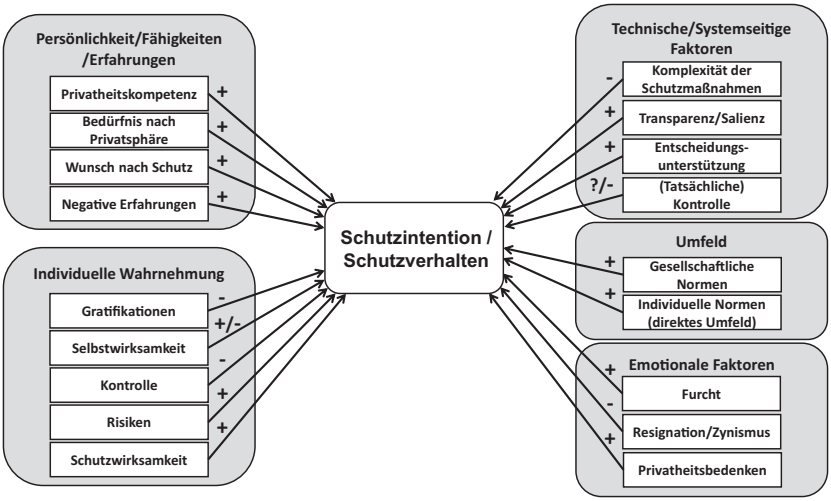

Abb. 3 Darstellung der Einflussfaktoren auf die Schutzintention, bzw. das Schutzverhalten

Ebenso können emotionale Aspekte einflussreich sein: Furcht hat sich als Motivator erwiesen, sich besser zu schützen. Auf der anderen Seite tragen Resignation und Privatheitszynismus dazu bei, dass zumindest die Intention, sich zu schützen, sinkt.

Sowohl unsere als auch Studien anderer Forscher:innen zeigen den Einfluss verschiedener individueller Aspekte im Sinne von beispielsweise Persönlichkeitsvariablen. Besonders zentral ist dabei die Privatheitskompetenz. Eine hohe Privatheitskompetenz ermöglicht ein besseres Verstehen und dadurch auch verbessertes Anwenden von Schutzmechanismen. Die subjektive Seite der Privatheitskompetenz hingegen – im Sinne einer Einschätzung der eigenen Fähigkeiten – ergibt keine konsistenten Ergebnisse. So kann eine hohe Einschätzung der eigenen Fähigkeiten zu mehr oder zu weniger Privatheitsschutz führen. Gegebenenfalls Einfluss nehmende Randbedingungen müssen noch weiter untersucht werden.

Schließlich haben sich auch einige systemseitige, oft technische Faktoren als einflussnehmend erwiesen. Dabei hat sich vor allem die Komplexität der Schutzmaßnahmen als bedeutungsvoll herausgestellt: Je komplexer und aufwendiger die jeweilige Schutzmaßnahme in ihrer Anwendung ist, desto weniger wird sie gewählt bzw. angewendet. Auch die Salienz der Schutzmaßnahmen spielt eine Rolle. Wenn die Möglichkeit, sich zu schützen, versteckt wird, herrscht eine höhere Unsicherheit vor, inwieweit man geschützt ist oder nicht. Auch die Eigenschaften des Schutztools können die Nutzung beeinflussen: Insbesondere wenn das genutzte Tool selbst wiederum Daten sammelt, muss darüber eine sehr transparente Aufklärung erfolgen. Schließlich wurden Warnmeldungen, dass die Privatsphäre nicht gut geschützt ist und ein Privacy Score in ihrer Wirkung überprüft. Diese Formen der verkürzten, direkten Warnungen erbringen allerdings inkonsistente Effekte. An anderer Stelle hat sich dagegen herausgestellt, dass verkürzte Formen positive Wirkungen haben: Die insbesondere auf Webseiten zu findenden Datenschutzerklärungen führen zu höherem Wissen und zu höherer Schutzintention, wenn sie kurz gehalten sind.

Die hier nun aufgeführten Faktoren sind natürlich nicht exhaustiv und in jedem der Bereiche sind viele weitere Variablen vorstellbar, die das Schutzverhalten beeinflussen. Neben der Notwendigkeit, die Liste weiter zu ergänzen, ergibt sich besonderer Forschungsbedarf insbesondere durch die erweiterten technischen Möglichkeiten. Dies bezieht sich einerseits darauf, dass Tools zum Schutz der Privatheit weiterentwickelt bzw. überhaupt verfügbar werden. Hier ist zu prüfen, ob je nach System neue Faktoren berücksichtigt werden müssen, die die Nutzung des Tools beeinflussen. Andererseits ergeben sich durch die Weiterentwicklung der Technologien (zum Beispiel die steigende Verfügbarkeit und

Präsenz von intelligenten Algorithmen) immer neue Schutzbedarfe. Inwieweit sich dadurch auch die Variablen, die das Schutzverhalten beeinflussen, verändern, muss in zukünftiger Forschung betrachtet werden.

Literatur

Ammicht Quinn, R., Baur, A., Bile, T., Bremert, B., Büttner, B., Grigorjew, O., Hagendorff, T., Heesen, J., Krämer, N., Meier, Y., Nebel, M., Neubaum, G., Ochs, C., Simo Fhom, H., & Weiler, S. (2018). *Tracking: Beschreibung und Bewertung neuer Methoden*. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt.

Bartsch, M., & Dienlin, T. (2016). Control your facebook: An analysis of online privacy literacy. *Computers in Human Behavior, 56,* 147–154.

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research,* 48(7), 953-977.

Brandimarte, L., Acquisti, A., & Loewenstein, G. (2013). Misplaced confidences privacy and the control paradox. *Social Psychological and Personality Science, 4,* 340–347.

Christofides, E., Muise, A., & Desmarais, S. (2012). Risky disclosures on facebook. *Journal of Adolescent Research, 27,* 714–731.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10,* 104–115.

Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In S. Trepte & L. Reinecke (Hrsg.), *Privacy online: Perspectives on privacy and self-disclosure in the social web*. Springer.

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative U.S. *Sample. Journal of Computer-Mediated Communication, 21,* 368–383.

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10.*

Krasnova, H., & Veltri, N. F. (2010). Published. In Privacy Calculus on Social Networking Sites: Explorative Evidence from Germany and USA. (Hrsg.), Proceedings of the 43rd Hawaii International Conference on System Sciences, Honolulu, 5–8 Jan. 2010.

Masur, P. (2018). *Situational privacy and self-disclosure: Communication processes in online environments*. Springer.

Matzner, T., Masur, P. K., Ochs, C., & von Pape, T. (2016). Do-it-yourself data protection—empowerment or burden? In S. Gutwirth, R. Leenes, & P. De Hert (Hrsg.), *Data protection on the move: Current developments in ICT and privacy/data protection*. Springer.

Meier, Y., Schäwel, J., & Krämer, N. C. (2021). Between protection and disclosure: applying the privacy calculus to investigate the intended use of privacy-protecting tools and self-disclosure on different websites. Studies in Communication and Media, 10(3), 283-306.

Meier, Y., Schäwel, J., & Krämer, N. C. (2020a). The shorter the better? Effects of privacy policy length on online privacy decision-making. *Media and Communication, 8,* 291–301.

Meier, Y., Schäwel, J., Kyewski, E., & Krämer, N. C. (2020b). Applying protection motivation theory to predict facebook users' withdrawal and disclosure intentions. Proceedings of the 11th International Conference on Social Media and Society, 2020 Toronto, ON, Canada. 21–29.

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs, 43,* 449–473.

Neubaum, G., Krämer, N. C., Kyewski, E., & Metzger, M. (2020). How subjective norms shape personal privacy regulation in social media communication: A cross-cultural approach. Manuscript submitted for publication.

Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research, 40,* 215–236.

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91,* 93–114.

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Hrsg.), *Social psychophysiology: A sourcebook*. Guilford Press.

Rogers, R. W., & Deckner, C. W. (1975). Effects of fear appeals and physiological arousal upon emotion, attitudes, and cigarette smoking. *Journal of Personality and Social Psychology, 32,* 222–230.

Smit, E. G., Noort, V., & Guda und Voorveld, Hilde A. M. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior, 32,* 15–22.

Stainback, R. D., & Rogers, R. W. (1983). Identifying effective components of alcohol abuse prevention programs: Effects of fear appeals, message style, and source expertise. *International Journal of the Addictions, 18,* 393–405.

Trepte, S., Dienlin, T., & Reinecke, L. (2014). Risky behaviors: How online experiences influence privacy behaviors. In B. Stark, O. Quiring, & N. Jackob (Hrsg.), *Von der Gutenberg-Galaxis zur Google-Galaxis: Alte und neue Grenzvermessungen nach 50 Jahren DGPuK*. Herbert von Halem Verlag.

Trepte, S., & Masur, P. K. (2017). *Privacy attitudes, perceptions, and behaviors of the German population*. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A., & Lind, F. (2015). Do people know about privacy and data protection strategies? Towards the „Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. De Hert (Hrsg.), *Reforming European data protection law*. Springer.

Dr. Yannic Meier ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Sozialpsychologie – Medien und Kommunikation an der Universität Duisburg-Essen in der Fakultät für Ingenieurwissenschaften.

Dr. Judith Meinert ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Sozialpsychologie – Medien und Kommunikation an der Universität Duisburg-Essen in der Fakultät für Ingenieurwissenschaften.

Dr. Nicole C. Krämer ist Professorin für Sozialpsychologie – Medien und Kommunikation an der Universität Duisburg-Essen in der Fakultät für Ingenieurwissenschaften.

Gestaltung von technischem und gesellschaftlichem Wandel

Digitaler Fußabdruck

Bernd Conrad, Michael Kreutzer, Johanna Mittermeier, Linda Schreiber und Hervais Simo Fhom

„Warning: Your kid's digital footprint starts before birth"
Marisa Dellatto, New York Post, 8. Nov. 2018

1 Einleitung: Technik als Auslöser – hohe Dynamik, neue Möglichkeiten

Neue digitale Technologien rufen grundlegende gesellschaftliche und soziale Veränderungen hervor und sind sowohl Auslöser für einen umfassenden sozioökonomischen und institutionellen Wandel als auch Nebenfolge sich ändernder gesellschaftlicher Zusammenhänge, Praktiken und Normen. Dieser Beitrag steht vor dem Hintergrund des zunehmenden Umfangs von gesammelten Daten sowie dem Grad der Vernetzbarkeit und Analysemöglichkeiten von Daten und den daraus resultierenden Herausforderungen für die Privatheit. Der hieraus entstehende digitale

B. Conrad · M. Kreutzer · J. Mittermeier · L. Schreiber · H. Simo Fhom (✉)
Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt, Deutschland
E-mail: hervais.simo@sit.fraunhofer.de

M. Kreutzer
E-mail: michael.kreutzer@sit.fraunhofer.de

J. Mittermeier
E-mail: johanna.mittermeier@sit.fraunhofer.de

L. Schreiber
E-mail: linda.schreiber@sit.fraunhofer.de

J. Mittermeier
TU Darmstadt, Darmstadt, Deutschland

A. Roßnagel und M. Friedewald (Hrsg.), *Die Zukunft von Privatheit und Selbstbestimmung,* DuD-Fachbeiträge,
https://doi.org/10.1007/978-3-658-35263-9_7

Fußabdruck einer Person steht im Zentrum dieser Betrachtung, denn er stellt vielfältige Herausforderungen an den Privatsphärenschutz sowie den gesellschaftlichen Diskurs.

Der nachfolgende Abschn. 2 skizziert drei technische Trends, auf deren Basis und an Hand von Beispielen sowohl Auswirkungen auf die Privatheit als auch neue Möglichkeiten dargestellt werden. Unter Forscherinnen und Forschern gibt es große Übereinstimmung darüber, dass Analysen und Gestaltungsvorschläge auf Basis von Angreifer- und Bedrohungsmodellen durchgeführt werden müssen, wie Abschn. 3 aufzeigt. Im nächsten Abschn. 4 werden dementsprechend aktuelle und zukünftige *generelle* Bedrohungen für die Privatheit identifiziert und anhand von Beispielen veranschaulicht. Ausgehend davon adressiert Abschn. 5 das scheinbare Spannungsverhältnis zwischen dem Innovationspotential von Digitalisierung und Privatheitsinteressen und geht auf den wirtschaftlichen Kontext von Unternehmen und den bestehenden rechtlichen Rahmen ein. Die Thesen des Abschnitts lauten, dass Innovation und Privatheit vereinbar sind und das technischer Fortschritt für „Privacy-enhancing Technologies" genutzt werden kann, um Innovationen im Bereich der Privatheit zu fördern und Prinzipien wie informationelle Selbstbestimmung und Nutzerermächtigung zu stärken. Abschn. 6 ist die Einleitung in drei konkrete technische Gestaltungsvorschläge. Diese Gestaltungsvorschläge werden in den darauffolgenden Abschn. 6.1, 6.2 und 6.3 abgebildet, um exemplarisch aufzuzeigen, wie der digitale Fußabdruck zur Erhöhung der Transparenz abgebildet und genutzt werden kann. In unserer Schlussbetrachtung Abschn. 7 betonen wir die Wichtigkeit von Transparenz für die informationelle Selbstbestimmung und heben die Mechanismen des digitalen Fußabdrucks als herausragend hervor.

2 Techniktrends, Auswirkungen und Möglichkeiten

2.1 Trends in der digitalen Technikentwicklung

Der Möglichkeitsraum durch die digitale Technik erweitert sich mit ihr. Die von der OECD in 1997 beschriebenen Trends[1] wurden durch eine von DG Connect im Jahr 2009 publizierte Studie[2] bestätigt und präzisiert. Die Autoren der DG-Connect-Studie beschreiben eine Zukunft, in der Informationen automatisch fließen (Hyperkonvergenz) und von jedem Ort und zu jeder Zeit mit einer großen Anzahl von Geräten abgerufen und ausgetauscht werden kann (Hyperkonnektivität).

[1] OECD (1997).

[2] Cave et al. (2009).

Informations-Ökosysteme wie Online Social Networks weisen hohe Dynamiken in mehreren Dimensionen auf.

Hyperkonnektivität, Hyperkonvergenz und dynamische Informations-Ökosysteme entstehen weder isoliert noch parallel, sondern sind miteinander verschränkt und befördern sich gegenseitig. Sie ermöglichen eine Vielzahl von neuen Anwendungen und induzieren soziotechnische Transformationsprozesse.

2.2 Bereichsübergreifende Auswirkungen und Möglichkeiten

Zusammen erweitern und effektivieren diese Entwicklungen bestehende Informationstechnologien und machen sie effizienter. Sie ermöglichen darüber hinaus neue digitale Produkte, Dienste und datenbasierte Geschäftsmodelle, die zur digitalen Transformation von immer mehr Lebensbereichen beitragen und einen großen Veränderungsdruck auf bestehende Akteure, Infrastrukturen, Praktiken und Prozesse innerhalb relevanter wirtschaftlicher- und gesellschaftlicher Bereiche (z. B. im Bildungs-, Gesundheits- und Transportwesen) ausüben. Der Einfluss ist im Alltag unmittelbar sichtbar, pars pro toto seien genannt: Das Smart Home, das Fahrzeug (Smart Car), sowie neuartige Endgeräte, die direkt am Körper (Wearables) getragen werden können.[3]

Durch die Gesamtheit aller „Spuren“ dieser digitalen Aktivitäten, Beiträge und Kommunikationen, die durch die dargestellten Technologien in den verschiedensten Anwendungsfällen entstehen sowie verknüpft und ausgewertet werden, entsteht ein einzigartiger, stetig wachsender digitaler Fußabdruck einer Person. Das Bewusstsein über diesen digitalen Fußabdruck und dessen Umfang sowie die Möglichkeit zur Kontrolle dessen und den daraus ableitbaren Schlussfolgerungen ist für den Betroffenen oftmals sehr eingeschränkt.[4]

Diese Informationen zu einer Person, die durch diese bewusst oder unbewusst, selbstständig oder durch andere preisgegeben werden, lassen es zu, detaillierte Aussagen zur Persönlichkeit und den Vorlieben einer Person zu treffen. Unternehmen, staatliche Einrichtungen oder auch eigene (Online-) Freundinnen und Freunde können so mit unterschiedlich komplexen (automatisierten oder händischen) Methoden auf Eigenschaften und Vorlieben einer Person schließen, die diese möglicherweise nicht beabsichtigt hat, mit anderen zu teilen.[5] Dadurch kann der digitale Fußab-

[3] Rosner und Kenneally (2018).

[4] Osborne und Connelly (2015).

[5] Lambiotte und Kosinski (2014).

druck umfassende Auswirkungen auf das online und offline Leben einer Person haben – von personalisierten Suchmaschinen, Empfehlungssystemen und gezieltem Online-Marketing[6] zu personalisierten Preisen, gemessen an der jeweiligen Zahlungsbereitschaft eines Verbrauchers[7] bis hin zu Job- und Karriereaussichten.[8]

Was verbindet diese und weitere Fragen der Privatheit, wenn sie systematisch betrachtet werden sollen?

3 Angreifer- und Bedrohungsmodell als Konstante für den Diskurs über Privatheit

Die Vorstellung darüber, was Privatheit ist, was sie für Individuen bedeutet und wie wichtig[9] sie ist, ändert sich mit der Zeit.[10] Seit der Jahrtausendwende scheint die Änderungsgeschwindigkeit zuzunehmen, wenn man den Privatheitsdiskurs[11] verfolgt. Die Meinungen gehen auseinander,[12] wer oder was das Problem verursacht und was Problemverstärker sind. Die Wechselwirkungen zwischen den Akteurinnen, Artefakten und Praxen werden uneinheitlich[13] beschrieben. Es gibt Dissens darüber, was zu den personenbeziehbaren Daten[14] zählt. Wissenschaftlerinnen und Wissenschaftler ringen um die Frage, ob es das Privacy Paradox[15] noch gibt oder ob es überhaupt je existierte, also ein Mythos[16] ist. Die kulturellen und sozialen Anschauungen über Privatheit weichen voneinander ab[17] und ändern sich mit der Zeit. Es variieren die Annahmen der Forschung über die Kultur und die Zeit, welche Faktoren für die Messung der Einstellung und des Verhaltens in Bezug auf die Privatheit am relevantesten sind. Dieser Wandel spiegelt sich auch in der Rechtsent-

[6] Lambiotte und Kosinski (2014, S. 1939).
[7] Reisch et al. (2016, S. 21).
[8] Van Ouytsel et al. (2014).
[9] Acquisti et al. (2013).
[10] Goldfarb und Tucker (2012).
[11] Cichy und Salge (2015).
[12] Pohle (2017).
[13] O'Rourke und Kerr (2017) und Raab und Koops (2009).
[14] Stalla-Bourdillon und Knight (2017).
[15] Dienlin und Trepte (2015).
[16] Solove (2020).
[17] Heisenberg (2005).

wicklung[18] wieder. Metastudien, die anderen Disziplinen wertvolle Erkenntnisse liefern, stoßen somit an methodische Grenzen.

Lediglich über wenige Begriffe wurde Konsens erreicht: Der Kristallisationspunkt ist das Angreifer- und Bedrohungsmodell. Es ist der Dreh- und Angelpunkt für Gestaltungsvorschläge.

4 Identifizierung aktueller und zukünftiger Bedrohungen für die Privatheit

Der Einsatz innovativer Technik wird stets von dem Paradox begleitet, dass Menschen zwar neue Handlungsmöglichkeiten erlangen, damit jedoch auch neuen Risiken und Gefahren ausgesetzt sind. Für fast alle digitalen Innovationen stellt sich die Frage der Privatheit: *„Der Zugang zum Thema Privatheit von juristischen, politischen und technischen Gesichtspunkten her verdankt sich der Aktualität des Themas durch die Bedrohung und tendenzielle Auflösung von Privatheit in Zeiten der Netzgesellschaft“*.[19] Die technologischen Trends Hyperkonnektivität, Hyperkonvergenz und die hohe Dynamik der Informations-Ökosysteme erfordert, dass die digitale Welt immer wieder auf den Prüfstand hinsichtlich der Einhaltung von Grundwerten wie informationelle Selbstbestimmung, Entscheidungsfreiheit, Nichtdiskriminierung und Meinungspluralität gestellt werden muss.

Vier Beispiele aus den Forschungsaktivitäten des Fraunhofer SIT veranschaulichen exemplarisch die aktuellen und zukünftigen Bedrohungen für die Privatheit.

4.1 Datenschutz im Domain Name System – Risiken und Lösungsansätze

Das Domain Name System (DNS) ist eines der Rückgratsysteme, von denen das Funktionieren des Internets abhängig ist. Als sogenanntes „Adressbuch des Internets“ bietet die DNS Namensauflösungsfunktionen für Internet-Dienste, von denen die wichtigste die Übersetzung von Domänennamen in Internet-Protokoll-Adressen (IP-Adressen) und umgekehrt ist. Obwohl immer mehr Internet-Dienste auf verschlüsselte Kommunikation umsteigen, die sensible Informationen vor potenziellen Lauschangriffen verbirgt, bleibt das unverschlüsselte und nicht authentifizierte DNS-Protokoll eine entscheidende Schwachstelle der gesamten

[18] Lewinski (2012).

[19] Böhme (2018, S. 17).

Internet-Infrastruktur in Bezug auf Datenschutz. DNS-Daten sind Metadaten, sie beinhalten Adressen aufgerufener Webseiten, Adressen der sie aufrufenden Systeme, Zeitpunkte und vielfach auch Rückschlüsse auf Standorte. Mit diesen Metadaten kann man die Kompetenzen, Vorlieben und Neigungen einzelner Personen ableiten und in Profilen speichern. Aus Metadaten werden hierdurch Inhaltsdaten. Der hierarchische und zentralisierte Aufbau des DNS ermöglicht es verschiedenen Einrichtungen, einschließlich kommerzieller und staatlicher, die Online-Aktivitäten von Internetnutzern zu überwachen und sensible Rückschlüsse über sie zu ziehen, wodurch letztlich das Recht des Einzelnen auf Privatsphäre untergraben wird.[20]

4.2 Datenschutz, IT-Sicherheit und Privatheitsschutz bei mobilen Diensten

Beispiel Dating-Apps Der Markt für Online-Dating-Dienste boomt. Eine stetig wachsende Anzahl Liebesuchender erhofft sich die große Liebe via Internet finden zu können[21] und verlässt sich dabei u. a. auf Smartphones, Tablets und dedizierte mobile Dating-Apps. Die Nutzer schätzen besonders die personalisierten und lokationsbasierten Angebote dieser Apps. Sie können Profile anlegen und den Suchradius einstellen, in dem ein möglicher Flirtpartner gesucht werden soll. Ebenso lassen sich die gewünschten Altersgruppen und das Geschlecht des potenziellen Partners dynamisch einstellen. Anhand dieser und weiterer auf dem Nutzergerät befindlichen Informationen – darunter Wohnort und Kontaktliste – schlägt die App einen möglichen Profil-Match vor. Die dabei anfallenden Daten über Nutzerverhalten und -vorlieben, ihre Weitergabe und Verarbeitung sowie die zunehmende intransparente Akteurslandschaft des Dating-App-Ökosystems stellen den Schutz der Privatheit und die informationelle Selbstbestimmung vor neue Herausforderungen. Doch wie privatheitsinvasiv sind Dating-Apps tatsächlich? Wir sind dieser Frage nachgegangen und haben eine Analyse der Top-250 Android Dating-Apps durchgeführt. In mehr als der Hälfte der im offiziellen Play Store beliebtesten kostenlosen Dating-Apps (Stand: 29 September 2016) sind mehrere Anfälligkeiten, z. B. unverschlüsselte Datenübertragung via HTTP, unsichere Codes für SSL/TLS oder das Laden aktiver Webinhalte wie JavaScript, festgestellt worden. Solche Anfälligkeiten erlauben potenziellen Angreifern, sensitive Nutzerdaten (z. B. Log-in-Daten) abzufangen, um u. a. Kontrolle über die Konten der Nutzenden zu erlangen. Ein Vergleich mit den Top-250 Nicht-Dating-Apps zeigte, dass ein deutlich höherer

[20] Kelpen und Simo (2018).
[21] BITKOM (2020a).

Prozentsatz der Dating-Apps keinen Link zu einer Datenschutzrichtlinie in ihrem Anwendungs-Dashboard eingebunden hatten (34 %), während nur 18 % der Nicht-Dating-Apps dies taten. 5 % dieser URL waren tote Links, d. h. sie führten zu gar keiner Datenschutzerklärung. Darüber hinaus ergab eine weitere Überprüfung der Datenschutzrichtlinien, dass Englisch die häufigste verwendete Sprache zur Formulierung der Datenschutzrichtlinien ist (44 % vs. 58 % für Nicht-Dating-Apps), gefolgt von Deutsch (9 % vs. 21 % für Nicht-Dating-Apps), Chinesisch (<2 %), Französisch (<1 %), Spanisch (<1 %) und Dänisch (<1 %), bulgarisch (<1 %) usw. Eine weitere bemerkenswerte Feststellung ist, dass etwa ein Viertel der untersuchten Apps, unabhängig davon ob Dating-Apps oder nicht, keine Postanschrift des App-Anbieters im Play-Store bereitstellte. Aus Sicht des Datenschutzes wird es für Nutzende dementsprechend erheblich schwieriger, die für die Datenverarbeitung verantwortliche Stelle zu kontaktieren, oder die Gerichtsbarkeit zu bestimmen um mögliche Ansprüche gegenüber der Stelle durchsetzen zu können. Ein weiteres Risiko für die Privatsphäre entsteht mit dem ebenfalls im Rahmen unserer Untersuchung festgestellten verbreiteten Einsatz sog. Advertisement/Tracking Frameworks. Für viele Funktionen von Apps werden solche Frameworks, auch Zusatzbibliotheken genannt, verwendet, um Details über die App-Nutzenden zu erfassen. Im besten Fall sind dies Informationen, die die Anbieter zur Verbesserung ihrer Services verwenden. Werbetreibende verwenden die Informationen oft, um Nutzerprofile zu erstellen und so z. B. maßgeschneiderte Werbung einzublenden.[22] Die Zusatzbibliotheken sind jedoch häufig auch Einfallstore für Cyber-Angriffe, da sie oft Sicherheitslücken aufweisen. Aus unseren Untersuchungen ging hervor, dass 44 % der 250 Dating-Apps zwischen 3 und 5 Werbe-/Tracking-Frameworks enthielten. 34 % Dating-Apps hatten höchstens 2 Werbe-/Tracking-Frameworks. Eine Dating-App hat die meisten Werbe-/Tracking-Frameworks (über 12). Bei Nicht-Dating-Apps waren es im Gegensatz nur knapp 33 % der Top-250 Apps mit 3 bis 5 Werbe-/Tracking-Frameworks. 45 % der getesteten Nicht-Dating-Apps hatten maximal 2 Werbe-/Tracking-Frameworks im Code integriert. Eine Zusammenfassung unserer Forschungsergebnisse inkl. weiterer Aspekte u. a. hinsichtlich der Art und Privacy-Implikationen der im Kontext von Dating-Apps benötigten Berechtigungen, stellten wir auf dem Web Monday am 20. November 2017 in Darmstadt vor.[23]

Beispiel Learning-Apps In den letzten Jahren hat die Popularität von mobilen Learning-Apps für Kinder und Jugendliche stark zugenommen – insbesondere im Kontext der aktuell herrschenden Corona-Pandemie in dem der Schulbetrieb zuletzt

[22] Ammicht Quinn et al. (2018).

[23] https://wemoda.de/fuenf-minuten-fuer-hervais-simo/

massiv eingeschränkt werden musste. Viele dieser Apps überwachen das Nutzerverhalten und sammeln personenbezogene Daten, die nach gängiger Meinung zu einem entscheidenden Faktor für erfolgreiche Innovationen geworden sind. Als Folge dessen könnte eine zunehmende Verbreitung von Bildungs- und Lern-Apps die Privatheit von Kindern, Kleinkindern und sogar Säuglingen erheblich beeinträchtigen.[24]

In der Tat muss bei Kindern und Jugendlichen davon ausgegangen werden, dass sie, je kleiner sie sind, umso weniger die Bedeutung und Konsequenzen der Preisgabe von personenbeziehbaren Informationen verstanden wird und es fraglich ist, ob sie eine „informierte" Zustimmung erteilen können. Dienstanbieter und Dritte (z. B. Angreifer, Datenvermittler, Datenaggregatoren, etc.) die Daten von Kindern und Jugendlichen von Learning-Apps erhalten, können diese beispielsweise weiterverkaufen und so das Versenden von personalisierten Werbeinhalten an Kinder und Jugendliche weiterhin ermöglichen. In der EU erhalten Minderjährige im Rahmen der DSGVO einen besonderen Schutz.[25] So sind u. a. eine Zustimmung vor der Verwendung personenbezogener Daten durch den Träger der elterlichen Verantwortung für das Kind und ein Verbot des Behavioral Targeting vorgeschrieben.[26] Im Rahmen einer zum Zeitpunkt der Finalisierung dieses Beitrags sich noch in der Durchführung befindlichen Analyse untersuchen wir, inwieweit Android Learning-Apps vor dem Hintergrund der DSGVO die Privatheit ihrer Nutzenden gewährleisten bzw. Anforderungen an Datensicherheit erfüllen. Die Datengrundlage für die Untersuchung besteht aus 199 Apps (167 „Kostenlose"-Applikationen und 32 „Kostenpflichtige"-Applikationen) aus dem Google Play-Store. Die Analyse unterteilt sich in zwei Schritte: die grobgranulare und feingranulare Analyse. Die grobgranulare Analyse befasst sich mit Beobachtungen und statistischen Erkenntnissen, welche direkt aus den bereits gesammelten Metadaten der Applikationen ersichtlich sind. Darunter fallen Statistiken zu einzelnen Metadaten wie Entwickler-Adresse bei der Ursprungsland-Analyse oder die durchschnittliche Bewertung und Anzahl an Installationen oder Kommentare. Weiterhin werden die Ergebnisse hinsichtlich Datensicherheit und Cybersicherheit kritisch hinterfragt, sodass Metadaten bezüglich Datenschutzerklärung und Berechtigungen eingestuft werden. Somit folgt eine Datenschutzerklärungs-Analyse, bei der die Verteilung zwischen Applikationen mit bzw. ohne Datenschutzerklärung zusammen mit anderen Metadaten in Verbindung gebracht wird. Zuletzt folgt eine Berechtigungs-Analyse, wobei Berechtigungen hinsichtlich normaler und gefährlicher Berechtigungen statistisch dargestellt und analysiert werden. Die feingranulare Analyse baut auf der grobgranularen Analyse

[24] Reyes et al. (2018) und Gillula (2015).

[25] Stapf et al. (2021).

[26] Roßnagel et al. (2020).

auf. Hierbei wird die App-Software mittels Tools zur statischen und dynamischen Analyse genauer betrachtet. Wichtige Untersuchungsgegenstände sind vor allem die Unterteilung von Berechtigungen, gemäß Google Protection Levels, sowie eingebettete Tracking Libraries im Code einer Applikation. Des Weiteren wird die Applikation auf schädliche Software, wie Malware oder Viren untersucht werden. Zuletzt wird das Vorhandensein und die Qualität von Maßnahmen zur Absicherung des Datenverkehrs der ausgewählten Applikationen mit entsprechenden Tools bewertet.[27]

4.3 Vernetzte und Smarte Objekte – Herausforderungen für Privatheit und Cyber-Sicherheit

Beispiel Smart TVs Die zunehmende Vernetzung von Haushaltsgeräten betrifft mittlerweile alle Geräteklassen. Smart Home ist der Sammelbegriff für alle Haushaltsgeräte, die Verbindungsmöglichkeiten mit anderen Parteien bieten. Diese Parteien können unter anderem Dienstleister im Internet oder auch lokale Geräte sein. Häufig ist die Rechenleistung so hoch wie bei älteren Computersystemen. Smart TVs, können beispielsweise eine Vielzahl von Funktionen bieten, die bisher nur von herkömmlichen Computersystemen bekannt waren. Dies sind zum Beispiel die Nutzung von Skype, das Abspielen von Videos oder auch das Herumstöbern im Internet. Durch die neuen Verbindungsmöglichkeiten nehmen nicht nur die Vorteile für den Nutzer zu, sondern auch die Gefahrenquellen für solche Geräte. Wie auch von anderen Geräten bekannt, können verschiedene schadhafte Programme, wie zum Beispiel Viren, Computersysteme beeinträchtigen. Auch der Missbrauch von Geräten zum Schaden Dritter ist möglich. Schutzmaßnahmen sind unumgänglich, um Nutzer und Unternehmen vor Schäden zu schützen. Wir haben in einem Arbeitspapier einen Überblick über Chancen und wachsende Möglichkeiten im Bereich Smart TVs geliefert und lenken dabei den Blick auf die damit verbundenen Risiken und Gefahren für die Privatsphäre der Nutzenden.[28]

Beispiel Vernetzte Fahrzeuge Moderne Fahrzeuge werden zunehmend von einer Vielfalt von IT- und elektronischen Komponenten durchdrungen, mit deren Hilfe fahrzeuginterne Abläufe überwacht und unterschiedliche Daten über Insassen und Fahrzeugumgebung erfasst und an die Außenwelt weitergeleitet werden. Dies birgt das Potenzial neue Dienstleistungen, Produkte, und Geschäftsmodelle zu schaffen

[27] Dass et al. (2021).

[28] Ghiglieri et al. (2016a, b).

und letztendlich Innovationen voranzutreiben. Mit der zunehmenden Vernetzung und Datensammlung im Automotive-Kontext entsteht jedoch auch ein Bedrohungspotential für das Recht auf informationelle Selbstbestimmung des Einzelnen. Über die Vielzahl interner und externer Kommunikationsschnittstellen können nicht nur ECUs untereinander und mit der Außenwelt kommunizieren, sondern auch Schad- und Fremdsoftware in das digitale Ökosystem des Autos eingeschleust und dort verbreitet werden.[29] Infiziert und kompromittiert werden können nicht nur die Fahrzeuge, sondern auch die kritischen Infrastrukturkomponenten seitens der Betreiber und Zulieferer.[30] Neben unerlaubten Datenzugriffen können Angriffe auf vernetzte Fahrzeuge schnell lebensbedrohliche Folgen haben.[31] Darüber hinaus steht im Kontext von Smart Cars die Besonderheit im Mittelpunkt, dass die Betroffenen sich bei der Nutzung moderner PKWs und den damit verbundenen (online) Diensten im Zentrum komplexer für sie völlig undurchschaubarer Datenverarbeitungsprozesse befinden. Die daraus folgende Überforderung wird noch dadurch verstärkt, dass PKW-Nutzende (Fahrer und Insassen) auf diese in zunehmender Weise angewiesen sind. In derartigen Situationen kann kaum von informierter und selbstbestimmter Einwilligung zur Datenverarbeitung ausgegangen werden. Vielmehr besteht die Gefahr, dass sich PKW-Hersteller und Anbieter von Dienstleistungen und Produkten mit verklausuliert formulierten AGBs und Datenschutzerklärungen absichern bzw. einseitig durchsetzen. Angreifer und unseriöse Anbieter von Mobilitätsdienstleistungen könnten mittels der so gewonnenen Daten beispielsweise systematisch Profilbildung (Location Profiling) durchführen und Rückschlüsse auf sensitive Informationen über Personen (z. B. Vorlieben, Interessen, Gewohnheiten) erleichtern. In drei Veröffentlichungen[32] gehen wir der Frage nach, wie diesem Bedrohungspotenzial entgegenzuwirken ist und Fahrzeugnutzende technisch befähigt werden können, ihr Recht auf informationelle Selbstbestimmung effektiv auszuüben. Hieraus leitet sich eine weitere zentrale Forschungsfrage ab: Wie können entstehende datengetriebene Dienstleistungen, Produkte und Geschäftsmodelle im Automotive-Kontext gestaltet werden, damit inhärent eine Privatheit schützende Erhebung und Verarbeitung personenbezogener Daten technisch gewährleistet ist?

[29] Miller und Valasek (2015).

[30] Miller und Valasek (2014), Garcia et al. (2016), Lang et al. (2016) und Checkoway et al. (2011).

[31] Miller und Valasek (2013) und Greenberg (2016).

[32] Singh und Simo Fhom (2016), Simo Fhom et al. (2019) und Franke et al. (2021).

4.4 Bedrohungs- und Überwachungspotenziale in öffentlichen WLAN-Infrastrukturen

In öffentlichen WLANs existiert eine Vielzahl von Ausspäh- und Zugriffsmöglichkeiten auf personenbezogene oder -beziehbare Daten.[33] Während sich passive Angreifer auf das Abhören und Abspeichern des Datenverkehrs im WLAN beschränken, können aktive Angreifer explizit in die Kommunikation eingreifen und die Integrität des Datenverkehrs kompromittieren. WLAN-Infrastrukturen werden häufig auch von einzelnen Gewerbetreibenden bereitgestellt und selbst verwaltet. Darüber hinaus gibt es aber eine Vielzahl von Dienstleistern, die die Bereitstellung der Infrastruktur übernehmen und Gewerbetreibende zudem mit Analysen über ihre Kundschaft versorgen. Die daraus resultierenden Möglichkeiten für Tracking und Profilbildung können zwar durchaus auch positive Auswirkungen haben und von den Nutzerinnen und Nutzern gewünscht sein, wenn ihnen beispielsweise auf Grundlage von Standortdaten und Bewegungsprofilen spezielle Angebote gemacht werden oder ein gesuchtes Produkt im Supermarkt schneller gefunden werden kann. Gleichzeitig birgt diese Art des meist intransparent praktizierten Kundentrackings auf Basis von WLAN-Signalen aber auch eine Reihe von Privatheitsrisiken:[34] Der Zugriff der WLAN-Betreibenden auf Konto- und Registrierungsdaten, gerätespezifische und ableitbare Daten sowie auf Nutzungs- und Verhaltensdaten kann sich negativ auf die informationelle Selbstbestimmung auswirken und etwa zum Verlust bzw. zu einer Einschränkung der Entscheidungsfreiheit führen, sehr weitgehende elektronische Überwachung ermöglichen und die Offenlegung sensibler oder vertraulicher Daten zur Folge haben. Auf diese Weise können Nutzerinnen und Nutzer bei ihrem Weg durch eine Stadt auf Schritt und Tritt verfolgt, auch unbescholtene Demonstrationsteilnehmer identifiziert, und selbst sensibelste Kommunikationsinhalte und Persönlichkeitsmerkmale offengelegt werden.

5 Innovationspotential der Digitalisierung und des Privatheitsschutzes

Fortschreitende Digitalisierung durch Big Data beeinflusst alle Lebens-, Wirtschafts- und Verwaltungsbereiche, sie verspricht gesellschaftlichen Fortschritt und gestaltet die Arbeitsplätze der Zukunft. Sie verspricht Neuerungen im medizinischen

[33] Eisele et al. (2017).

[34] Gassen und Simo Fhom (2016).

Bereich,[35] sie soll die Arbeitswelt von Routineaufgaben befreien können,[36] umfangreichere und vielfältigere Datenanalysen sind möglich und gezieltere Auswertungen und Optimierungen von Prozessen werden versprochen.[37]

> *„In der jüngsten Gegenwart ist Big Data zum populären Schlagwort aufgestiegen und wird oftmals als Sammelbegriff für digitale Technologien verwendet, die in technischer Hinsicht für eine neue Ära digitaler Kommunikation und Verarbeitung und in sozialer Hinsicht für einen gesellschaftlichen Umbruch verantwortlich gemacht werden."*[38]

Big Data beschreibt auf der einen Seite das exponentielle Wachstum der Menge an Informationen, die gesammelt und ausgewertet werden können, wie auch eine neu entstehende Vielfalt an Datenquellen und – typen.[39] Diese zunehmende Menge an Daten, die erhoben, verarbeitet und gespeichert werden[40] eröffnet neue Größenordnungen. Diese neuen Größenordnungen, der Grad der Vernetztheit und der Mehrwert der daraus generierten Daten bieten ein noch nicht da gewesenes Potenzial. Mit der zunehmenden Durchdringung von Gesellschaft und Lebenswelt durch digitale Technologien entstehen andererseits auch gesellschaftliche Grenzverschiebungen und Verwischungen traditioneller Vorstellungen von Privatheit und Öffentlichkeit. In rechtlicher Hinsicht resultieren hieraus weitreichende Eingriffe und oftmals Verstöße gegen geschützte Grundrechte.

Wandel und Veränderungen sind allgegenwärtig und nicht wegzudenken, sie sind sogar von Nöten für eine sich evolvierende Gesellschaft bzw. Menschheit. Dieser Wandel in und durch Technik birgt Potenziale, die in einer Weise gestaltet werden können, dass gesellschaftliche Werte widergespiegelt und geschützt werden. Grundsätzlich gilt es, Datensparsamkeit ernst zu nehmen,[41] um vor nachteiliger Datenverarbeitung zu schützen, denn „non-existent data needs no protection".

5.1 Volkswirtschaftliche Ebene

Am 25.05.2018, dem Tag des vollständigen Inkrafttretens der Datenschutzgrundverordnung, wird Bitkom-Präsident Berg mit den Worten zitiert: *„Datenschutz-*

[35] BMBF (2020).
[36] Absenger et al. (2016).
[37] Kraus (2013).
[38] Reichert (2014).
[39] Callegaro und Yang (2018).
[40] Roßnagel et al. (2017, S. 3).
[41] Simo Fhom (2015).

regeln dürfen nicht zum Hemmschuh für sinnvolle und notwendige Innovationen werden".[42] Im Jahr 2019 betonte Ulrich Kelber, der Bundesbeauftragte für den Datenschutz: *„Datenschutz ist kein Hemmschuh für Innovationen, er förderte diese sogar, wenn die Nutzer Vertrauen in die Sicherheit neuer Technologien haben."*[43] Einerseits wird argumentiert, dass technische Innovationskraft sich entfalten können muss und hierfür der Zugang und die Verarbeitung – auch personenbezogener Daten – notwendig ist. Andererseits ist Innovation nur dann möglich, wenn sie in das gesellschaftliche Wertesystem – gerade auch bezüglich informationeller Selbstbestimmung – eingebettet ist.

5.2 Unternehmen

Die Erschließung neuer Geschäftsfelder und -modelle durch Unternehmen sowie zunehmende Effizienzgewinne beruhen weitestgehend auf dem Handel mit Daten, personalisierter Werbung und generell auf möglichst umfassenden Auswertungen – (auch) mit Hilfe maschinellen Lernens. Die dabei angewendeten Methoden beziehen sich meist auf Big Data Analysen von bestehenden, potenziellen oder perspektivischen Kundendaten.

Doug Laney beschrieb Big Data erstmals durch die Eigenschaften Volume, Velocity, Variety (kurz „3V").[44] Diese drei Eigenschaften sind charakterisierend für Big Data: in digitaler Form vorliegende Daten großer Masse („Volume"), die schnell entstehen („Velocity") und sehr unterschiedlicher Art und Herkunft sein können („Variety").[45] Teilweise werden weitere Aspekte hinzugefügt und mit einem „V" beschrieben, beispielsweise die Folgenden: *Veracity* steht für Vertrauenswürdigkeit der Daten oder der gezogenen Schlüsse. *Value* betont, dass Big Data letztendlich immer eine Wertschöpfung der Daten beabsichtigt. *Visualization* stellt die intuitive Darstellung der Ergebnisse heraus.[46]

Unternehmen haben eine intrinsische Motivation für die Einhaltung der Datenschutzauflagen und auch darüber hinausgehende Maßnahmen: Sie erfahren Nachteile wie Reputationsverlust, wenn sie berechtigte, kodifizierte und/oder konsensuale Privatheitsbedürfnisse von Individuen nicht beachten würden.

---

[42] BITKOM (2020b).
[43] Kelber (2019).
[44] Laney (2001).
[45] Laney (2001).
[46] Steinebach et al. (2015, S. 21).

5.3 Grundrechte auf Datenschutz und informationelle Selbstbestimmung

Der Schutz von personenbezogenen Daten ist als Grundrecht (Art. 8 GRCh) im europäischen Recht verankert und ist damit für die Rechtsordnung und demokratische Prozesse von wesentlicher Bedeutung. In Deutschland hat das Bundesverfassungsgericht 1983 mit dem Volkszählungsurteil das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) definiert. Das Recht umfasst die Befugnis des Einzelnen grundsätzlich selbst über Preisgabe und Verwendung seiner persönlichen Daten und Offenbarung von Lebenssachverhalten zu bestimmen, sowie den Schutz vor einer unbegrenzten Erhebung, Speicherung, Verwendung und Weitergabe von persönlichen Daten[47] Das Gericht erkannte an, dass es für die Freiheit selbstbestimmte Entscheidungen treffen zu können unerlässlich ist, einen Sachverhalt zu überschauen und Sicherheit darüber zu haben welche Informationen in einem bestimmten Bereich und sozialen Umfeld über einen bekannt sind sowie welche Verhaltensweisen und Informationen überhaupt gespeichert werden. Diese Freiheit wiederum ist nicht nur Voraussetzung für die persönliche Entwicklung des Einzelnen, sondern auch für die Ausübung anderer Grundrechte und Mitwirkungsmöglichkeiten an freiheitlich demokratischen Prozessen und damit Grundlage für eine demokratische Gesellschafts- und Rechtsordnung selbst[48]. Durch die Möglichkeiten der automatisierten Verarbeitung in „modernen“ Informationssystemen, den Zugriffs- und Einflussnahmemöglichkeiten hierauf, sowie der Erstellung von Persönlichkeitsbildern werden diese Freiheiten und Befugnisse zunehmenden gefährdet[49].

Der in der DSGVO festgeschriebene Grundsatz der Transparenz (Art. 5 Abs. 1 lit. a DSGVO) in der Datenerhebung und -verarbeitung soll Betroffene in die Lage versetzen Verarbeitungsprozesse zu verstehen und in Frage zu stellen, sowie Kontrolle über ihre Daten auszuüben.[50] Die Kontrolle von personenbezogenen Daten durch den Betroffenen lässt sich als Kernelement der DSGVO ausmachen (ErwG 7 und 68 DSGVO).

5.4 Technische Umsetzung von Regulierung

Der amerikanische Verfassungsrechtler Lawrence Lessig schrieb bereits 1990, dass der Cyberspace ein neues Verständnis von Regulierung erfordert, das über die Regu-

[47] BVerfG NJW 1984, 419, 422, Rn. 147.

[48] BVerfG NJW 1984, 419, 422, Rn. 146.

[49] BVerfG NJW 1984, 419, 421, Rn. 145.

[50] Article 29 Data Protection Working Party (2018), Rn. 2/4.

lierung durch Gesetz hinausgeht. Im Cyberspace erfolgt Regulierung vor allem durch den Code des Cyberspace. Dies meint, dass die Software und Hardware, die den Cyberspace zu dem machen, was er ist, auch den Cyberspace regulieren, so wie er ist. Er führt weiter aus, dass Code hierbei gleichzeitig die größte Bedrohung als auch das größte Versprechen für freiheitliche Ideale darstellt. Der Cyberspace kann so konstruiert, gestaltet und codiert werden, dass Werte, die eine Gesellschaft für grundlegend hält, geschützt werden oder eben sodass diese Werte untergehen. Code wird niemals entdeckt oder erfunden, er wird immer von Menschen gemacht.[51]

Technik kann also das oben beschriebene Spannungsverhältnis zwischen gesetzlich reguliertem Privatheitsschutz sowie digitalem Innovationspotential auflockern oder gar auflösen durch die Entwicklung von proaktiven, normkonformen und Wertschöpfung unterstützenden Werkzeugen und Verfahren. Dazu wird in der Informatik insbesondere verstärkt auf Ansätze zur Durchsetzung des Rechts auf informationelle Selbstbestimmung und zur Nutzerermächtigung gesetzt, die sich allgemein unter dem Begriff der „Privacy-enhancing Technologies“ (PETs) zusammenfassen lassen. Dabei lassen sich zwei Kategorien unterscheiden: zum einen die „klassischen“ datenschutzfördernden PETs, zum anderen umfassen sie sog. „Transparency-enhancing Technologies“ (TETs). Dadurch werden Betroffene unterstützt Kontrolle und ihre Rechte über ihre Datenpreisgabe und - verarbeitung auszuüben, sowie Risiken und Bedrohungen zu erkennen.[52] PETs setzen somit zum einen direkte Anforderungen aus der DSGVO technisch um, zum anderen fördern sie privatheitsbewusstes Verhalten von Nutzern und ermächtigen diese dazu, aktive Teilnehmer in Datenmärkten zu werden. TETs, die Transparenz bezüglich des digitalen Fußabdrucks liefern, sind hierzu auf spezielle Weise geeignet, wie die Gestaltungsvorschläge in Abschn. 6 aufzeigen.

5.5 Nutzung des technischen Fortschritts für Privatheitsinnovationen

Die im nächsten Abschnitt präsentierten Vorschläge greifen folgende Empfehlungen des Dagstuhl-Manifests[53] aus 2011 auf: Forschung sollte kreative, innovative Instrumente wie „Privatheits-Assistenzsysteme“ hervorbringen, damit Nutzende ihre informationelle Selbstbestimmung durch die Verbesserung der Transparenz praktikabel verwirklichen können. Die Forschung sollte zudem vorausschauend

[51] Lessig (2006).

[52] Fischer-Hübner et al. (2011, S. 7).

[53] Fischer-Hübner et al. (2011).

„known unknowns“,[54] also die möglichen Veränderungen der technologischen und gesellschaftlichen Rahmenbedingungen antizipieren und sog. blue skies researches durchführen.

Die Kritik, dass technische Datenschutzmechanismen per se digitale Innovationen verhindern, ist dabei zurückzuweisen. Denn es zeigt sich, dass datengetriebene Innovationen im Rahmen der Anforderungen der DSGVO möglich sind. Auch privatheitsfördernde Technologien können innovativ und wirtschaftlich erfolgreich sein.[55]

Mit den nachfolgenden Gestaltungsvorschlägen wird beispielhaft aufgezeigt, wie Technik für Privatheitsinnovationen im Sinne des Manifests genutzt werden kann.

6 Gestaltungsvorschläge

Die drei Gestaltungsvorschläge wurden vom Fraunhofer SIT im Forum Privatheit als Forschungsgegenstand ausgewählt, weil sie alle drei beispielhaft eine Verbesserung der Transparenz bezüglich des digitalen Fußabdrucks liefern (im Sinne der Empfehlung des Manifests) und damit dazu beitragen, dass die Nutzenden ermächtigt werden, ihre informationelle Selbstbestimmung im aktuellen technologischen und gesellschaftlichen Umfeld effektiv durchzusetzen. Dies ist das verbindende Konzept in den drei Gestaltungsvorschlägen, welche jeweils unterschiedlich in ihrer Ausrichtung sind. Me&MyFriends (siehe Abschn. 6.1) und WallGuard (siehe Abschn. 6.2) unterstützen Transparenzbedürfnisse der Privatheit von Nutzenden in Online Social Networks (OSN) während Metaminer (siehe Abschn. 6.3) Transparenzbedürfnisse von Nutzenenden mobiler Ökosysteme unterstützt.

6.1 Me&MyFriends

Das Erfordernis nach innovativen Werkzeugen, die Internetnutzern Transparenz über Privatheitsrisiken verschaffen, ergibt sich aus der Datenschutz-Grundverordnung sowie anderen internationalen Datenschutzbestimmungen. Die unbeabsichtigte, unfreiwillige Offenlegung sensibler Informationen birgt die Gefahr einer möglichen Untergrabung des grundgesetzlich garantierten Rechts auf informationelle Selbstbestimmung und einer achtungswürdigen Selbstdarstellung. Eine solche Offenlegung kann dadurch stattfinden, dass ein Dritter bzw. Unbefugter in der Lage

[54] Fischer-Hübner et al. (2011, S. 15).

[55] Roßnagel et al. (2017, S. 11).

ist, aus digitalen Spuren, Identitäts-, Persönlichkeits- und Verhaltensmerkmale, die eine natürliche Person geheim halten möchte, zu schlussfolgern. Eine zentrale Rolle spielen dabei die i. d. R. kaum vorhandenen Möglichkeiten für Nutzer, sich Kenntnisse darüber anzueignen, wie öffentlich gemachte Informationen oder Handlungen zu Schlussfolgerungen führen können, die intime, vermeintlich private Informationen oder falsche Annahmen bzw. Vermutungen offenbaren.

Um die eigene Privatsphäre zu wahren und das Durchsickern sensibler Informationen in sozialen Netzwerken verhindern zu können, ist das Vorhandensein eines Bewusstseins für Inferenz-Risiken bzw. das Wissen über das Gefahrenpotenzial aus den eigenen, vermeintlich unkritischen digitalen Spuren entscheidend. Da dieses Wissen für den durchschnittlichen Nutzer sozialer Netzwerke nicht zugänglich oder offensichtlich ist, besteht Bedarf nach einer technologischen Plattform, die es Nutzern ermöglicht, eine Selbsteinschätzung zum Datenschutz durchzuführen. Das Selbstbewertungs-Tool soll Nutzer ermächtigen, detailliertes Wissen über hinterlassene digitale Spuren zu erlangen und eine automatisierte Bewertung potenzieller Inferenzrisiken durchzuführen. Dadurch kann der Einzelne in die Lage versetzt werden, geeignete Maßnahmen zu ergreifen, um weitere Rückschlüsse zu verhindern. Ziel hierbei ist es, Nutzer in die Lage zu versetzen, ermessen zu können, was aus den von ihnen selbst oder ihren Kontakten bereitgestellten Informationen über sie gefolgert werden könnte.

Eine solche Plattform fördert das Recht auf informationelle Selbstbestimmung, indem es Transparenz schafft über mögliche unerwünschte als auch unbekannte Schlussfolgerungen, die sich aus vermeintlichen nicht-sensitiven Social Media Daten ergeben. Damit unterstützt es die Möglichkeit von Nutzern, bewusste Entscheidungen über die Offenlegung bestimmter Daten und ihres Social Media Verhaltens insgesamt zu treffen.

Architektur Das Client-Server basierte Werkzeug nutzt statistische Methoden der Datenanalyse, um eine Gruppe verbundener Nutzer zu ermächtigen, Inferenzrisiken für sensible Attribute, auf der Grundlage von aggregierten Informationen aus ihren öffentlichen Social-Network-Profilen und Freundschaftsverbindungen, zu quantifizieren. In der Tat ist die privatsphärefördernde Plattform eine zwischengeschaltete Komponente zwischen dem Nutzer und seinen sozialen Netzwerken wie in Abb. 1 zu sehen ist.

Das Me&MyFriends-Framework umfasst Module und Mechanismen zur Sammlung, Aggregation und Analyse von Daten aus verschiedensten Sozialen Netzwerken. Ein Inferenz-Modul erlaubt die Quantifizierung und Visualisierung möglicher unerwünschter Rückschlüsse aus den öffentlichen Ego-Graphen. Hierzu wird ein Naive Bayes basierter Inferenzalgorithmus genutzt, der zuvor einer

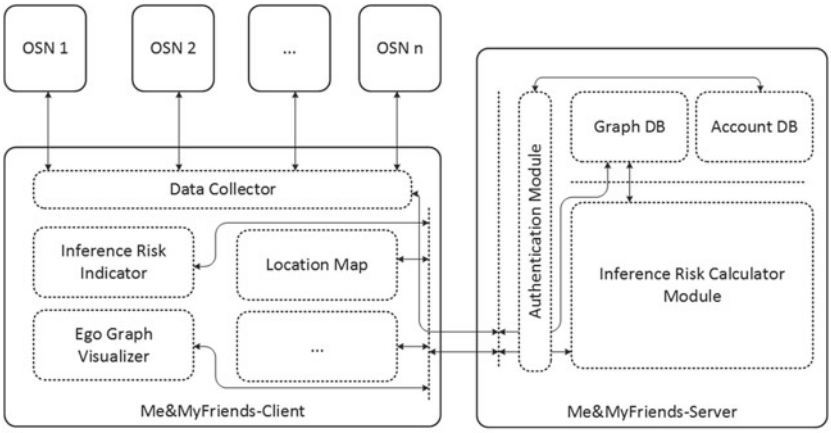

Abb. 1 Me&MyFriends – Architektursicht

experimentellen Evaluation mit drei Datensätzen von Facebook und Twitter unterzogen wurde. Die Ergebnisse der Evaluation weisen auf ein konkurrenzfähiges Modell im Vergleich zu mehreren Baseline Algorithmen hin. Ein Proof-of-Concept des Me&MyFriends-Frameworks in Form einer Web Anwendung implementiert Verbindungen zu den Sozialen Netzwerken Facebook und Twitter. Als solche besteht die Me&MyFriends-Architektur aus zwei Hauptkomponenten: Me&MyFriends-Client und Me&MyFriends-Server. Der Datenfluss kann wie folgt zusammengefasst werden: Ein Nutzer registriert sich bei der Me&MyFriends-Plattform über eine Client-Anwendung die es ihm ermöglicht Informationen aus unterschiedlichen sozialen Netzwerken abzurufen und andere Teilnehmer einzuladen, die Me&MyFriends-App zu nutzen und ihre öffentlichen Informationen ebenfalls abzurufen. Alle abgerufenen Informationen, d. h. Ego-Graphen der Me&MyFriends-Nutzer, werden zur Analyse an einen zentralen Server weitergeleitet. Dort werden auf Grundlage der von allen Teilnehmern bereitgestellten Informationen Attribut-Inferenz-Risiken berechnet und Empfehlungen für Korrekturmaßnahmen generiert. Über die Client-Webanwendung bekommt der Nutzer anschließend personalisierte Analyseergebnisse und Empfehlungen angezeigt.

Inference Model Es wird ein gewichtetes Naive-Bayes'sches Modell verwendet, um die Wahrscheinlichkeit für Attribut-Inferenz, basierend auf den 1-Hop-Nachbarn des Nutzers und den von ihm bereitgestellten Attributwerten im Ego-Graphen zu berechnen. Die Attributgewichtung sollte quantitativ die Abhängigkeit zwischen

der Bedeutung des Attributs für den Nutzer und der Bedeutung für die Verbindungen/Alter Egos des Nutzers erfassen. Fünf Hilfsfunktionen sind entscheidend bei der Gewichtung von Attributen, die mit den Details aus dem Ego-Graphen eines Nutzers berechnet werden können. Die Zusatzfunktionen erfassen Metriken aus fünf Kategorien: Die Bedeutung eines bestimmten Freundes/Alter Egos, die Popularität eines Attributs und eines bestimmten Attributwerts für einen Nutzer und die Bedeutung eines bestimmten Attributs und Attributwerts für den Nutzer.

Gesamtschätzung des Inferenzrisikos Unter Berücksichtigung der oben genannten Funktionen und Überlegungen wird die Gesamtschätzung des Inferenzrisikos definiert, das Gesamtniveau der Korrektheit bei der Rekonstruktion des Profils des Nutzers durch Dritte. Dies geschieht durch die Kombination der Inferenzrisikoschätzung,

$$I(a^k) = \max_{1 \le r \le |C|} P\left(\widehat{v^r_{a^k} | \theta(a^k)}\right) \omega(a^k) \phi\left(v_{a^k}\right) \tag{1}$$

jedes einzelnen verborgenen Attributs a^k und der Modellierung der Gesamtschätzung des Inferenzrisikos für den Zielnutzer U, die durch $I(U)$ als folgende logistische Funktion angegeben wird:

$$I(U) = 1/\left(1 + exp\left(-\partial \cdot \sum_{k=1}^{|H(U)|} I(a^k)\right)\right) \tag{2}$$

wobei $\partial = 1/|H(U)$ und $\omega(a^k)$ das Gewicht des sensitiven Attributs ist. Wir definieren $C = \left\{v^1_{a^k}, v^2_{a^k}, \cdots, v^m_{a^k}\right\}$ als die endliche Menge von allen möglichen Werten, die dem Attribut a_k vergeben werden kann. $\theta(a^k) = \left\{\theta^j_{a^k} = \left\langle U^j, (a^k, v_{a^k})\right\rangle : \forall_{1 \le j \le n}\right\}$ ist die Menge aller Beobachtungen in Bezug auf das Attribut a^k, die ein Widersacher aus einem aggregierten Ego-Netzwerk $G = (E, V, \varphi)$ machen kann, wobei $n = |V|$ und t die Gesamtzahl der möglichen Attribute in jedem Benutzer U^j Profil ist. Es ist zu beachten, dass sich die Inferenzrisikoschätzung $I(a^k)$ von a^k auf die Wahrscheinlichkeit bezieht, dass ein Gegner den verborgenen Wert $v^r_{a^k}$ korrekt ableiten kann. Das Gesamtinferenzrisiko für den Zielnutzer $U - I(U)$ – nimmt Werte im Bereich [0, 1] an. Wie oben erwähnt bezeichnet $H(U)$ die Menge der herleitbaren Profilattribute, die entweder fehlen (d. h. vom Zielnutzer U nicht angegeben wurden) oder für Dritte einfach nicht sichtbar sind.

Gesamt-Privatheits-Score Der Privatheits-Score des Zielnutzers U, $Score(U)$, bezieht sich auf das Gesamtniveau der Unsicherheit des Gegners (d. h. die Gesamtfehlerwahrscheinlichkeit) in Bezug auf die Ableitung der korrekten Werte der verborgenen Attribute von U. Dies ergibt die folgende Formel:

$$Score(U) = 1 - I(U) \tag{3}$$

Damit wird intuitiv die Tatsache erfasst, dass die Privatsphäre des Nutzers umso besser gewahrt wird, je niedriger $I(U)$ (der Grad des Vertrauens eines Dritten in die korrekte Schätzung der Werte versteckter Attribute auf der Grundlage des oben beschriebenen Inferenzmodells) ist.

Schlussfolgerung, Grenzen und zukünftige Arbeiten Die aktuelle Version des Me&MyFriend-Frameworks ist als zentralisierte Cloud-basierte Lösung realisiert – das vorgeschlagene Inferenz-Model ist auf Serverseite implementiert und wird dort ausgeführt. Als Folge dessen gilt der Me&MyFriends-Server als sogenannter Single-Point-of-Failure, über den Nutzer nur bedingt Kontrolle ausüben können. Dementsprechend müssen Nutzer dem Server und allen darauf laufenden Prozessen vollständig vertrauen. Für die zukünftige Arbeit sind eine Erweiterung und Verbesserung des Frameworks in Bezug auf zahlreiche Aspekte geplant. Darunter fallen folgende Aspekte:

Verbesserter Ego-Graph-Aggregationsprozess Da Daten aus mehreren sozialen Netzwerken verwendet werden, muss ein ausgefeilterer Ansatz zum Abgleich von Entitäten über diese Netzwerke hinweg erarbeitet werden. Dies gilt sowohl für das Erkennen von Attributen als auch von einzelnen Entitäten. In der Tat kann schon die (String-)Repräsentation von Profilattributen, z. B. eines Standortes (bzw. Arbeitgeber, Hochschule, ...), in verschiedenen sozialen Netzwerken in Bezug auf Sprache, Abkürzungen und vielen weiteren Aspekten variieren. Mögliche Abhilfe könnten Werkzeuge aus dem Kontext des Natural Language Processing, z. B. Named Entity Recognizer (NER),[56] schaffen. Mittels NER in Kombination mit entsprechenden semantischen Kategorien, lexikalischen Ressourcen und Datenbanken sollen aus Freitextbeschreibungen Attribute wie Orte, Personen, Organisationsnamen, Datums- und Zeitangaben oder Berufsbezeichnungen extrahiert werden können. Des Weiteren soll untersucht werden inwieweit die so extrahierten Attribute als Input eines holistischen Ansatzes zum Abgleich von Ego-Graphen, in Kombination

[56] Nadeau und Sekine (2007).

mit Textähnlichkeitsmetriken[57] und Graph Embeddings,[58] zu berücksichtigen sein könnten. Ein solcher holistischer Ansatz für Ego-Graphen-Ähnlichkeitsanalysen soll zur Steigerung der Effizienz, Präzision und Effektivität des Ego-Graph-Aggregationsprozess führen.

Verbesserung des Inferenzmodells Die Verbesserung des Vorhersagemodells und das Finden alternativer Ansätze, z. B. überwachte Algorithmen, ist als weitere zukünftige Arbeit in Betracht zu ziehen.

Privacy-Preserving Me&MyFriends-Server Die unserem Framework zugrundeliegende Client-Server-Architektur stellt ein offensichtliches Problem dar – Nutzer und der Me&MyFriend-Anbieter verlieren Kontrolle über höchst sensitive Daten. Für Nutzer sind dies vor allem Ego-Graphen ihrer sozialen Netzwerke, die aus verschiedenen Domänen erfasst und zum Server geschickt wurden. Aus Sicht des Me&MyFriend-Anbieters stellt sich das Problem überwiegend hinsichtlich einer möglichen Gefährdung des Rechts auf geistiges Eigentum (Intellectual Property Rights). Die Me&MyFriends-Software (inkl. das Inferenz-Modell) muss über eine fremde Cloud-basierte Infrastruktur betrieben und einem halbwegs vertrauenswürdigen (engl. semi-trusted) Infrastruktur-Betreiber quasi anvertraut werden. Daraus ergibt sich die Notwendigkeit für eine neue dezentrale und privatheitsfördernde Plattform. Mit einer solchen Plattform ist das Hochladen von Nutzerdaten aus Sozialen Netzwerken auf einen nicht vertrauenswürdigen Server nicht mehr erforderlich. Auf Nutzerseite werden in einer sog. Trusted Execution Environment (TEE),[59] aggregierte Ego-Graphen rekonstruiert und das Inferenzmodell und weitere sensitive Daten aufbewahrt bzw. ausgeführt. Auf Serverseite werden ausschließlich allgemeine Parameter für eine Community-basierte Aktualisierung und Verteilung des Inferenzmodells bereitgestellt.

Usability Nicht zuletzt soll die Proof-of-Concept Implementierung abgeschlossen und im Hinblick auf Benutzerfreundlichkeit und Leistung erprobt werden. Erste Ergebnisse in dieser Richtung sind kürzlich auf der internationalen wissenschaftlichen Konferenz IEEE Infocom 2021 eingereicht und akzeptiert worden.[60]

[57] Bär et al. (2013).
[58] Cai et al. (2018).
[59] Sabt et al. (2015).
[60] Kohlhammer et al. (2021).

6.2 WallGuard

Zahlreiche Literaturquellen aus der Verhaltensökonomie und der medienpsychologischen Forschung weisen auf die Tatsache hin, dass eine wachsende Zahl von Social-Media-Nutzern Bedenken bzgl. der Wahrnehmung ihrer Erscheinung in der Online Öffentlichkeit haben. Wang et al. (2011) verknüpfen diese Problematik mit Ängsten der Nutzenden bezogen auf die Veröffentlichung von Inhalten zu möglicherweise kontroversen Themen mit unbeabsichtigter Audienz und den daraus folgenden Konsequenzen. Hierunter fallen u. a. Reue, Peinlichkeiten und die Untergrabung des eigenen Rechts auf informationelle Selbstbestimmung. In diesem Projekt fokussierten sich die Forschungsarbeiten in einem ersten Schritt auf Ansätze zur automatisierten Erkennung kontroverser Social-Media-Beiträge die möglicherweise ein späteres Bereuen nach sich ziehen könnten. Entwickelt wurden eine Reihe von Multi-Label-Modellen die Soziale-Medien-Texte in Facebook und Twitter entlang acht empirisch validierter Kategorien von auf Bedauern bezogenen Themen klassifizieren: Alkohol und Drogenkonsum (T1), Misogynie (T2), Familienangelegenheiten (T3), Politik (T4), Profanität und Obszönität (T5), Religion (T6), Sex (T7), und Arbeitsumfeld und Arbeitgeber (T8).

Architektur Um den Benutzern zusätzliche Hilfe beim Umgang mit auf OSN veröffentlichten Inhalten zu bieten und damit die Forderung nach einer detaillierteren Datenschutzlösung für unerwünschte/bedauerliche Offenlegungen zu beantworten, müssen zwei Hauptszenarien betrachtet werden, siehe Abb. 2. Neue Inhalte auf der persönlichen OSN-Seite eines Benutzers können entweder vom Benutzer selbst (Anwendungsfall 1) oder von den OSN-Freunden des Benutzers (Anwendungsfall 2) generiert werden. Während Posts, die vom Kontoinhaber selbst verfasst wurden, möglicherweise zu Reue und Bedauern führen können (weil Sie selbst der Autor sind), ist Reue durch die Verknüpfung mit den Posts von Freunden ebenfalls möglich.

Als Lösung, die beide Szenarien berücksichtigt, haben wir WallGuard entwickelt – ein technisches Tool, welches Social-Media-Nutzende unterstützen soll, informierte Offenlegungsentscheidungen treffen zu können. Informiert durch empirische Befunde, argumentieren wir, dass eine automatisierte Festlegung kontroverser, bedauerlicher bzw. peinlicher Veröffentlichungen sowie die Identifizierung und Einschränkung der entsprechenden Audienz wichtige Merkmale einer derartigen technischen Lösung sein müssen. Um die eingeführten Szenarien abzudecken und die identifizierten Anforderungen zu erfüllen, besteht WallGuard aus neun Komponenten, die in Abb. 3 dargestellt und nachfolgend erläutert werden. Die einzelnen Komponenten können wie folgt zusammengefasst werden:

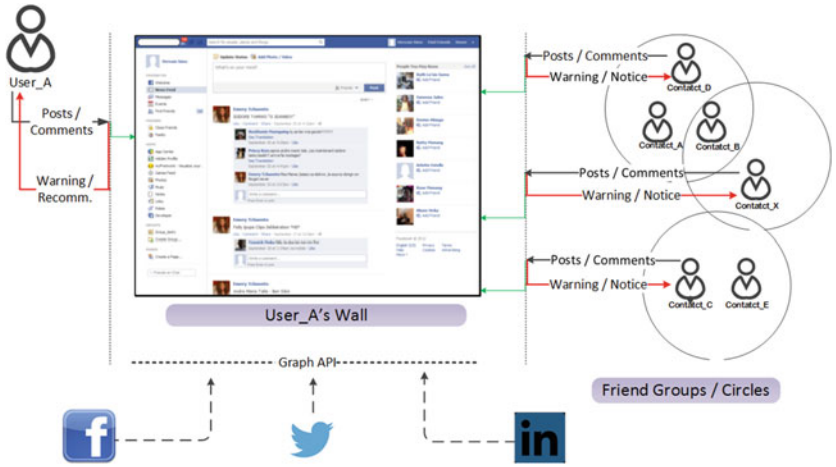

Abb. 2 WallGuard Szenarien

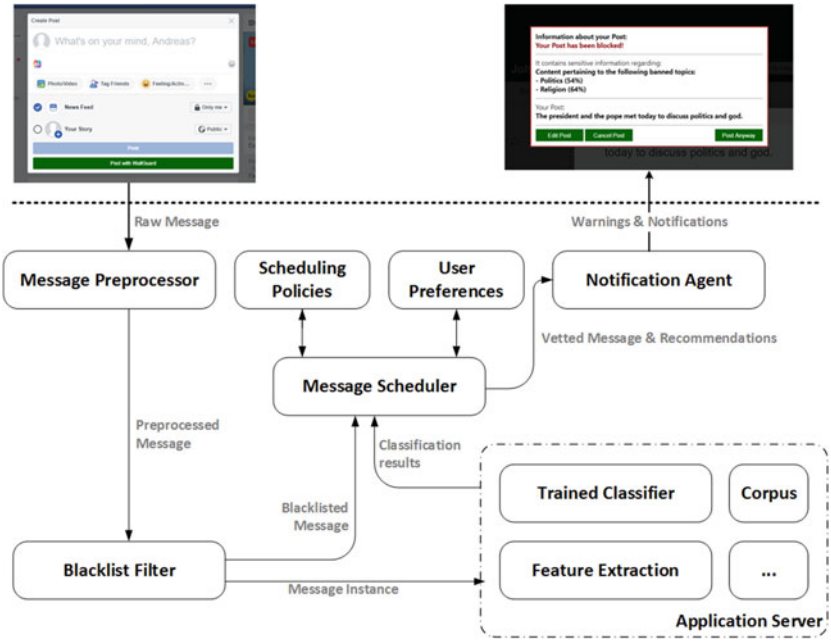

Abb. 3 Überblick über die Architektur des WallGuard Frameworks

User-Agent Auf der Clientseite zeigt der Benutzeragent (in diesem Fall der Webbrowser) den vom OSN-Server und WallGuard empfangenen Inhalt an und ist gleichzeitig für die Verarbeitung aller Anweisungen (Eingaben) des Benutzers verantwortlich. Der Benutzeragent dient als Schnittstelle zwischen der tatsächlichen Person und dem Internet.

Nachrichten-Preprocessor Da redundante Informationen in einer Nachricht (z. B. Satzzeichen) typischerweise nur den Klassifizierungsprozess behindern, entfernt diese Komponente in einem ersten Schritt solche Informationen und standardisiert jeden eingehenden Text. Auf diese Weise wird sichergestellt, dass jeder Text allen noch kommenden Komponenten im gleichen Format präsentiert wird. Daher dient der Nachrichten-Preprocessor auch als Mittel, um Fehler aufgrund möglicher Sonderzeichen oder Formatverletzungen zu vermeiden. Zusätzlich werden während dieses Prozesses Stoppwörter (z. B. „and“, „or“) entfernt und alle verbleibenden Wörter werden gestoppt, wodurch die Darstellung der Nachricht auf ihre relevanten Daten reduziert und letztendlich die Klassifizierung erleichtert wird.

Blacklist Filter Der Blacklist Filter verwendet eine vordefinierte Liste von Wörtern, die als unangemessen und inakzeptabel angesehen werden können. Mit dem Filter wird jede eingehende Nachricht mit dieser Liste verglichen. Wenn mindestens eines dieser Wörter vorhanden ist, wird die gesamte Nachricht markiert. Die Liste besteht aus Standardwörtern und kann vom Benutzer bearbeitet werden, indem entweder vorhandene Wörter entfernt oder neue Wörter hinzugefügt werden.

Benutzerdefinierte Richtlinien Wie bereits erwähnt, hat der Benutzer die Möglichkeit, die Blacklist zu bearbeiten. Darüber hinaus kann der Benutzer selbst entscheiden, über welches der eingeführten potenziell bedauerlichen bzw. unangemessen Themen er benachrichtigt und von der Wand verbannt werden möchte. Diese Regeln sind in den benutzerdefinierten Richtlinien enthalten.

Scheduling Policies Die Richtlinien definieren, welche allgemeinen Schritte in einem der möglichen Szenarien ausgeführt werden sollen. Unabhängig davon, ob ein Beitrag aufgrund unangemessener Wörter auf die schwarze Liste gesetzt wird oder eines der vom Benutzer gesperrten Themen enthält, werden in den Scheduling Policies die erforderlichen Maßnahmen aufgeführt.

Message Schedule Der Message Scheduler/Nachrichtenplaner ist die zentrale Einheit in WallGuard, die die unterschiedlichen Ergebnisse der verschiedenen Komponenten validiert und mithilfe der oben beschriebenen Planungsrichtlinien

Tab. 1 Verwendete Methoden und Bibliotheken zur Merkmalsextraktion

Feature Type	Extraction Method	Used Libraries
Word Occurrence	tf-idf	WEKA (StringToWordVector & WordTokenizer)
	word2vec	Deeplearning4j word2vec
Semantic Features	word2vec	Deeplearning4j word2vec
Basic Word N-Gram	n-gram tokenizer	WEKA (StringToWordVector & NGramTokenizer)

die erforderlichen Aktionen an alle erforderlichen Komponenten weiterleitet (insbesondere dem Notification Agent/Benachrichtigungsagenten signalisiert, was angezeigt werden soll).

Feature Extraction (Merkmalsextraktion) Auf der Grundlage des Nachrichten-Preprocessor werden bei der Merkmalsextraktion identifizierbare Informationen aus einem Text herausgesucht, um Merkmale zu erhalten, die die verschiedenen Themen eindeutig darstellen. Tab. 1 fasst die in diesem Projekt verwendeten Feature-Extraktionsmethoden zusammen.

Post Classifier Nach dem erfolgreichen Extrahieren der Features aus einem Text werden diese Features vom Klassifizierer verwendet, um das Thema oder die darin enthaltenen Themen zu identifizieren. Da sich viele Texte in Themen überschneiden und viele Funktionen verschiedenen Themen zugewiesen werden können (z. B. kann das Wort „Buch“ eine Aktion sein, wenn es als Verb verwendet wird oder etwas, das gelesen werden kann, wenn es als Substantiv verwendet wird), befasst sich die Themenklassifizierung mit der Wahrscheinlichkeit. Ziel ist es, einem Text, der den Features am besten entspricht/enthält, bestimmte Themen zuweisen zu können. Beispielsweise kann ein Text Merkmale enthalten, die zu einer Übereinstimmung von 80 % mit Thema A, einer Übereinstimmung von 55 % mit Thema B und einer Übereinstimmung von 20 % mit Thema C führen. Zu diesem Zweck wird ein Klassifizierer mit Klassifizierungsregeln, der auf einem Korpus mit ca. 976.540 Nachrichten aus verschieden Quellen trainiert, verwendet. Für diese Arbeit sind verschiedene Multi-Label-Algorithmen auf einem eigenen kompilierten Datensatz (mit über 1,5 Mio. Nachrichten) evaluiert worden. Wir experimentierten mit Naive Bayes, Decision Tree, KNN, SVM und Random Forest,

jeweils mit einem der drei gebräuchlichen Ansätze für Multi-Label-Klassifizierung: Binary Relevance (BR), Label Powerset (LP) und paarweise und Threshold (PT). Mit einem gewichteten F1-Score von 0,786 zeigt Binary Relevance in Kombination mit Random Forest und einer zugrunde liegenden word2vec-Feature-Darstellung das beste kombinierte Ergebnis der getesteten Modelle. Dieses Modell wird daher für die spätere Verwendung in unserer Proof-of-Concept Implementierung von WallGuard eingesetzt.

Notification Agent Nachdem WallGuard die Verarbeitung einer Nachricht abgeschlossen hat, zeigt der Benachrichtigungsagent die Ergebnisse an. Je nach Ergebnis kann dies eine einfache Benachrichtigung, Empfehlung oder Warnung sein und dem Benutzer weitere Optionen und Schritte anbieten. Insbesondere zeigt der Benachrichtigungsagent bestimmte Ausgaben für jede der vordefinierten Scheduling Policies und möglichen Nachrichten an, die vom Message Scheduler übertragen werden.

Schlussfolgerung, Grenzen und zukünftige Arbeiten Zwar existiert mit der Wallguard Browser Erweiterung eine Proof-of-Concept Implementierung der in dieser Arbeit vorgeschlagenen Lösung zur Mitigation von Reue im Kontext von Sozialen Netzwerken, dennoch soll diese Implementierung in Bezug auf einige in diesem Kapitel genannte Aspekte weiter verbessert werden. Zum aktuellen Zeitpunkt ist daher der Hauptaugenmerk von zukünftigen Arbeiten die bestehende Implementierung zu analysieren und verbessern, um sowohl die Genauigkeit der Klassifikationsergebnisse zu erhöhen als auch die generelle Performanz und Nutzbarkeit der Erweiterung zu verbessern.

Klassifizierung basierend auf Deep Learning Ansätzen Basierend auf der Arbeit von Zhang et al. (2016) planen wir die Implementierung und Evaluierung von Ansätzen, die auf sog. Deep Learning Methoden setzen. Im Detail geht es hierbei darum, Features aus einem Beitrag durch character-level convolutional neuronales Netzwerk zu extrahieren. Die auf diese Weise gewonnenen Features sollen dann als Eingabe für das Training eines multi-label Klassifizierers verwendet werden. Die Anwendung von Modellen, die Analysen von Beiträgen aus Sozialen Medien auf Character-Ebene ausführen, sind besonders vielversprechend. Hauptgrund hierfür ist, das derartige Modelle in der Lage sind damit umzugehen, wenn Beiträge nur begrenzte kontextuelle Informationen enthalten, besondere Unicode Zeichen enthalten (z. B. Sonderzeichen, die in OSN oft verwendet werden, wie das Hashtag Symbol #) oder aber Rechtschreib- und Grammatikfehler enthalten, die in solch kurzen Texten vergleichsweise oft vorkommen. Im nächsten Schritt werden derzeit mehrere Deep-Learning-Modelle, u. a. Convolutional Neural Network (CNN),

Recurrent neural networks (RNN) und Long-short term memory (LSTM) trainiert und evaluiert. Hierbei sollen die oben erwähnten Multi-Label-Modelle zum Teil als Baselines berücksichtigt werden.

Vollständige Implementierung auf Client-Seite Aus dem WallGuard-Server ergeben sich potenzielle Risiken für die Privatsphäre von Nutzern. Jeder Beitrag, der vom Nutzer zur Klassifizierung zum Server gesendet wird, kann potenziell sensitive Informationen enthalten, die erst zu einem späteren Zeitpunkt nach der Klassifizierung herausgefiltert werden. Um hierfür eine Lösung und Alternative zu bieten, soll in zukünftige Arbeiten die Möglichkeit erforscht werden, eine vollständig clientseitige Implementierung zu realisieren. Dies bedeutet, dass keine zusätzliche Kommunikation mit einem externen Server mehr notwendig ist und alle Berechnungen lokal auf der Maschine des Nutzers stattfinden. Für solch eine Implementierung bieten sich multi-label Klassifizierer Frameworks an die nicht auf Java angewiesen sind und direkt in der Webumgebung einer Chrome Erweiterung lauffähig sind. Solch eine Lösung könnte die Implementierung sicherer und potenziell auch schneller machen.

Nutzbarkeitsstudie Des Weiteren soll auch die Benutzeroberfläche von Wall Guard im Hinblick auf einfache Benutzbarkeit und angebotene Features untersucht werden. Hauptsächlich geht es bei dieser Studie darum herauszufinden, ob Nutzer in der Lage sind, das WallGuard Tool sinnvoll anzuwenden und dabei auch erfolgreich das Posten von Nachrichten verhindert wurde, die der Nutzer im Nachhinein bedauern könnte. Darum soll das Tool in einer zukünftigen Nutzbarkeitsstudie mit Hilfe einer größeren Gruppe von Nutzern evaluiert werden.

6.3 MetaMiner

Mit der immer weiter ansteigenden Nutzung von Drittanbieter Anwendung auf mobilen Geräten setzen sich Nutzer Risiken aus, die ihre Privatsphäre bedrohen. Dabei sind sich viele Nutzer gar nicht bewusst, wie weit solche Anwendung in ihre Privatsphäre eingreifen und wie viele potenziell kritische Daten diese in der Lage sind, unbemerkt zu sammeln und an externe Server zu senden.

Um diesem Problem vorzubeugen und Nutzer aufzuklären, haben wir PISA entwickelt: ein leichtgewichtiges und nutzerzentriertes Framework, das eine Verbesserung der Transparenz über die Netzwerkinteraktionen des mobilen Geräts mit

ATM-Domains[61] ermöglicht und damit zur Befähigung der Nutzer ihr Recht auf informationelle Selbstbestimmung auszuüben, beiträgt. Die Vision unseres Frameworks ist es, Datenverkehrsanalysen datenschutzerhaltend durchzuführen. Des Weiteren war es uns besonders wichtig, dass auch unerfahrene Nutzer in der Lage sind, unsere Anwendung zu installieren und zu benutzen, es also nicht nötig ist sein Gerät erst zu rooten oder sonstige Modifikationen durchzuführen. Wir haben einen Proof-of-Concept-Prototyp implementiert und umfangreiche Experimente durchgeführt, um die Machbarkeit und Wirksamkeit des PISA-Frameworks zu demonstrieren. Unsere Auswertungen in einem realen Datensatz zeigen eine hohe Effektivität bei der Erkennung von Interaktionen mit ATM-Hosts und einem angemessenen Performance-Overhead.

Architektur und Implementierung Das MetaMiner Framework ist modular aufgebaut und setzt sich aus fünf Kernkomponenten zusammen: Network Traffic Metadata Collector (1), Database Manager (2), Metadata Analyzer (3), Visualization Engine (4) und Privacy Controller (5). Einen groben Überblick der Interaktion der verschiedenen Komponenten untereinander zeigt Abb. 4. Im folgenden werden die fünf Kernkomponenten und deren entsprechenden Aufgaben im Rahmen des MetaMiner Frameworks eingeführt.

Network Traffic Metadata Collector (NTMC) Die wichtigste Komponente des MetaMiner Frameworks stellt der Network Traffic Metadata Collector (NTMC) dar. Die Hauptfunktion dieser Komponente ist das Abfangen, Verabeiten und Weiterleiten von Netzwerkpaketen auf dem mobilen Gerät. Beim Verarbeiten von Paketen extrahiert der NTMC die Netzwerkmetadata des Pakets und leitet diese an eine Unterkomponente zur Aggregierung und späteren Speicherung dieser Daten weiter. Um Zugriff auf den Netzwerkverkehr des mobilen Android Geräts zu erhalten verlässt sich der NTCM auf die offizielle Android VPN Schnittstelle. Dies ist die zum aktuellen Zeitpunkt einzige Methode auf einem nicht gerooteten Android Gerät, um Zugriff auf den Netzwerkverkehr zu erhalten. Der NTMC besteht aus zwei Unterkomponenten: dem *VPN Proxy* und dem *Metadata Aggregator.*

Database Manager (DM) Der DM fungiert hauptsächlich als zentrale Komponente zur persistenten Speicherung von Daten, die im Rahmen des MetaMiner Frame-

[61] ATM Domains sind potenziell unerwünschte Domains, die ein mobiles Gerät kontaktieren. Der Name leitet sich von der englischen Bezeichnung **a**dvertisement, **t**racking or **m**alicious Domain ab.

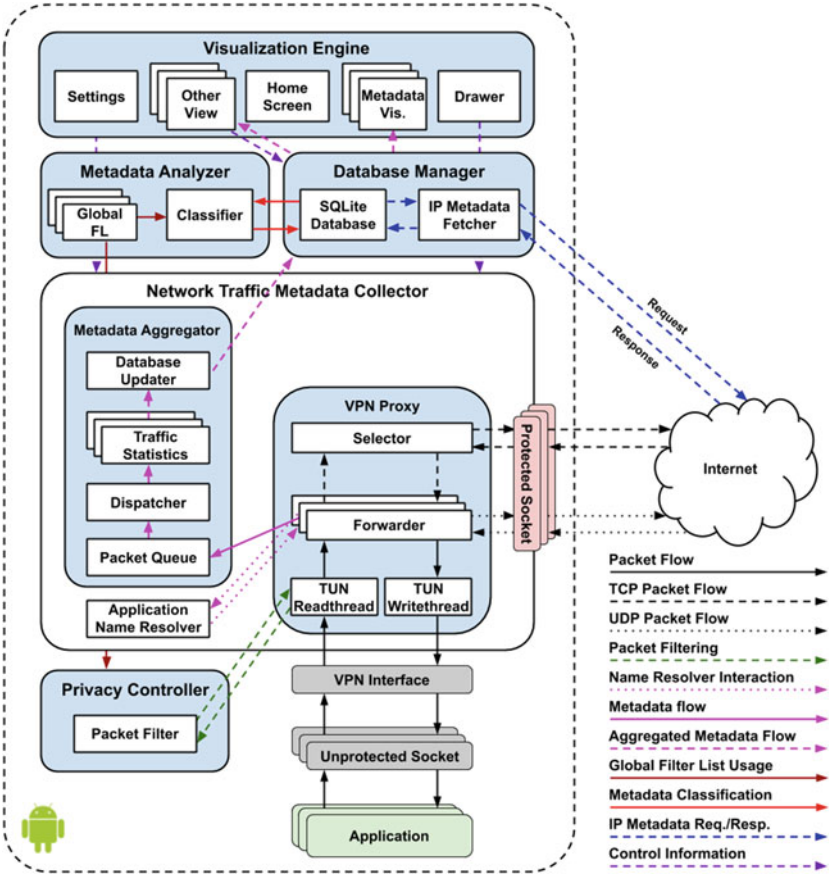

Abb. 4 Detailierte Darstellung der Framework Komponenten inkl. Unterkomponenten und verschiedener Kommunikationsflüsse

works anfallen und zur Analyse und Visualisierung benötigt werden. Generell erfüllt der DM zwei wichtige Funktionen: i) Speicherung von Netzwerkverkehr-Metadaten (u. a. eine historische Perspektive auf die Internet-Interaktionen des Geräts zu ermöglichen) und ii) Abruf von IP-Adress-Metadaten.

Metadata Analyzer (MA) Diese Komponente erledigt alle Aufgaben im Zusammenhang mit der Analyse der gesammelten Metadaten des Netzwerkverkehrs. Dazu gehören insbesondere die automatisierte geräteinterne Verfeinerung und

Aktualisierung einer globalen Filterliste. Die globale Filterliste entsteht offline durch das Zusammenführen verschiedenster Arten von Filterlisten, darunter Listen, die von bekannten Werbe- und Tracker-Blockierern, z. B. Browser Plugins zur Blockierung von Werbung verwendet werden und spezielle auf mobile Werbe- und Analyseprovider ausgerichtet sind. Der MA verwendet die globale Filter-Liste, um die kontaktierten Hosts in drei Kategorien zu klassifizieren: i) Hosts, die die Privatsphäre verletzen, ii) bösartige Hosts und iii) gutartige Hosts. Auf der Grundlage der Ergebnisse der Klassifizierung bietet das MetaMiner Framework eine umfassende Visualisierung darüber an, an welche ATM- Hosts das mobile Gerät Informationen sendet, und liefert visuelle Hinweise darauf, welche Anwendungen für solche Interaktionen verantwortlich waren.

Visualisierungs-Engine (VE) und Grafische Benutzeroberfläche (GUI) Die VE umfasst eine Sammlung verschiedenster Unterkomponenten aus denen sich die sogenannte GUI (Graphical User Interface) zusammensetzt.

Die GUI des MetaMiner Frameworks, siehe Abb. 3 und 4, bietet eine Fülle von Optionen für Menüs, Einstellungen und Ansichten zu Details über durchgesickerte Daten, Entitäten, die die Daten des Benutzers sammeln, und Länder, an die diese Daten gesendet werden. Genauer, die GUI ermöglicht die Visualisierung der Netzwerkinteraktionen des Geräts mit ATM-Hosts und bietet dem Endnutzer Optionen zur Interaktion mit anderen Komponenten des MetaMiner Frameworks (Abb. 5 und 6).

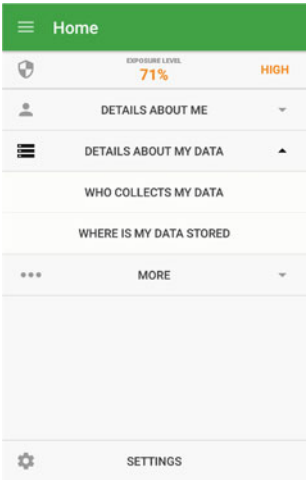

Abb. 5 Home Screen: Die generelle GUI der Anwendung. Hierüber kann der Nutzer auf die verschiedenen Visualisierungen, zusätzlichen Funktionen des MetaMiner Frameworks, als auch auf die Einstellungen zugreifen

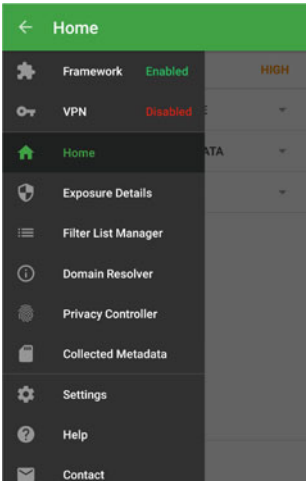

Abb. 6 Navigation Drawer: Hierüber kann der Nutzer schnell auf alle wichtigen Features zugreifen, z. B. das Aktivieren des VPNs für die Netzwerkanalyse oder der Zugriff auf best. Komponenten wie den Privacy Controller

Privacy Controller (PC) Das MetaMiner Framework soll nicht nur für mehr Transparenz über die Interaktionen des Geräts mit ATM-Domains sorgen, sondern den Endnutzern auch Mittel an die Hand geben, ihr Recht auf informationelle Selbstbestimmung auszuüben. MetaMiner bietet ein solches Mittel in Form eines IP-basierten Paketfilters, welcher als Unterkomponente des PCs implementiert ist. Alle MetaMiner-Privatsphärekontrollmethoden sind in der PC-Komponente gebündelt.

Der Benutzer kann zwischen zwei verschiedenen Blockierungsmodi wählen: normaler Modus und erweiterter Modus. Während der normale Modus nur die Kommunikation mit böswilligen Hosts blockiert und damit einen allgemeinen Sicherheitsstandardansatz ermöglicht, zielt der erweiterte Modus darauf ab, zusätzlich die Kommunikation mit Werbe- und Trackinghosts zu blockieren (Abb. 7 und 8).

Evaluation Die Evaluierung des MetaMiner-Frameworks zielte auf die Beantwortung der folgenden beiden Fragen ab: i) Beeinträchtigt MetaMiner den Nutzer bei seiner alltäglichen Nutzung seines Smartphones (Streaming, Browsing, Messaging, etc.)?; und ii) Welche Performance-Einbußen muss ein Nutzer in Kauf nehmen, um das MetaMiner-Framework auf seinem Smartphone verwenden zu können?

Laufzeitrobustheit Es ist wichtig, dass das MetaMiner-Framework nahezu unsichtbar im Hintergrund agiert. Dementsprechend darf das Framework weder Fehler hervorrufen, noch sollte es andere auf dem Smartphone des Nutzers vorhandene

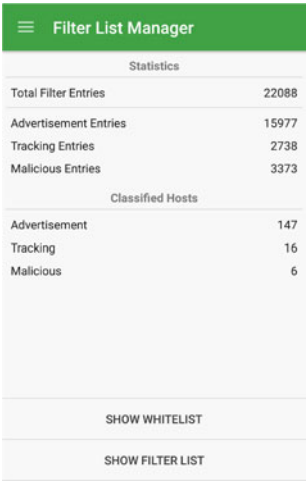

Abb. 7 Filter List Manager: Zeigt generelle Statistiken zur globalen Filter Liste an und ermöglicht das Einsehen der Filterliste

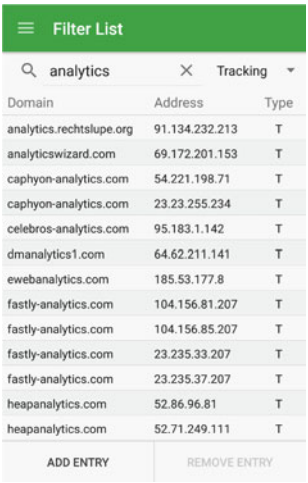

Abb. 8 Filter Liste: Hier kann der Nutzer beliebig nach Einträgen suchen und diese modifizieren oder eigene Einträge hinzufügen

Anwendungen beeinflussen oder zum Abstürzen bringen. Um dieses gewünschte Verhalten zu testen, welches wir Laufzeitrobustheit nennen, haben wir zwei verschiedene Experimente durchgeführt: i) Automatisierte Tests der GUI-Robustheit der MetaMiner-Anwendung; und ii) Installation und Ausführung von Anwendungen von Drittanbietern, wobei das MetaMiner-Framework im Hintergrund lief. Im Verlauf eines zweitägigen automatisierten Tests ist die App weder abgestürzt noch hat sie Fehler produziert.

Energiekosten bzw. Energieverbrauch Ein häufiger Grund für die Ablehnung von Apps ist der ungewöhnlich hohe Batterieverbrauch der Apps. Um die Akzeptanz durch die Nutzer zu erleichtern, muss MetaMiner niedrige Energiekosten induzieren, insbesondere, wenn sich das Gerät im Ruhezustand befindet. Für die Evaluation des Energieverbrauchs haben wir jeweils Messungen ohne und mit dem Framework durchgeführt. Des Weiteren wurden die Messungen sowohl im Ruhezustand (Idle) als auch unter Hoher Last (High Load durchgeführt) durchgeführt. Hohe Last in diesem Kontext bedeutet, dass das Framework aktiv den Netzwerkverkehr abfängt und ein hoher Netzwerkdurchsatz erreicht wird, in unserem Fall durch das Streaming von 1080p Video Content. Die Ergebnisse dieser Messungen finden sich in Tab. 2. Die Ergebnisse zeigen, dass sich im Idle Status der Energievebrauch im Durchschnitt nur um 5,5 % erhöht, während sich unter Hoher Last diese Zahl auf 9.3 % erhöht.

Netzwerkdurchsatz und Netzwerklatenzen Da das Framework den kompletten Netzwerkverkehr abfängt und weiterleitet, ist der maximale Netzwerkdurchsatz eingeschränkt und es entstehen zusätzliche Netzwerklatenzen. Um das Maximum und Mean des Netzwerkdurchsatzes für TCP und UDP-Flows zu messen, die durch das MetaMiner-Framework erreicht werden können, haben wir das iPerf-Tool[62] in seiner Version 3 verwendet. Für die tatsächliche Messung wurde der iPerf-Client so konfiguriert, dass er einen Satz von 1000 TCP-Durchsatzmessungen unter Verwendung eines Sekundenzeitintervalls zwischen jeder aufeinanderfolgenden Messung durchführt. Die Messungen wurden sowohl im Normal- als auch im Reverse-Modus durchgeführt, sodass nachgeschaltete Durchsatzmessungen möglich waren. Die Ergebnisse dieser Messungen sind in Tab. 3 dargestellt.

Neben dem Netzwerkdurchsatz ist auch die Netzwerklatenz ein kritischer Aspekt der die Benutzererfahrung mit dem MetaMiner-Framework stark negativ beeinflussen kann. Auf Grund des Abfangens und Weiterleitens des Netzwerkverkehrs werden durch die VPN Proxy Komponente unausweichlich zusätzliche Latenzen

[62] https://iperf.fr/

Tab. 2 Evaluation des Energieverbrauchs

No.	Idle w/o MetaMiner	Idle w. MetaMiner	High Load w/o MetaMiner	High Load w. MetaMiner
#1	921,3 mW	1013,9 mW	2383,7 mW	2588 mW
#2	938,7 mW	1034,6 mW	2217,4 mW	2481,3 mW
#3	953,5 mW	1023,2 mW	2283,4 mW	2435,4 mW
#4	893,2 mW	978,2 mW	2335,4 mW	2509,3 mW
#5	962,2 mW	1002,7 mW	2412,1 mW	2399,6 mW
#6	976,1 mW	953,4 mW	2354,5 mW	2565 mW
#7	994,8 mW	998,3 mW	2290 mW	2573,1 mW
#8	935,7 mW	934,9 mW	2335,3 mW	2603,1 mW
#9	932,2 mW	987,2 mW	2412,1 mW	2477,5 mW
#10	937,3 mW	1040,6 mW	2166 mW	2480,7 mW
Mean	*944,5 mW*	*996,7 mW*	*2318,9 mW*	*2511,3 mW*
Increase	**5,53 %**		**9,30 %**	

Tab. 3 Ergebnisse der Messung des Netzwerkdurchsatzes

Protokoll	Richtung	Durchschnitt	Maximum
TCP	Upstream	5,2 Mbit/s	6,3 Mbit/s
TCP	Downstream	17,3 Mbit/s	20,7 Mbit/s
UDP	Upstream	27,5 Mbit/s	33,3 Mbit/s

erzeugt. Zur Messung der zusätzlich durch die Nutzung des VPNs entstehenden Netzwerklatenzen wurde das MetaMiner Framework modifiziert, um diese Werte direkt in der VPN Proxy Komponente erfassen zu können. Die Messungen wurden unter verschiedenen Szenarien durchgeführt um realistische Ergebnisse für verschiedene Nutzungsaspekte des Smartphones zu erhalten. Die Ergebnisse der Messungen sind in Abb. 9 (Durchschnitt), Abb. 10 (Min) und Abb. 11 (Max) zu sehen. Es stellt sich heraus, dass im Durchschnitt keine merkbaren zusätzlichen Latenzen entstehen, es aber je nach Last der VPN Proxy Komponente selten zu längeren Verzögerungen kommen kann.

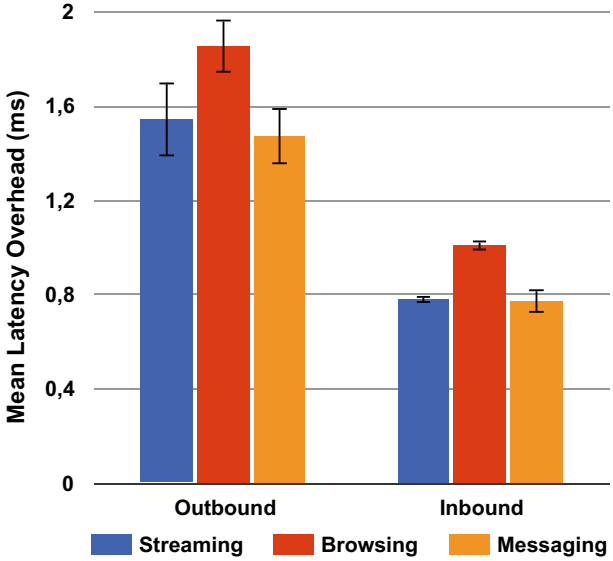

Abb. 9 Ergebnisse der Messung der Netzwerklatenzen (Durchschnitt)

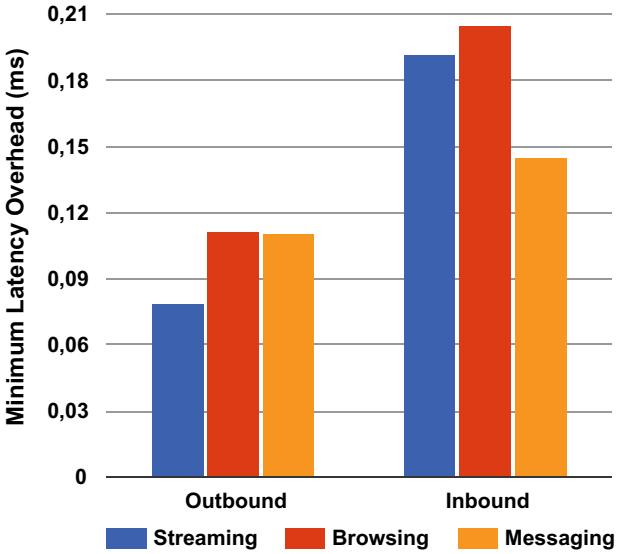

Abb. 10 Ergebnisse der Messung der Netzwerklatenzen (Min)

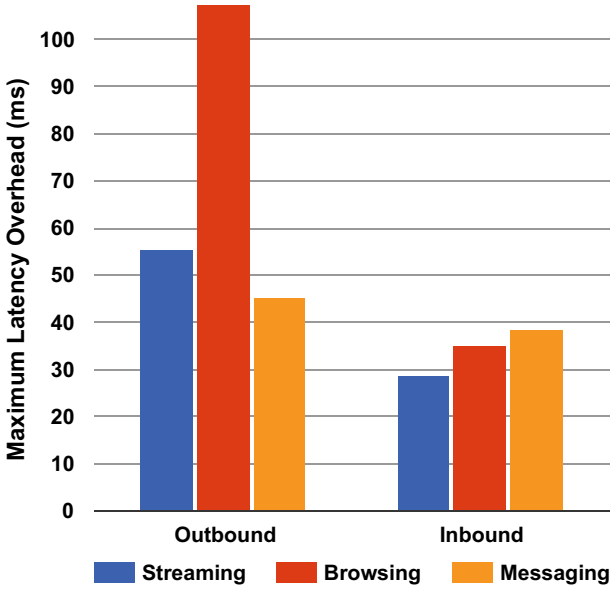

Abb. 11 Ergebnisse der Messung der Netzwerklatenzen (Max)

Schlussfolgerung, Grenzen und zukünftige Arbeiten Die oben vorgestellten Forschungsbemühungen zur Verbesserung der Transparenz und Benutzerkontrolle über die Netzwerkinteraktionen von Android-betriebenen Mobilgeräten sind vielversprechend. Dennoch ist die Arbeit von einigen Einschränkungen betroffen.

Ein Prototyp von PISA wurde implementiert und evaluiert. Die Evaluierungsergebnisse zeigen, dass PISA in Bezug auf Wirksamkeit und Einsatzfähigkeit zufriedenstellend ist. PISA kann die Geräteinteraktion mit ATM-Domänen wirksam erkennen und induziert dabei gleichzeitig nur einen moderaten Overhead. Darüber hinaus planen wir, den derzeitigen Overhead, der durch das PISA Framework hervorgerufen wird, weiter zu reduzieren, indem wir unseren Ansatz für das Verarbeiten und Weiterleiten von Netzwerkpaketen weiter optimieren. Ein Hauptziel ist dabei die weitere Reduzierung des CPU-Overheads, ohne dabei die Netzwerklatenz signifikant zu erhöhen.

7 Schlussbetrachtung

Informationstechnologie kann konform zu Privatheit und gesellschaftlichen Werten entworfen sowie genutzt werden. Mit ihr kann die wirtschaftliche Entwicklung befördert werden und sie kann Enabler für Innovationen in allen Bereichen sein. Technische Innovationen lassen sich konform zu Wertesystemen, auch zum europäischen, realisieren.

Jeder und jedem kann ein individueller Zugang zu ihrem und seinem persönlichen digitalen Fußabdruck ermöglicht werden, der so aufbereitet ist, dass Privatheitsrisiken erfasst werden können. Unsere hier präsentierten Gestaltungsvorschläge zeigen dies für drei kleine Beispiele auf. Bisher werden von Unternehmen überwiegend nur Rohdaten zur Verfügung gestellt, die nur für technisch versierte Personen Transparenz liefern. Welche Schlussfolgerungen Unternehmen und Dritte aus dem digitalen Fußabruck ableiten können, ist für den Benutzer weitestgehend nicht ersichtlich. Durch das Sichtbarmachen und Aufbereiten des digitalen Fußabdrucks werden privatheitsinvasive Mechanismen offengelegt und Veränderungen zu ihrer Eindämmung können gestaltet und implementiert werden. Mit Hilfe dieser technischen Maßnahmen ist es NutzerInnen möglich, ihr Handeln zu reflektieren, über das Handeln von Unternehmen aufgeklärt zu werden, um dadurch selbstbestimmt handeln zu können. Diese Simulation von möglichen Schlussfolgerungen haben wir mit zwei der drei Gestaltungsvorschläge geschaffen. Die Offenlegung kann ohne Aufgabe des Geschäftsmodells als Empfehlung mit dem Anreiz der vertrauensbildenden Maßnahme an Unternehmen gegeben werden. Hier gibt es allerdings noch erheblichen Forschungsbedarf über das „wie“. Wir schlagen vor, dass die Forschungsförderung mit dem Schwerpunkt Transparenz ausgebaut wird.

Europa kann an und mit der Digitalisierung wachsen – mit Hilfe von Technik, kreativen Köpfen und konform zu europäischen Werten. Privacy-Ready bedeutet Transparency-Ready zu sein.

Literatur

Absenger, N., et al. (2016). „Digitalisierung der Arbeitswelt!? Ein Report aus der Hans-Böckler-Stiftung“. *Mitbestimmungs-Report, 24,* 1–18. https://d-nb.info/1118758307/34. Zugegriffen: 1. Apr. 2021.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). „What Is privacy worth?“ *The Journal of Legal Studies, 42*(2), 249–274. https://doi.org/10.1086/671754.

Ammicht Quinn, R., et al. (2018). *Tracking: Beschreibung und Bewertung neuer Methoden*. White Paper. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Karlsruhe: Fraunhofer ISI, S. 1–48.

Article 29 Data Protection Working Party. (2018). *Guidelines on transparency under regulation 2016/679*. Working Paper 17/EN, WP 260 rev. 01. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025. Zugegriffen: 1. Apr. 2021.

Bär, D., Zesch, T., & Gurevych, I. (2013). „DKPro similarity: An open source framework for text similarity". In *Proceedings of the 51st annual meeting of the association for computational linguistics, Sophia, Bulgaria, August 4–9 2013* (S. 121–126).

BITKOM. (2020a). Jeder Dritte sucht online nach der großen Liebe. Presseinformation. https://www.bitkom.org/Presse/Presseinformation/Jeder-Dritte-sucht-online-nach-der-grossen-Liebe. Zugegriffen: 1. Apr. 2021.

BITKOM. (2020b). Zwei Drittel der Unternehmen sehen sich durch Datenschutzregeln behindert. Presseinformation. https://www.bitkom.org/Presse/Presseinformation/Zwei-Drittel-der-Unternehmensehen-sich-durch-Datenschutzregeln-behindert.html. Zugegriffen: 1. Apr. 2021.

BMBF. (2020). „Digitalisierung in der Medizin". https://www.bmbf.de/de/digitalisierung-in-der-medizin-2897.html. Zugegriffen: 26. Juni 2020.

Böhme, G. (2018). „Eine Kultur der Privatheit". In G. Böhme & U. Gahlings (Hrsg.), *Kultur der Privatheitin der Netzgesellschaft*. Aisthesis.

Cai, H., Zheng, V. W., & Chang, K. C.-C. (2018). „A Comprehensive survey of graph embedding: Problems, techniques, and applications". *IEEE Transactions on Knowledge and Data Engineering, 30*(9), 1616–1637. https://doi.org/10.1109/tkde.2018.2807452.

Callegaro, M., & Yang, Y. (2018). „The role of surveys in the era of big data". In D. L. Vannette & J. A. Krosnick (Hrsg.), *The Palgrave handbook of survey research*. Palgrave Macmillan. https://doi.org/10.1007/978-3-319-54395-6_23.

Cave, J., et al. (2009). *Trends in connectivity technologies and their socioeconomic impacts. Final report of the study: Policy options for the ubiquitous internet society*. RAND Europe. https://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR776.pdf. Zugegriffen: 1. Apr. 2021.

Checkoway, S., et al. (2011). „Comprehensive experimental analyses of automotive attack surfaces". In *20th USENIX security symposium (USENIX Security 11)*. USENIX Association. https://www.usenix.org/conference/usenix-security-11/comprehensiveexperimental-analyses-automotive-attack-surfaces. Zugegriffen: 1. Apr. 2021.

Cichy, P., & Salge, T. O. (2015). „The evolution of privacy norms: Mapping 35 years of technology-related privacy discourse, 1980–2014". *Proceedings of the 36th International Conference on Information Systems (ICIS)*. Fort Worth, Texas, USA. http://aisel.aisnet.org/icis2015/proceedings/SecurityIS/18/. Zugegriffen: 1. Apr. 2021.

Dass, S., et al. (2021). „Datenschutz- und Sicherheitsanalyse von Mobilen Learning Apps". In M. Friedewald, M. Kreutzer, & M. Hansen (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg*. Springer Vieweg.

Dienlin, T., & Trepte, S. (2015). „Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors". *European Journal of Social Psychology, 45,* 285–297. https://doi.org/10.1002/ejsp.2049.

Eisele, D., et al. (2017). *Privatheit in öffentlichen WLANs: Spannungsverhältnisse zwischen ökonomischen Interessen, gesellschaftlicher Verantwortung und rechtlichen Anforderungen*. White Paper. Karlsruhe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. https://www.forum-privatheit.de/download/privatheit-in-oeffentlichen-wlans-2017/.

Fischer-Hübner, S., et al. (2011). „Online privacy: Towards informational self-determination on the Internet". *Dagstuhl Manifestos, 1*(1), 1–20. https://doi.org/10.4230/DagMan.1.1.1. http://drops.dagstuhl.de/opus/volltexte/2011/3205. Zugegriffen: 1. Apr. 2021.

Franke, P., Kreutzer, M., & Simo Fhom, H. (2021). „Privacy-preserving IDS for In-Car-Networks with Local Differential Privacy". In M. Friedewald, S. Schiffner, & S. Krenn (Hrsg.), *Privacy and identity management. 15th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 international summer school, Maribor, Slovenia, September 20–23, 2020, revised selected papers. IFIP advances in information and communication technology* (Bd. 619). Springer International. https://doi.org/10.1007/978-3-030-72465-8.

Garcia, F. D., et al. (2016). „Lock it and still lose it -on the (in)security of automotive remote keyless entry systems". In *25th USENIX security symposium (USENIX Security 16)*. USENIX Association. https://www.usenix.org/conference/usenixsecurity16/technicalsessions/presentation/garcia. Zugegriffen: 1. Apr. 2021.

Gassen, M., & Simo Fhom, H. (2016). „Towards privacy-preserving mobile location analytics". In T. Palpanas, et al. (Hrsg.), *Proceedings of the workshops of the EDBT/ICDT 2016 joint conference (EDBT/ICDT 2016), Bordeaux, France, March 15, 2016* (Bd. 1558). CEUR Workshop Proceedings. http://ceur-ws.org/Vol-1558/paper31.pdf.

Ghiglieri, M., Hansen, M., et al. (2016a). *Smart-TV und Privatheit: Bedrohungspotenziale und Handlungsmöglichkeiten. Forschungsbericht*. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. https://www.forum-privatheit.de/wp-content/uploads/Forschungsbericht-Smart-TV-und-Privatheit_Druckfassung-1.pdf. Zugegriffen: 1. Apr. 2021.

Ghiglieri, M., Lange, B., et al. (2016b). „Security und Privacy bei Smart TVs: Bedrohungspotential und technische Lösungsansätze". In J. Lichdi (Hrsg.), *Digitale Schwellen: Freiheit und Privatheit in der digitalisierten Welt* (S. 67–84). Heinrich-Böll-Stiftung Sachsen.

Gillula, J. (2015). *Google's student tracking isn't limited to Chrome Sync*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2015/12/googles-student-tracking-isnt-limited-chromesync. Zugegriffen: 1. Apr. 2021.

Goldfarb, A., & Tucker, C. (2012). „Shifts in privacy concerns". *American Economic Review, 102*(3), 349–353. https://doi.org/10.1257/aer.102.3.349.

Greenberg, A. (2016). „The FBI warns that car hacking is a real risk". *Wired*. https://www.wired.com/2016/03/fbi-warns-carhacking-real-risk/. Zugegriffen: 1. Apr. 2021.

Heisenberg, D. (2005). *Negotiating privacy: The European Union, the United States, and personal data protection*. Lynne Rienner Publ.

Kelber, U. (2019). „Datenschutz ist kein Hemmschuh für Innovationen". In *Wettbewerb – Der Treiber für die Gigabit-Gesellschaft. VATM-Jahrbuch 2019* (S. 76). VATM e. V. https://www.vatm.de/wp-content/uploads/2019/04/Jahrbuch-2019-Web-1.pdf. Zugegriffen: 1. Apr. 2021.

Kelpen, K., & Simo, H. (2018). „Privacy and data protection in the domain name system: Threats and countermeasures". In M. Friedewald (Hrsg.), *Privatheit und selbstbestimmtes Leben in der Digitalen Welt: Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes* (S. 253–302). Springer Vieweg. https://doi.org/10.1007/978-3-658-21384-8.

Kohlhammer, J., et al. (2021, May). „PrivInferVis: Towards enhancing transparency over attribute inference in online social networks". In *IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)* (pp. 1-2). IEEE.

Kraus, H. (2013). *Big Data – Einsatzfelder und Herausforderungen. Arbeitspapiere der FOM 41*. MAAkademie. https://www.fom.de/fileadmin/fomalt/downloads/forschungsberichte/arbeitspapiere/AP41.PDF. Zugegriffen: 1. Apr. 2021.

Lambiotte, R., & Kosinski, M. (2014). „Tracking the digital footprints of personality". *Proceedings of the IEEE, 102*(12), 1934–1939. https://doi.org/10.1109/jproc.2014.2359054.

Laney, D. B. (2001). *3D data management: Controlling data volume, velocity and variety*. Research Note 6. META Group.

Lang, D., Corbett, C., & Kargl, F. (2016). „Security evolution in vehicular systems". *Fachgespräch Inter-Vehicle Communication,2016,* 7–9. https://doi.org/10.18452/1433.

Lessig, L. (2006). *Code: Version 2.0*. Basic Books.

Lewinski, K. von (2012). „Zur Geschichte von Privatsphäre und Datenschutz – Eine rechtshistorische Perspektive". In J.-H. Schmidt & T. Weichert (Hrsg.), *Datenschutz: Grundlagen, Entwicklungen und Kontroversen* (S. 23–33). Bundeszentrale für politische Bildung.

Miller, C., & Valasek, C. (2013). „Adventures in automotive networks and control units". *Def Con,21,* 260–264.

Miller, C., & Valasek, C. (2014). *A survey of remote automotive attack surfaces* (S. 94). Black Hat USA.

Miller, C., & Valasek, C. (2015). *Remote exploitation of an unaltered passenger vehicle*. Technical White Paper. Black Hat USA.

Nadeau, D., & Sekine, S. (2007). „A survey of named entity recognition and classification". *Linguisticae Investigationes, 30*(1), 3–26.

O'Rourke, C., & Kerr, A. (2017). „Privacy shields for whom? Key actors and privacy discourses on Twitter and in Newspapers". *Westminster Papers in Communication and Culture, 12*(3), 21–36. https://doi.org/10.16997/wpcc.264.

OECD. (1997). *Global information infrastructure – Global information society (GIIGIS): Policy recommendations for action*. Organisation for Economic Co-operation und Development. https://www.oecd.org/sti/broadband/1912232.pdf.

Osborne, N., & Connelly, L. (2015, July). „Managing your digital footprint: Possible implications for teaching and learning". *Proceedings of the 2nd European Conference on Social Media ECSM,* 354–361. Porto, Portugal.

Pohle, J. (2017). „Datenschutz und Technikgestaltung: Geschichte und Theorie des Datenschutzes aus informatischer Sicht und Folgerungen für die Technikgestaltung". Dissertation. Humboldt-Universität zu Berlin. https://edoc.hu-berlin.de/bitstream/handle/18452/19886/dissertation_pohle_joerg.pdf. Zugegriffen: 1. Apr. 2021.

Raab, C., & Koops, B.-J. (2009). „Privacy actors, performances and the future of privacy protection". In S. Gutwirth, et al. (Hrsg.), *Reinventing data protection?* (S. 207–221) Springer. https://doi.org/10.1007/978-1-4020-9498-9_12.

Reichert, R. (2014). *Big Data: Analysen zum digitalen Wandel von Wissen, Macht und Ökonomie*. transcript.

Reisch, L., et al. (2016). *Digitale Welt und Handel. Verbraucher im personalisierten Online-Handel*. Sachverständigenrat für Verbraucherfragen. https://www.svr-verbraucherfragen.de/wp-content/uploads/Digitale-Welt-und-Handel.pdf. Zugegriffen: 1. Apr. 2021.

Reyes, I., et al. (2018). „Won't somebody think of the children? Examining COPPA compliance at scale". *Proceedings on Privacy Enhancing Technologies 2018, 3,* 63–83. https://doi.org/10.1515/popets-2018-0021.

Rosner, G., & Kenneally, E. (2018). *Clearly opaque: Privacy risks of the internet of things*. IoT Privacy Forum. https://www.iotprivacyforum.org/wp-content/uploads/2018/06/Clearly-Opaque-Privacy-Risks-of-the-Internet-of-Things.pdf?d8bd54&d8bd54. Zugegriffen: 1. Apr. 2021.

Roßnagel, A., Friedewald, M., et al. (2017). *Datensparsamkeit oder Datenreichtum? Zur neuen politischen Diskussion über den datenschutzrechtlichen Grundsatz der Datensparsamkeit*. Policy Paper. Karlsruhe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. https://www.forumprivatheit.de/download/datensparsamkeit-2017/.

Roßnagel, A., Bile, T., et al. (2020). *Einwilligung: Möglichkeiten und Fallstricke aus der Konsumentenperspektive*. White Paper. Karlsruhe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. https://www.forum-privatheit.de/download/einwilligung/. Zugegriffen: 1. Apr. 2021.

Sabt, M., Achemlal, M., & Bouabdallah, A. (2015). „Trusted execution environment: What it is, and what it is not". *2015 IEEE Trustcom/BigDataSE/ISPA, 1,* 57–64. https://doi.org/10.1109/Trustcom.2015.357.

Simo Fhom, H. (2015). „Big data: Opportunities and privacy challenges". In P. Richter (Hrsg.), *Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data. Der elektronische Rechtsverkehr* (Bd. 32, S. 13–44). Nomos. https://doi.org/10.5771/9783845264165-13.

Simo Fhom, H., Waidner, M., & Geminn, C. (2019). „Intrusion Detection – Systeme für vernetzte Fahrzeuge – Konzepte und Herausforderungen für Privatheit und Cyber-Sicherheit". In A. Roßnagel (Hrsg.), *Grundrechtsschutz im Smart Car: Kommunikation, Sicherheit und Datenschutz im vernetzten Fahrzeug* (S. 311–333). Springer Vieweg. https://doi.org/10.1007/978-3-658-26945-6_18.

Singh, A., & Simo Fhom, H. (2016). „Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection". *International Journal of Information Security, 16*(2), 195–211. https://doi.org/10.1007/s10207-016-0328-y.

Solove, D. J. (2020). „The myth of the privacy paradox". Geo. Wash. L. Rev., 89, 1. https://doi.org/10.2139/ssrn.3536265.

Stalla-Bourdillon, S., & Knight, A. (2017). „Anonymous data v. personal data – A false debate: An EU perspective on anonymization, pseudonymization and personal data". *Wisconsin International Law Journal, 34*(2), 284–322.

Stapf, I., et al. (2021). „Das Recht von Kindern und Jugendlichen auf Privatheit in digitalen Umgebungen: Handlungsempfehlungen des Forum Privatheit". In I. Stapf, et al. (Hrsg.), *Aufwachsen in überwachten Umgebungen: Interdisziplinäre Positionen zur Privatheit und Datenschutz in Kindheit und Jugend* (S. 351–376). Nomos.

Steinebach, M., et al. (2015). *Chancen durch Big Data und die Frage des Privatheitsschutzes. Begleitpaper Bürgerdialog*. Bericht SIT-TR-2015-06. Fraunhofer- Institut für Sichere Informationstechnologie. http://publica.fraunhofer.de/dokumente/N-374560.html. Zugegriffen: 1. Apr. 2021.

Van Ouytsel, J., Walrave, M., & Ponnet, K. (2014). „How schools can help their students to strengthen their online reputations". *The Clearing House: A Journal of Educational Strategies, Issues and Ideas, 87*(4), 180–185. https://doi.org/10.1080/00098655.2014.909380.

Wang, Y., et al. (2011, July). „I regretted the minute I pressed share: A qualitative study of regrets on Facebook". In *Proceedings of the seventh symposium on usable privacy and security* (S. 1–16). Pittsburgh, Pennsylvania, USA.

Zhang, Y., & Wallace, B. (2016). *A sensitivity analysis of (and practitioners' guide to) convolutional neural networks for sentence classification*. arXiv: 1510.03820 [cs.CL].

Dr. Michael Kreutzer forscht und publiziert seit mehr als 20 Jahren zu Fragestellungen des technischen Privatsphärenschutzes und der IT-Sicherheit. Seit 2015 verantwortet er beim Fraunhofer-Institut für Sichere Informationstechnologie (SIT) den Bereich Internationalisierung und strategische Industriebeziehungen.

Johanna Mittermeier studiert Philosophie und Soziologie an der Technischen Universität Darmstadt. Sie beschäftigt sich schwerpunktmäßig mit der praktischen Philosophie und inspiriert von Prof. Dr. Christoph Hubig, insbesondere mit der Technikphilosophie. Sie betreut die Lehrveranstaltung „Ingenieurwissenschaft & Gesellschaft“ in der Technikphilosophie bei Prof. Dr. Nordmann und ist wiederholt zugleich als Tutorin in derselben tätig. Frau Mittermeier arbeitet am Fraunhofer SIT für das Forum Privatheit.

Linda Schreiber ist Mitarbeiterin in der Geschäftsstelle des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE am Fraunhofer-Institut für Sichere Informationstechnologie in Darmstadt.

Hervais Simo Fhom ist wissenschaftlicher Mitarbeiter am Fraunhofer Institut für Sichere Informationstechnologie SIT in Darmstadt. Seine Forschungsschwerpunkte liegen in den Bereichen Privacy Engineering, Cybersecurity und Applied Machine Learning.

Datenschutz und Privatheitsschutz durch Gestaltung der Systeme

Marit Hansen, Felix Bieker und Benjamin Bremert

1 Einführung

Das Forum Privatheit hat sich von Anfang an damit beschäftigt, wie sich die Anforderungen von Datenschutz und Privatheitsschutz umsetzen lassen. Eine prominente Rolle dabei spielt die Gestaltung der Systeme, die bezüglich der Verarbeitung personenbezogener Daten zum Einsatz kommen. Dies wird in Bezug auf die heutige und künftige Relevanz in diesem Beitrag diskutiert. Wie sich der Ansatz der datenschutzkonformen Systemgestaltung über die letzten Jahrzehnte entwickelt hat, stellt der folgende Abschn. 2 vor. Abschn. 3 erörtert den Risikobegriff der Datenschutz-Grundverordnung als zentralen Maßstab für die Gestaltung der Systeme. Darauf aufbauend beschreibt Abschn. 4, wie sich die Anforderungen durch technische und organisatorische Maßnahmen über den Lebenszyklus der Systementwicklung und im Betrieb umsetzen lassen. Abschn. 5 beschreibt Spannungsfelder, die bei der Gestaltung nicht außer Acht gelassen werden sollten, um nachhaltige Lösungen zu erreichen. Der letzte Abschn. 6 fasst den aktuellen Forschungsstatus zusammen und leitet Schlussfolgerungen ab.

M. Hansen (✉) · F. Bieker · B. Bremert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Kiel, Deutschland
E-Mail: marit.hansen@datenschutzzentrum.de

F. Bieker
E-Mail: fbieker@datenschutzzentrum.de

B. Bremert
E-Mail: benjamin@bremert.de

B. Bremert
DZ HYP AG, Hamburg, Deutschland

A. Roßnagel und M. Friedewald (Hrsg.), *Die Zukunft von Privatheit und Selbstbestimmung,* DuD-Fachbeiträge,
https://doi.org/10.1007/978-3-658-35263-9_8

Die hier verwendeten Begriffe des Schutzes der Privatheit und des Datenschutzes gehen auf die Grundrechte der EU-Grundrechte-Charta (GrCh) in Artt. 7 und 8 zurück. Eine genaue Abgrenzung gestaltet sich häufig schwierig, da beide Grundrechte in den Fällen, in denen personenbezogene Daten mit Bezug zum Privatleben betroffen sind, nebeneinander verwendet werden[1] und sich gegenseitig verstärken[2]. Der Privatheitsschutz lässt sich am ehesten mit dem aus Artt. 2 Abs. 1, 1 Abs. 1 GG abgeleiteten Allgemeinen Persönlichkeitsrecht vergleichen. Der Schutzbereich des Art. 8 GrCh geht dagegen über den Bezug zum Privatleben hinaus[3], setzt nur am Vorhandensein personenbezogener Daten an und stellt somit das allgemeinere Datenschutz-Grundrecht dar. In seiner neueren Rechtsprechung verwendet der EuGH beide Grundrechte in der Regel in Form einer gemeinsamen Anwendung[4] bzw. sieht die Schutzbereiche beider Grundrechte[5] eröffnet[6]. Gerade im englischsprachigen Raum werden die Begriffe „Privacy“ und „Data Protection“ aber häufig synonym verwendet.

2 Die Entwicklung des Ansatzes einer Systemgestaltung für Datenschutz und Privatheit

Eine der Neuerungen, die mit der Datenschutz-Grundverordnung (DSGVO) eingeführt wurden, ist die Anforderung „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“. Diese sperrige Überschrift betitelt den Artikel 25 DSGVO. Im Ergebnis geht es um „eingebauten Datenschutz“, d. h. eine Gestaltung der (nicht nur) technischen Systeme auf eine Art und Weise, dass die Datenschutz-Grundsätze umgesetzt oder unterstützt werden. Die Logik hinter dieser Anforderung ist unmittelbar nachvollziehbar: Werden die Systeme, die zur Verarbeitung personenbezogener Daten eingesetzt werden, datenschutzgerecht gestaltet, dient dies insgesamt der Rechtskonformität. Andersherum: Hat man bei der Gestaltung jener Systeme Datenschutzanforderungen nicht berücksichtigt, kann es sein, dass ein rechtskonformer Einsatz nur unter Schwierigkeiten, möglicherweise allenfalls mit zeit- oder kostenintensiven Maßnahmen, oder gar nicht möglich ist.

[1] Jarass (2021), Art. 8 Rn. 4.

[2] Roßnagel (2019), S. 2.

[3] Jarass (2021), Art. 8 Rn. 6.

[4] Kingreen (2016), Rn. 1.

[5] Felber (2020), § 38 Rn. 3.

[6] Teilweise in Analogie zur strafrechtlichen Konkurrenzlehre als Idealkonkurrenz bezeichnet.

Diese simple Logik eines in Technik implementierten Datenschutzes und ihre Umsetzung in spezifischen technischen Datenschutzkonzepten wurde bereits vor mehreren Jahrzehnten in Informatik-Fachveröffentlichungen verfolgt.[7] Mitte der 1990er Jahre erstellten dann die Datenschutzbeauftragten der Niederlande und von Ontario, Kanada, den Report „The Path to Anonymity", in dem sie den Begriff der „Privacy-Enhancing Technologies" (PETs, übersetzt als datenschutzfördernde Technik oder datenschutzfreundliche Technologien) einführten.[8] Der *Arbeitskreis Technik* der Datenschutzbeauftragten des Bundes und der Länder erarbeitete daraufhin im Jahr 1997 zwei Orientierungshilfen zu datenschutzfreundlichen Technologien.[9] Während der Begriff der PETs zunächst primär die technischen Konzepte und Implementierungen zur Datenvermeidung und Datensparsamkeit beschrieb, wurde er später erweitert, um auch solche Funktionen zu umfassen, die eine Konformität mit den rechtlichen Datenschutzanforderungen ermöglichen.[10]

Das Konzept des einzubauenden Datenschutzes wurde in Deutschland unter der Bezeichnung „Datenschutz durch Technik" diskutiert, wobei zusätzlich die Begriffe „Selbstdatenschutz"[11] für die nutzerseitige Technik und „Systemdatenschutz"[12] für die Umsetzung aufseiten der Organisation einschließlich der Infrastrukturen unterschiedliche Ausprägungen verdeutlichten. Die Erkenntnis, dass Ansatzpunkte auf verschiedenen Seiten für die Gewährleistung von Sicherheit wie auch Datenschutz eine Rolle spielen können und dafür ein Zusammenspiel der Akteure relevant ist, führten ab Ende der 1990er Jahre zu dem Konzept der mehrseitigen Sicherheit[13]: Damit sollen die Perspektiven und Interessen aller Beteiligten in der Gestaltung der konkreten Datenverarbeitung, insbesondere bezüglich der elektronischen Kommunikation, einbezogen und in einen fairen

[7] Chaum (1985, S. 1030); Pfitzmann, Waidner u. a. (1990, S. 243 und 305).

[8] Van Rossum, Gardeniers u. a. (1995); Borking (1996, S. 654); Borking (1998, S. 636); Hansen (2003), Abschn. 3.3, Rn. 291 ff.

[9] AK Technik der Datenschutzbeauftragten des Bundes und der Länder (1997a, b).

[10] Beispielsweise die Definition der Europäischen Kommission (2007): „The use of PETs can help to design information and communication systems and services in a way that minimises the collection and use of personal data and facilitate compliance with data protection rules. The use of PETs should result in making breaches of certain data protection rules more difficult and/or helping to detect them.".

[11] Roßnagel, in: Roßnagel (2003), Abschn. 3.4 Rn. 325 ff.

[12] Dix, in: Roßnagel (2003), Abschn. 3.5 Rn. 363 ff.; vgl. auch Bieker (im Erscheinen).

[13] Müller und Rannenberg (1999); Pfitzmann (2006, S. 1 ff).

und transparenten Ausgleich gebracht werden. Ein Schwerpunkt liegt auf den Nutzerinnen und Nutzern, die ihre Rechte und Interessen gegenüber mächtigen Organisationen, die über die Datenverarbeitung bestimmen, nicht leicht durchsetzen können. Statt unüberprüfbarer Versprechungen, denen die Nutzenden ohne Kontrollmöglichkeiten vertrauen müssen, sollen nachgewiesene und überprüfbare Garantien gegeben werden, um damit eine Vertrauenswürdigkeit zu rechtfertigen. Die Forschung zur mehrseitigen Sicherheit beschäftigte sich insbesondere mit Verfahren zu Anonymität oder Pseudonymität, verbesserter Transparenz und fairen Aushandlungsmöglichkeiten.

Im internationalen Kontext propagierten Datenschutzbeauftragte, herausragend darunter Ann Cavoukian als *Information and Privacy Commissioner* der kanadischen Provinz Ontario, das verwandte Konzept von „Privacy by Design“[14], das auch in einer Resolution der Internationalen Konferenz der Datenschutzbeauftragten Eingang fand[15] und in zahlreichen Ausarbeitungen diskutiert wurde[16]. Mit Einführung der Datenschutz-Grundverordnung – dort in Art. 25 DSGVO mit der englischen Bezeichnung „Data Protection by Design and by Default“ – hat das Thema seit einigen Jahren weitere Sichtbarkeit und vor allem normative Relevanz erlangt, sodass der datenschutzrechtlich Verantwortliche nun technische und organisatorische Maßnahmen treffen muss, um die Datenschutz-Grundsätze aus Art. 5 DSGVO wirksam umsetzen zu können.

3 Der Maßstab: das Risiko für die Rechte und Freiheiten natürlicher Personen

Der Risikobegriff ist zentraler Bestandteil und wesentliche Neuerung im harmonisierten Datenschutzrecht. Der Schutz der Rechte und Freiheiten natürlicher Personen vor den Risiken von automatisierter und nichtautomatisierter Verarbeitung personenbezogener Daten gehört zu den Zielen der DSGVO. Um dies zu gewährleisten, müssen die Risiken für eben diese Rechte erkannt und entsprechende Schutzmaßnahmen identifiziert und implementiert werden.

[14] Cavoukian (2011).

[15] International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy by Design, 27.–29. Oktober 2010, Jerusalem.

[16] Stellvertretend sei hier mit weiteren Verweisen genannt: Danezis, Domingo-Ferrer u. a. (2015).

Anhand des Risikos wird beispielsweise bestimmt, ob eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO notwendig ist oder – nach Durchführung einer solchen – eine vorherige Konsultation der Datenschutzaufsichtsbehörde gemäß Art. 36 DSGVO vorgenommen werden muss. Nach dem Risiko für die betroffenen Personen bestimmen sich auch die Verpflichtungen des Verantwortlichen im Fall einer Datenpanne („Data Breach", Verletzung des Schutzes personenbezogener Daten) nach Artt. 33 f. DSGVO.

Zudem ist der Risikobegriff für die Gestaltung von Verarbeitungsvorgängen von großer Bedeutung. Die Auswahl und Umsetzung der technischen und organisatorischen Maßnahmen nach Artt. 24, 25 und 32 DSGVO bestimmt sich ebenfalls nach dem Risiko, das sich aus der Verarbeitung für die Rechte von Individuen ergibt.

3.1 Risikobegriff

Der Begriff des Risikos im EU-Datenschutzrecht bezieht sich direkt auf die individuellen Grundrechte, wie sie in der EU-Grundrechte-Charta und der Europäischen Menschenrechtskonvention (EMRK) verbürgt sind. Diese Rechte sind für die EU und die Mitgliedstaaten nach Art. 6 EUV verbindlich. Die Formulierung „Rechte und Freiheiten" ist Art. 52 Abs. 1 GrCh entnommen, der wiederum auf den Gebrauch des Begriffs in der EMRK zurückgeht, die diesen in der französischen Rechtstradition für Grundrechte üblichen Begriff verwendet, da dort Freiheitsrechte nicht vom engeren Verständnis der (subjektiven) Rechte erfasst werden.[17]

Die Zielbestimmung des Art. 1 Abs. 2 DSGVO verweist dabei insbesondere auf das Grundrecht auf Datenschutz nach Art. 8 GrCh, beschränkt ihre Reichweite aber nicht darauf, sondern nimmt sämtliche Grundrechte in Bezug. Damit unterscheidet sich der Bezugspunkt des Risikobegriffs in der DSGVO von anderen bekannten Risikobegriffen[18] und insbesondere vom Ansatz des Risikomanagements. Im Risikomanagement werden Risiken für eine Organisation und ihre Tätigkeit betrachtet. So bezieht sich das Informationssicherheitsmanagement als Unterkategorie des Risikomanagements auf die Auswirkungen eventueller Sicherheitslücken oder anderer sicherheitsrelevanter Ereignisse für die Organisation.

[17] Schwerdtfeger, in: Meyer und Hölscheidt (2019), Art. 52 Rn. 25.

[18] Dazu ausführlicher Friedewald, Bieker u. a. (2017, S. 16).

Der Risikobegriff der DSGVO hat also ein anderes Schutzgut als bisherige Risikobegriffe.[19] Er schützt die Rechte von Individuen, insbesondere der von der Verarbeitung betroffenen Personen. Aus diesem verändertem Schutzgut ergibt sich auch eine weitere Abweichung von anderen Risikomodellen: Der Verantwortliche als datenverarbeitende Organisation ist ebenfalls eine Risikoquelle. Da er grundsätzlich Zugriff auf sämtliche Daten hat, kann er diese auch zum Nachteil der betroffenen Personen einsetzen.

Die DSGVO definiert den Risikobegriff nicht explizit. Aus Wortlaut, Systematik und Telos des Gesetzes hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (Datenschutzkonferenz, DSK) die folgende Definition des Risikos abgeleitet:

> *„Ein Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann.“*[20]

Diese Definition ist auf ErwGr. 75 gestützt, wonach sich aufgrund der Risiken einer Verarbeitung physische, materielle und immaterielle Schäden ergeben können. Insofern folgt daraus, dass Risiken **mögliche** Schäden beschreiben. Dass darunter auch die Verletzungen von Grundrechten der betroffenen Personen fallen können, stellt ErwGr. 94 S. 2 DSGVO klar.[21] Dies verdeutlicht den Unterschied zum Risikomanagement oder dem Risikobegriff in der Informationssicherheit. Allerdings ist nur eine Verletzung von Grundrechten ein Schaden, nicht dagegen jede Beeinträchtigung. Wenn eine Beeinträchtigung nicht gerechtfertigt ist, liegt ein Schaden vor. Wenn es jedoch Gründe für die Beeinträchtigung gibt, die die Voraussetzungen von Art. 52 Abs. 2 GrCh an eine Rechtfertigung erfüllen, liegt auch keine Verletzung und somit kein Schaden vor.

Bei dem Risiko nach der DSGVO handelt es sich also um Risiken für Grundrechte. Das Risiko besteht darin, dass die Beeinträchtigung eines Grundrechts

[19] Dazu ausführlich Bieker (im Erscheinen).

[20] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2018, S. 1).

[21] Ungerechtfertigte Beeinträchtigungen von Grundrechten können dabei sowohl physischer, materieller als auch immaterieller Art sein. Dies wird – richtigerweise – in Datenschutzfällen zunehmend auch in Gerichtsentscheidungen berücksichtigt, die den klagenden Personen aufgrund erlittener immaterieller Schäden durch Verstöße gegen das Datenschutzrecht einen Schadensersatz zusprechen, siehe die Zusammenstellung von Wybitul (2020), der sich allerdings kritisch dazu äußert.

nicht ausreichend gerechtfertigt ist und dieses dadurch verletzt wird. Dabei ist zunächst auf das Grundrecht auf Datenschutz gemäß Art. 8 GrCh abzustellen. Das Risiko für das Grundrecht auf Datenschutz besteht darin, dass die Beeinträchtigung, die in der bloßen Verarbeitung personenbezogener Daten besteht, nicht in dem erforderlichen Maße verringert wird, um – etwa mit Hilfe technischer und organisatorischer Maßnahmen – ein angemessenes Schutzniveau zu erreichen.[22]

Allerdings ist der Risikobegriff eben nicht auf Art. 8 GrCh beschränkt, sondern bezieht sich auch auf sämtliche weitere einschlägige Grundrechte. Als Grundrechte, die im Rahmen der Verarbeitung personenbezogener Daten relevant seien können, kommen nach ErwGr. 4 DSGVO insbesondere das Recht auf Privatleben, Meinungsfreiheit und Nichtdiskriminierung[23] in Betracht.[24]

Insbesondere im Hinblick auf das Recht auf Nichtdiskriminierung bergen Datenverarbeitungsvorgänge teils erhebliche Risiken für die betroffenen Personen. Das gilt beispielsweise beim Einsatz eines Algorithmus zur Gesichtserkennung, der die Gesichter Schwarzer Menschen oder People of Color nicht richtig erkennen kann.[25] Auch algorithmische Systeme, die durch Maschinenlernen auf Basis von Daten mit einem vorurteilsbehafteten Bias (Verzerrung) trainiert werden, können diese Vorurteile bei ihrem Output (Entscheidungen oder Prognosen) verstärken. Dies war z. B. der Fall bei der Software COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), die Gerichte vieler US-Bundesstaaten zur Rückfallprognose für Straftäter eingesetzt haben oder noch einsetzen und die Fehlprognosen zulasten von marginalisierten Bevölkerungsteilen liefert.[26] Auf diese Weise können die algorithmischen Systeme zu weiteren repressiven Maßnahmen gegen diese Personengruppen beitragen.

---

[22] Bieker (im Erscheinen, S. 229 ff.); Bieker (2017, S. 29), detailliert zu den Risiken für Art. 8 GrCh: Rost (2018, S. 81 ff.).

[23] ErwGr. 71, 75 und 85 benennen zudem eine Diskriminierung explizit als möglichen Schaden für die Rechte und Freiheiten natürlicher Personen.

[24] Bieker (2017, S. 28 f.); Hornung und Spiecker, in: Simitis, Hornung u. a. (2019), Art. 1 Rn. 29 u. 32; Buchner, in: Kühling und Buchner (2020), Art. 1 Rn. 13 f.

[25] Kaltheuner und Obermüller 2018, Diskriminierende Gesichtserkennung: Ich sehe was, was du nicht bist, Netzpolitik.org, 10.11.2018, abrufbar unter: https://netzpolitik.org/2018/diskriminierendegesichtserkennung-ich-sehe-was-was-du-nicht-bist/.

[26] Angwin u. a., Machine Bias, ProPublica, 23.05.2016, abrufbar unter: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; Larson et al., How We Analyzed the COMPAS Recidivism Algorithm, ProPublica, 23.5.2016, abrufbar unter: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithme; Flores, Lowenkamp u. a. (2016).

Eine Diskriminierung kann auch niedrigschwelliger bestehen, zum Beispiel wenn bei einem auszufüllenden Formular, das Geschlecht oder die Anrede als Pflichtangabe auszufüllen sind, aber nur binäre Geschlechter erfasst sind und eine Angabe für nicht-binäre Personen fehlt.[27]

Datenverarbeitungsvorgänge lassen sich gezielt einsetzen, um die körperliche Integrität anzugreifen. Dies ist etwa durch den Einsatz von Smart-Home-Geräten möglich, mit denen (ehemalige) Partnerinnen überwacht oder gestalkt werden können. Zu diesen Geräten hat oft nur eine Person im Haushalt einen Administratorzugang, der es ermöglicht, auf umfassende Datenbestände zuzugreifen und die Konfiguration zu ändern. So können durch vernetzte Heimgeräte etwa aus der Ferne Alarme ausgelöst, Türschlösser geschlossen oder geöffnet werden, Lichter an- und ausgeschaltet werden.[28] Dies dient dazu, das Opfer massiv zu verunsichern und auf das eigene Umfeld psychisch instabil wirken zu lassen (sog. Gaslighting).[29]

Folglich kann sich ein Verarbeitungsvorgang auf eine Vielzahl von Grundrechten auswirken. Diese vollständig zu erfassen, kann im konkreten Fall eine Herausforderung für den Verantwortlichen darstellen.

3.2 Risikoerkennung

Eine wesentliche Aufgabe in Zusammenhang mit dem risikobasierten Ansatz der DSGVO ist die Risikoerkennung. Hierzu ist es nicht nur notwendig, dass die Verantwortlichen ihre eigene Datenverarbeitung im Detail kennen, sondern sie müssen auch mögliche Risiken auf Grundlage dieser Datenverarbeitung antizipieren.

Die Kenntnis der eigenen Datenverarbeitung setzt voraus, dass die konkreten technischen Abläufe der Verarbeitungsverfahren dem Verantwortlichen bekannt

[27] Bei der Auswahl einer Anrede ist „divers“ ungeeignet, da es sich um das rechtliche Geschlecht handelt. Es würde sicherlich zu vergleichbaren Irritationen führen, wenn eine Person mit „Mann“ angeredet würde. Vgl. umfassend Guyan (2022).

[28] Tanczer u. a. (2018, S. 3f.); Lopez Neira u. a. (2019, S. 22).

[29] Braithwaite, Smart home tech is being turned into a tool for domestic abuse, Wired, 22.07.2018, abrufbar unter: https://www.wired.co.uk/article/internet-of-things-smart-home-domestic-abuse.

sind und dass Verarbeitungsvorgänge als solche identifiziert werden. Bereits zum korrekten Bestimmen der Rechtsgrundlage für eine Datenverarbeitung darf es sich – dies ist eine generelle Anforderung der DSGVO – bei einem Verarbeitungsvorgang nicht um eine technische „Black Box“ handeln.[30]

Die Verantwortlichen müssen also wissen, welche Vorgänge zu welchen Zwecken personenbezogene Daten auf welche Art und Weise verarbeiten. Dies ist in den Fällen zumeist ein geringeres Problem, wo Verantwortliche die technische Entwicklung ihrer Software selbst in der Hand haben und diese auf Grundlage eigenen technischen Know-hows in eigener Verantwortung vornehmen. Schwieriger ist dagegen die Verwendung von Drittanbietersoftware in Form von Bibliotheken, Schnittstellen oder im Auftrag durch Dritte entwickelte Software.[31]

Verantwortliche, die nicht über das notwendige eigene Know-how verfügen, um alle technischen Details abschätzen zu können, dürfen sich zwar in gewissem Maße auf etwaige Auftragnehmer und Dienstleister verlassen[32], wenn diese die Infrastruktur für Datenverarbeitung entwickeln und einrichten. Ab dem Punkt, an dem substanzielle Risiken für die betroffenen Personen involviert sind, müssen aber die Verantwortlichen in der Lage sein, die Datenverarbeitung in eigener Kompetenz auf sämtlichen Ebenen in ausreichendem Maße nachvollziehen zu können. Hier steigen die Anforderungen an das konkrete Wissen des Verantwortlichen mit der Eingriffsintensität der Datenverarbeitung, die sich aus den konkreten Umstände der Verarbeitung ergibt.[33]

Die bei einem Verarbeitungsvorgang genutzten Komponenten müssen, sofern sie unmittelbar an der Verarbeitung personenbezogener Daten beteiligt sind und ein Risiko begründen können, in ihrer technischen Funktionsweise für den Verantwortlichen bekannt sein. Das bedeutet, dass auch der Verantwortliche selbst hinreichend über die konkrete Verarbeitung etwa in den genutzten Drittbibliotheken informiert sein muss.

Gerade hinsichtlich dieser Anforderung wurde oft kritisiert, dass der europäische Gesetzgeber damit den Verantwortlichen zu schwere Verpflichtungen

[30] Bieker, Bremert u. a. (2018a, b, S. 610).

[31] Hansen und Bremert (2020a, b, S. 141 f.).

[32] Etwa der Betreiber eines Weblogs in Bezug auf die technische Funktionsweise eines durch seinen Webhoster für ihn betriebenen Webservers (Software und Hardware).

[33] Bieker, Bremert u. a. (2018a, b, S. 608 ff.).

auferlegen würde[34] und dass die datenschutzrechtlichen Anforderungen als Innovationshemmnis wirken würden[35]. Diese Kritik lässt aber unberücksichtigt, dass die Verantwortlichen durch die Verarbeitung personenbezogener Daten und dabei durch den Eingriff in fremde Rechte erst die Ursache für die ihnen gesetzlich auferlegten Pflichten setzen.

Verantwortliche können für sich und ihre Tätigkeit zwar eigenen Grundrechtschutz in Anspruch nehmen, dieser wirkt dann aber, soweit Grundrechte anderer Personen betroffen sind, nicht grenzenlos. Die konkreten datenschutzrechtlichen Anforderungen sind damit nur Ergebnis des gesetzgeberischen Abwägungsprozesses, der sowohl die Rechte der Verantwortlichen berücksichtigt als auch die Rechte der durch die Datenverarbeitung betroffenen Personen.

Bei der Risikoerkennung kommt es immer wieder zu der Situation, dass die Verantwortlichen besonders die mit der IT-Infrastruktur zusammenhängenden Risiken beachten und dabei andere Risiken, insbesondere originäre Datenschutzrisiken, unberücksichtigt bleiben.[36] Diese Betrachtung setzt nicht die betroffenen Personen in den Fokus, sondern dient dem unmittelbare Eigeninteresse der Verantwortlichen an einer sicheren IT-Infrastruktur. Dabei kann nicht oft genug darauf hingewiesen werden, dass die Risikoerkennung zwar zuerst den Interessen der betroffenen Person(en) dienen soll, aber auch im Eigeninteresse der Verantwortlichen stattfindet, da die dort erkannten Risiken auch unternehmerische Risiken darstellen: Es ist z. B. denkbar, dass geistiges Eigentum in Form der Software oder Know-how (wie genutzten Algorithmen) verloren werden könnte oder auch Kundendaten, die oft der Monetisierung dienen und jedenfalls als Kundenkontakte unmittelbar den Wert eines Unternehmens bestimmen, von Angreifern entwendet werden könnten. Hierbei zeigt sich ein zentrales Problem im Datenschutz, nämlich dass die Verantwortlichen in Anlehnung an die Informationssicherheit nur Dritte als mögliche Angreifer auf die Grundrechte der betroffenen Personen sehen. Kaum Berücksichtigung findet der einer Datenverarbeitung nächste Akteur: der Verantwortliche, der im Datenschutz oft die erste Risikoquelle darstellt.

---

[34] Leitherer, Ein Schreckgespenst feiert Geburtstag, Springer Professional, 24.05.2019, abrufbar unter: https://www.springerprofessional.de/dsgvo/datenschutz/ein-schreckgespenst-feiert-geburtstag/16734274.

[35] Schürmann, Analyse: KI im Rahmen der Digitalisierungsstrategie – die DSGVO als Innovationsbremse?, t3n, 17.03.2019, abrufbar unter: https://t3n.de/news/ki-rahmen-dsgvo-1148992/.

[36] Friedewald, Bieker u. a. (2017).

3.2.1 Entwicklung eines Frameworks zur Risikoerkennung

Die umfassende Auseinandersetzung mit der eigenen Tätigkeit setzt einerseits die systematische Erfassung der konkreten Verarbeitungsvorgänge voraus und andererseits die Berücksichtigung sämtlicher durch die Verarbeitung tangierter Grundrechte. Der folgende Ansatz ist der Vorschlag für ein entsprechendes Framework[37] zur besseren Darstellung der eigenen Datenverarbeitungsvorgänge und der daraus resultierenden Sichtbarmachung von mit diesen Datenverarbeitungsvorgängen zusammenhängenden Risiken für natürliche Personen. Der Ansatz geht von drei Schritten aus, die Verantwortliche vorab durchführen müssen, um auf eine für die sodann zu erfolgende Risikoerkennung optimierte Verfahrensdokumentation zurückgreifen können:

- Identifikation der personenbezogenen Daten
- Identifikation von Verarbeitungsvorgängen
- Unterteilung der Verarbeitungsvorgänge in Abschnitte und Phasen

Im ersten Schritt sollte dafür eine Übersicht der verarbeiteten personenbezogenen Daten einschließlich ihrer Herkunft und des Ortes der jeweiligen Verarbeitung (d. h. welches (technische) System an welchem Standort welche Daten verarbeitet) angefertigt werden.

Im nächsten Schritt hilft eine systematische Darstellung der einzelnen Datenverarbeitungsvorgänge. Dabei ist es zunächst sinnvoll, einen Datenverarbeitungsvorgang in verschiedene Abschnitte zu unterteilen, um eine bessere Übersicht zu gewährleisten. Bei der Ausarbeitung der verschiedenen Datenverarbeitungsvorgänge ist zu berücksichtigen, dass wesentliche Teile der Datenverarbeitung isoliert dargestellt werden sollten, um die dortigen spezifischen Risiken besser erkennen und verstehen zu können. Hierzu sollten Teile, bei denen zeitliche, funktionelle oder räumliche Zäsuren aufzufinden sind, getrennt dargestellt werden. Zuletzt können die einzelnen Vorgänge in unterschiedliche Phasen eingeteilt werden, um den Kern des jeweiligen Vorgangs herauszuarbeiten. Dadurch werden für wesentliche Teile der Datenverarbeitung Herkunft und Fluss der Daten sichtbar und können bei der Risikoerkennung schneller berücksichtigt werden.

[37] Bieker und Bremert (2020, S. 7).

3.2.2 Verarbeitungsbegriff der DSGVO

Bei der Beschreibung der maßgeblichen Datenverarbeitung stehen die Verantwortlichen vor der Herausforderung, überhaupt alle maßgeblichen Verarbeitungsvorgänge zu erkennen. Die DSGVO selbst definiert dafür *Verarbeitung* in Art. 4 Nr. 2 DSGVO als *„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten“*. Darauf folgt eine Liste mit verschiedenen Beispielen abstrakter Verarbeitungsvorgänge. Verantwortliche sollten sich aber nicht nur an die (nicht abschließende) Liste mit konkreten Beispielen möglicher Verarbeitungsvorgänge in Art. 4 Nr. 2 DSGVO halten, sondern eher einen abstrakten Ansatz wählen.

Die im Gesetzeswortlaut verwendeten Begriffe zeigen, dass ein Verarbeitungsvorgang einerseits technisch (etwa „speichern“ oder „löschen“) und andererseits tatsächlich (etwa „verwenden“ oder „vernichten“) beschrieben werden kann. Daneben können Anknüpfungspunkte die Plattform der Verarbeitung sein (tätigkeitsbezogen, also etwa Software und Hardware) oder eine eher datenbezogene (bzw. ergebnisbezogene, wie z. B. „Offenlegung“) Beschreibung sein.

Für die Einschlägigkeit der Legaldefinition benötigt man lediglich einen „ausgeführten Vorgang“ bzw. eine „Vorgangsreihe“ in Zusammenhang mit personenbezogenen Daten. Dabei kommt es ebenso wenig darauf an, dass der Vorgang oder die Vorgangsreihe eine bestimmte Erheblichkeit aufweist, wie es auf die Laufzeit des konkreten Vorgangs ankommt. Weder kann von der Laufzeit eines Datenverarbeitungsvorgangs auf etwaige Abflüsse personenbezogener Daten, noch kann auf die konkrete Eingriffsstärke geschlossen werden. Sowohl technische und organisatorische Maßnahmen (wie etwa Verschlüsselung) können im konkreten Fall Verarbeitungsschritte darstellen, wie es auch die mittels Techniken des Machine Learnings verarbeiteten und dafür flüchtig gespeicherten Videobilder sind.

3.2.3 Risikoerkennung und datenschutzfremde Risiken

Um in der nun beschriebenen Datenverarbeitung zuverlässig die möglichen Risiken erkennen zu können, müssen die unterschiedlichen Phasen der Datenverarbeitung mit den möglicherweise betroffenen Grundrechten und Freiheiten abgeglichen werden.[38]

[38] Bieker und Bremert (2020, S. 7).

An dieser Stelle stehen die Verantwortlichen häufig vor dem nächsten Problem: der Bestimmung der einschlägigen Grundrechte. Im Zweifel werden die Verantwortlichen bei einer Datenverarbeitung, die bereits bei summarischer Betrachtung als eingriffsintensiv zu qualifizieren ist, einen umfassenden Blick auf infrage kommende Grundrechte werfen und auf etwaige Beeinträchtigungen prüfen müssen.

Gerade in Bereichen, in denen möglicherweise nur bestimmte, marginalisierte Personengruppen betroffen sind, liegen mögliche Ursachen für schwerwiegende Diskriminierungen. Diese aus Sicht der Verantwortlichen womöglich nicht naheliegenden Risiken zu berücksichtigen, ist die wesentliche Aufgabe des im Folgenden dargestellten Prozesses. Zugleich liegt darin eine besondere Schwierigkeit, denn die dargestellten Verarbeitungsvorgänge müssen nun aus einer grundrechtlichen Perspektive untersucht werden.

Das eigens dafür entwickelte Framework macht potenzielle Risiken besser sichtbar, indem eine übersichtliche und systematische Erfassung von Daten und Datenverarbeitungsvorgängen erstellt wird. Auf dieser Grundlage ist ein einfacheres Matching der Datenverarbeitung mit etwa betroffenen Rechten und Freiheiten möglich.

Beeinträchtigungen von Grundrechten können ihrer Wirkung entsprechend in einen zeitlichen Zusammenhang zur Datenverarbeitung gesetzt werden. Das führt dazu, dass die Auswirkungen einer Datenverarbeitung konkrete Auswirkungen auf die Grundrechtsausübung im zeitlichen Umfeld zur Datenverarbeitung haben kann. Eine zeitliche Betrachtung kann sich daher auf Auswirkungen im Vorfeld der Datenverarbeitung, Auswirkungen im Zeitpunkt der Datenverarbeitung sowie auf Auswirkungen im Nachgang der Datenverarbeitung beziehen (Abb. 1).

Im *Vorfeld der Datenverarbeitung* können insbesondere Chilling Effects und Überwachungsdruck dazu führen, dass die betroffene Person Grundrechte gar nicht oder nicht wie ursprünglich gewünscht ausübt. Die sog. Chilling effects beschreiben eine Situation, in der eine betroffene Person auf die Ausübung von Grundrechten verzichtet oder sie nicht wie gewünscht ausübt, da sie mit negativen (oft juristischen) Konsequenzen rechnet.[39] Es handelt sich im Ergebnis um eine Selbstbeschränkung durch Einschüchterung.[40] Überwachungsdruck führt dazu, dass sich eine betroffene Person bei der Ausübung ihrer Freiheitsrechte überwacht

[39] Bieker und Bremert (2020, S. 10); MMR-Aktuell (2014), 357362.

[40] Kersten (2017, S. 197).

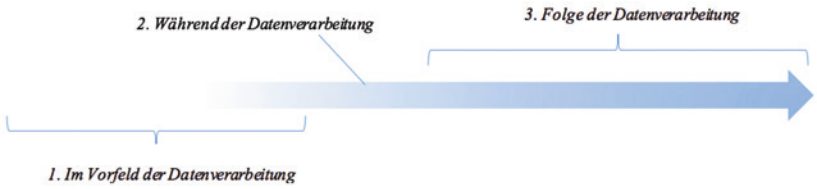

Abb. 1 Zeitliche Betrachtung grundrechtsrelevanter Auswirkungen

und deswegen beeinträchtigt fühlt. Dieses Gefühl kann auch in einer Situation eintreten, in der sie eine Überwachung „objektiv ernsthaft befürchten" muss.[41] Die betroffene Person unterlässt in diesen Fällen also in Ansehung einer Datenverarbeitung die Ausübung ihrer entsprechenden Grundrechte. Denkbar ist dies in Fällen, in denen an einer Demonstration nicht teilgenommen wird, weil die Polizei Teile der Demonstration filmt und man entweder mit Sanktionen rechnet oder schon die Verknüpfung von Teilnahme und Thema der Demonstration im konkreten Fall negative Implikationen für Teilnehmende haben kann.

Auch *während die eigentliche Datenverarbeitung stattfindet,* kann die Grundrechtsausübung als solche beeinträchtigt werden. Dies ist insbesondere in Fällen relevant, in denen Verantwortliche die Verarbeitung personenbezogener Daten auf eine Rechtsgrundlage stützen wollen, deren Tatbestandsvoraussetzungen gar nicht vorliegen und insoweit der Eingriff nicht gerechtfertigt wird.

Schließlich kann als *Folge der Datenverarbeitung* etwa der Erfolg der Grundrechtsausübung verhindert oder die Ausübung aus Sicht der betroffenen Person sanktioniert werden. Hier ist etwa der Fall denkbar, dass eine Online kundgetane Meinungsäußerung sanktioniert werden soll. Dafür will man sich eines sog. Social Scores bedienen, also mittels Beurteilung verschiedener Verhaltensweisen oder Äußerungen eine Bewertung der Nutzerinnen und Nutzer vornehmen. Gewünschte Verhaltensweisen und Äußerungen wirken sich dabei positiv auf die Bewertung aus, Unerwünschtes wirkt dagegen negativ. Dafür sollen Online getätigte Meinungsäußerung gecrawlt und verarbeitet werden, um diesen Social Score generieren zu können und ungewünschte Meinungsäußerung im Nachhinein sanktionieren zu können.

[41] BGH, Urteil vom 16.03.2010 – VI ZR 176/09 = NJW 2010, 1533 (1534).

3.3 Risikobewertung

Nachdem die Verantwortlichen die möglichen Risiken erfolgreich identifiziert haben, müssen diese Risiken bewertet werden. Dabei setzt der Risikobegriff der DSGVO grundsätzlich zwei Komponenten der Bewertung voraus, nämlich die Eintrittswahrscheinlichkeit und die Schwere des möglichen Schadens.[42] Dabei müssen die Verantwortlichen, wie auch bei der Risikoidentifizierung, die Perspektive der betroffenen Personen einnehmen und können sich nicht auf Risiken für ihre Organisation beschränken.

Grundsätzlich hängt die Einordnung maßgeblich von der Art, dem Umfang, den Umständen und den Zwecken der Datenverarbeitung ab.[43] Irrelevant ist dagegen, wenn die Risiken im konkreten Fall keine von den Verantwortlichen intendierte Folge der Datenverarbeitung sind. Zur Beurteilung der Eintrittswahrscheinlichkeit haben die Verantwortlichen eine Prognoseentscheidung zu treffen[44], sie beruht entweder auf statistischen Erfahrungswerten[45] oder auch nachvollziehbaren, objektiven Erwägungen[46].

Der erste Schritt in der Bewertung ist die Vorüberlegung, wie die Schwere und Eintrittswahrscheinlichkeit besser greifbar und vergleichbar bezeichnet werden kann. Zur besseren Handhabung beider Kategorien hat sich dafür die Nutzung einer Stufenskala bewährt. Hierbei kann etwa auf ein Modell aus drei (leicht, mittel und schwer)[47] oder vier Stufen (geringfügig, überschaubar, substanziell und groß)[48] zurückgegriffen werden. Durch die Nutzung eines Stufenmodells kann zwar eine Vergleichbarkeit hergestellt werden, es wird aber durch Vermeidung von absoluten Zahlenwerten nicht der Eindruck eines in Wirklichkeit nur pseudowissenschaftlichen Systems vermittelt.[49]

Bei der Frage der Bewertung können verschiedene Aspekte eine Rolle spielen. So ist die Bedeutung des Schadens für die betroffene Person ein erster Ansatz-

[42] ErwGr. 75 Satz 2 DSGVO.

[43] ErwGr. 76 bzw. 94 Satz 2 DSGVO.

[44] Lang, in: Taeger und Gabel (2019), Art. 24 Rn. 54.

[45] Martini, in: Paal und Pauly (2018), Art. 24 Rn. 30.

[46] ErwGr. 76 DSGVO.

[47] Alexy (2003, S. 772).

[48] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2018, S. 4).

[49] Vgl. Bieker, Hansen u. a. (2016, S. 193).

punkt. Es muss allerdings auch berücksichtigt werden, ob der betroffenen Person eine Möglichkeit der Einflussnahme offensteht oder sie sich der konkreten Datenverarbeitung entziehen kann. Genauso wie die konkrete Kenntnis der Datenverarbeitung sind diese Aspekte bei der Bewertung zu berücksichtigen.

Sowohl die Schwere möglicher Schäden als auch die Eintrittswahrscheinlichkeit können sodann von verschiedenen Aspekten der Datenverarbeitung abhängen; die DSGVO nennt dafür die Art (nature), den Umfang (scope), die Umstände (context) und die Zwecke (purposes) der Datenverarbeitung:

Art (nature)
Gerade die Beurteilung der Schwere der möglichen Rechtsgutverletzung kann im Einzelfall eine große Herausforderung für die Verantwortlichen und für die betroffenen Personen ein neues spezifisches Risiko der Fehleinschätzung darstellen. Zunächst sind die Gegebenheiten der Datenverarbeitung zu berücksichtigen, denn ihre Art im konkreten Fall kann eine besondere Schwere möglicher Rechtsverletzungen indizieren.

Hierbei ist sowohl die Art der Datenverarbeitung selbst zu berücksichtigen, also ihre technische Ausgestaltung im konkreten Fall, als auch die Art der personenbezogenen Daten, die Gegenstand dieser Datenverarbeitung sind. Gerade in den Fällen, in denen die Datenverarbeitung aufgrund ihrer technischen Ausgestaltung (etwa bei der Nutzung einer "Künstlichen Intelligenz") für die Verantwortlichen weniger handhabbar und dadurch besonders gefahrgeneigt ist, muss dieser Umstand bei der Bewertung berücksichtigt werden.

Im nächsten Schritt sind die Arten der verarbeiteten personenbezogenen Daten zu betrachten. Dabei ist gerade ihre spezifische Bedeutung für die betroffene Person zu berücksichtigen. So können auf den ersten Blick normal sensible personenbezogene Daten aufgrund besonderer Umstände der betroffenen Person ein besonderes Gefahrenpotenzial innewohnen. Diese besonderen Umstände können insbesondere mit den in Art. 9 Abs. 1 DSGVO genannten persönlichen Attributen der betroffenen Person zusammenhängen; die Fallgruppen sind allerdings nicht auf die dort genannten Fälle beschränkt.[50]

In anderen Situationen kann sich bereits aus der Art der personenbezogenen Daten ihre besondere Sensibilität ergeben, ohne dass es auf eine besondere Situation der betroffenen Person ankäme, da diese Daten für alle denkbaren Personen im Kontext einer Datenverarbeitung eine besondere Gefährlichkeit

[50] Weitere Kategorien ergeben sich etwa aus dem Recht auf Nichtdiskriminierung.

aufweisen würden. Diese sensiblen Daten stellen insbesondere die Gruppe der besonderen Kategorien von personenbezogen Daten aus Art. 9 Abs. 1 DSGVO dar.

Aus der Dauer einer Datenverarbeitung lassen sich nur sehr wenig Anhaltspunkte für das Risiko aus der Art der Datenverarbeitung ziehen. Die Dauer der Datenverarbeitung hängt neben der Art der Datenverarbeitung maßgeblich von deren Implementierung und der Leistungsfähigkeit der Hardware ab, auf der diese stattfindet. Da besonders die beiden letzten Faktoren sehr subjektiv sind und mit der notwendigen Hardware mittlerweile äußerst komplexe Datenverarbeitungsvorgänge in Bruchteilen einer Sekunde stattfinden, lässt die Dauer der Datenverarbeitung kaum Rückschlüsse auf ihre Gefahrgeneigtheit zu. Anders wäre dies eventuell zu werten, wenn es gerade um die Flüchtigkeit der während der Datenverarbeitung gewonnenen Daten ginge (etwa als Maßnahme zur Datenminimierung oder Verringerung des durch die Datenverarbeitung erfolgen Eingriffes) und Daten durch die Dauer länger persistent im Speicher existieren.[51]

Umfang (scope)

Der Umfang der Datenverarbeitung hängt eng mit der Art der Datenverarbeitung zusammen. In ErwGr. 91 Satz 3 sieht der Gesetzgeber eine „systematisch in großen Umfang" erfolgende Datenverarbeitung als mögliche Voraussetzung für eine Datenschutz-Folgenabschätzung, mithin als Indiz für ein hohes Risiko i.S.v. Art. 35 Abs. 1 Satz 1 DSGVO. Eine solche „systematisch in großen Umfang" erfolgende Datenverarbeitung kann auf verschiedenen Ebenen stattfinden: Naheliegend ist zunächst die quantitative Berücksichtigung der betroffenen Personen: das Risiko einer Datenverarbeitung steigt bereits mit der bloßen Anzahl an Personen deren personenbezogene Daten verarbeitet werden. Diesen Aspekt werden Verantwortliche in der Regel erkennen können, da sich bereits aus Informationssicherheitserwägungen ergibt, dass eine große Menge an Datensätzen zu Begehrlichkeit für Angreifer führen kann.

Der Umfang kann sich allerdings auch auf die technische Ebene der Datenverarbeitung auswirken, denn einerseits kann die quantitative Menge an Datenverarbeitungsvorgängen Berücksichtigung finden, die sich wiederum aus der Komplexität einer einzelnen zusammenhängenden Verarbeitungstätigkeit zusammensetzen können oder auf der anderen Seite eine große Anzahl an wiederkehrendenden Datenverarbeitungsvorgängen bestehen kann. Andererseits kann auch die bloße Menge an personenbezogenen Daten zu spezifischen Risiken

[51] Martini, in: Paal und Pauly (2018), Art. 24 DSGVO Rn. 35a.

führen, etwa umfangreiche Bewegungsprofile bestehend aus einzelnen Aufenthaltsorten und den jeweiligen abgeleiteten Bewegungsvektoren. Gleiches gilt für den Fall, dass große Mengen besonders schutzwürdiger Daten verarbeitet werden, da eine eingriffsintensivere Datenverarbeitung auch gleichzeitig eine risikoreichere Datenverarbeitung darstellt. Für diesen Rückschluss hat der Gesetzgeber dort eine Ausnahme vorgesehen, wo die Berufsausübung spezieller, aufgrund besonderer Vertrauensstellung privilegierter Berufsgruppen betroffen ist.[52]

Im Rahmen der Betrachtung des Umfangs einer Datenverarbeitung müssen aber auch etwaige Querbezüge und Auswirkungen unterschiedlicher Datenverarbeitungsvorgänge berücksichtigt werden. So können sich Wirkungen und Wirkweisen einer Datenverarbeitung im Zusammenspiel mit anderen Datenverarbeitungen verstärken oder verändern, sodass auch diese spezifischen Risiken im Sinne einer „Überwachungsgesamtrechnung“ Eingang in die Risikobetrachtung finden müssen.[53]

Umstände (context)

Die spezifische Schwere des möglichen Eingriffes kann sich auch aus den Umständen der Datenverarbeitung ergeben. Hierzu zählen einerseits persönliche Umstände, die etwa in der Person der Betroffenen zu finden sind, situative Umstände, also eine spezifische Gefährlichkeit etwa der Erhebung der personenbezogenen Daten und/oder der weiteren Verarbeitung und die qualitative Gefährlichkeit der Datenverarbeitung. Dieser Aspekt überschneidet sich auch mit der Art und dem Umfang der Datenverarbeitung.

Die Auswirkungen von Verarbeitungsvorgängen können auch über die Grenzen einzelner Verantwortlichkeit hinaus relevant sein. So sind gerade im Bereich der Überwachungsgesetze und Rechtsgrundlagen für konkrete Überwachungsmaßnahmen nicht nur die Auswirkungen des konkreten Vorhabens im Rahmen einer etwaigen Gesetzes-DSFA zu überprüfen, sondern auch bisherige Maßnahmen und deren Umsetzung bzw. konkrete Anwendung in die Risikobetrachtung einzubeziehen. Mithilfe dieser „Überwachungsgesamtrechnung“ muss sichergestellt werden, dass die „Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf“[54]. In die gleiche Richtung ging auch die Argumentation

[52] ErwGr. 91 Satz 4 DSGVO.

[53] Bieker, Bremert u. a. (2018a, b).

[54] BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08 u. a. = BVerfGE 125, 260 Rn. 218 („Vorratsdatenspeicherung“).

des BVerfG bei den Entscheidungen zum Scanning von Kfz-Kennzeichen.[55] Hier stellte das BVerfG fest, dass derartige anlasslose Maßnahmen[56] nicht flächendeckend stattfinden dürften.

Zwecke (purposes)
Auch die Zwecke der Datenverarbeitung haben in der Regel Auswirkung auf die Risikobewertung. So können die Zwecke ein besonderes Gefahrenpotenzial darstellen, wenn der Zweck ein spezifisches Risiko für Eingriffe in die Rechte und Freiheiten der betroffenen Personen schafft. Ähnlich deutlich sind auch die Auswirkungen auf die Eintrittswahrscheinlichkeit, denn durch die Zwecke kann die Eintrittswahrscheinlichkeit spezifischer Schäden deutlich erhöht werden: Denkbar sind Fälle, in denen es bei der Datenverarbeitung darum geht, personenbezogene Daten zu veröffentlichen, und so das Risiko der Verknüpfung mit anderen personenbezogenen Daten nicht nur abstrakt eröffnet, sondern durch die Veröffentlichung konkret erhöht wird.

Das Vorgehen nach dem vorgestellten Framework ermöglicht es Verantwortlichen die Risikoerkennung gerade im Kontext komplexer Datenverarbeitungsvorgänge zu optimieren. Der konkrete Umfang und notwendige Detailierungsgrad ist dabei jeweils von der Komplexität der jeweiligen Datenverarbeitung abhängig. Dabei obliegt den Verantwortlichen gerade bei Datenverarbeitungsvorgängen, die sich schon bei summarischer Betrachtung als besonders gefahrengeneigt für die Rechte und Freiheiten natürlicher Personen erweisen, eine besondere Darlegungslast für die Berücksichtigung dieser Risiken. Diese Pflicht wiegt umso schwerer, wenn die Gefahrengeneigtheit ansteigt. In diesen Fällen ist also eine systematische und kritische Auseinandersetzung mit der eigenen Datenverarbeitung angezeigt. Hier wäre das Framework eine mögliche Option der Systematisierung dieses Vorgehens und könnte im Sinne der Verantwortlichen auch dafür sorgen, dass neben der Erkennung von Datenschutz-Risiken auch ein allgemeines Risikomanagement besser funktioniert.

[55] BVerfG, Beschlüsse vom 18.12.2018 – 1 BvR 142/15 („Kfz-Kennzeichenkontrolle 2“) bzw. 1 BvR 2795/09, 1 BvR 3187/10 („Kfz-Kennzeichenkontrolle BW-HE“).

[56] Da das Kennzeichenscanning nicht an individuelles Verhalte anknüpfe und daher im größten Teil der Fälle alleine durch Abgleich des tatsächlichen mit dem gesuchten Kennzeichen einen Eingriff ohne entsprechende Gefährdung durch die betroffene Person darstelle.

4 Die Umsetzung der Anforderung einer datenschutzkonformen Systemgestaltung

Die Vorgaben für „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“, die der Verantwortliche erfüllen muss, sind in Art. 25 DSGVO geregelt.[57] Dieser Abschnitt beschreibt einerseits die Anforderungen an die Gestaltung (Art. 25 Abs. 1 DSGVO) – Datenschutz „by Design“ –, andererseits die Anforderung, dass datenfreundliche Voreinstellung – Datenschutz „by Default“ – zu verwenden sind (Art. 25 Abs. 2 DSGVO). Schließlich nimmt Art. 25 auch Bezug zu den Zertifizierungsmöglichkeiten nach der DSGVO (Art. 25 Abs. 3 DSGVO). Im Folgenden werden Datenschutz durch Technikgestaltung und Datenschutz durch datenschutzfreundliche Voreinstellungen erläutert.

4.1 Datenschutz durch (Technik-)Gestaltung

Der Verantwortliche muss nach Art. 25 Abs. 1 DSGVO geeignete technische und organisatorische Maßnahmen treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO zu genügen und die Rechte der betroffenen Personen zu schützen. Dabei zu berücksichtigen sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken. Diese Faktoren sind einerseits beschränkende Bedingung, denn es ist nicht in jedem Fall das Höchstmaß des Möglichen zu implementieren; andererseits stellen die Faktoren aber auch eine Minimalanforderung dar, hinter der der Verantwortliche nicht zurückbleiben darf. Auf keinen Fall darf man beispielsweise angesichts eines festgestellten hohen Risikos auf geeignete Maßnahmen verzichten, weil sie Geld kosten; stattdessen wäre ohne geeignete Maßnahmen

[57] Bieker und Hansen (2017).

zur ausreichenden Eindämmung eines hohen Risikos eine derartige Verarbeitung nicht zulässig.

Vielfach diskutiert wird der Faktor „Stand der Technik“[58], der bereits im Vorläufer der DSGVO – der Datenschutz-Richtlinie 95/46/EG – Erwähnung fand (Art. 17 der Richtlinie zur Sicherheit der Verarbeitung). Dieser Faktor ist sowohl für „Datenschutz durch Technikgestaltung“ (Art. 25 DSGVO) also auch für die „Sicherheit“ (Art. 32 DSGVO) anzulegen. Für den Bereich der Sicherheit der Verarbeitung personenbezogener Daten gibt es seit vielen Jahren umfangreiche Maßnahmenkataloge, die regelmäßig überarbeitet und an den Entwicklungsstand angepasst werden.[59] Für technische und organisatorische Maßnahmen oder insgesamt für datenschutzfreundliche und –fördernde Konzepte liegen noch keine vergleichbaren Ausarbeitungen vor, auch wenn erste Ansätze für Bewertungsmaßstäbe des Reifegrads unter Einbeziehung der Wirksamkeit und etwaiger Interdependenzen entwickelt worden sind.[60]

Die Maßnahmen müssen sowohl im Vorfeld, nämlich zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung, als auch während der Verarbeitung getroffen werden. Als Beispiel für eine Maßnahme wird die Pseudonymisierung genannt, als Beispiel eines der Datenschutzgrundsätze wird die Datenminimierung aufgeführt.

Allerdings bleibt es bei recht abstrakten Aussagen, sodass man in der DSGVO keine konkreten Hilfen dazu findet, was genau für die eigene Verarbeitung personenbezogener Daten zu tun ist.[61] Unterstützung leistet eine Veröffentlichung des Europäischen Datenschutzausschusses, die zwei Jahre nach Wirksamwerden der DSGVO erschienen ist.[62] Förderlich für den Entwicklungsprozess sind weitgehend unabhängig von der europäischen Gesetzgebung erarbeitete

[58] Bundesverband IT-Sicherheit e. V. und TeleTrusT, IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik“ – Technische und organisatorische Maßnahmen, 2021 (frühere Fassung: 2019), https://www.stand-der-technik-security.de/.

[59] Hansen, in Simitis, Hornung u. a. (2019), Art. 32 Rn. 22 ff.

[60] ENISA, (2015, 12, 19 ff.); Hansen et al. (2015, S. 8 ff.).

[61] Umfassender Hansen, in: Simitis, Hornung u. a. (2019), Art. 25.

[62] European Data Protection Board (2020).

Ausführungen zu „Privacy Design Strategies“[63] und „Privacy Design Patterns“[64]. Für den nach Art. 25 DSGVO verpflichteten Verantwortlichen sind die folgenden zwei miteinander verwandten Ansätze von Nutzen, um für ihre konkreten Verarbeitungen die datenschutzrechtlichen Anforderungen umsetzen.

4.1.1 Operationalisierung der Datenschutzgrundsätze

Da die Essenz der DSGVO in den Datenschutzgrundsätzen widergespiegelt wird und diese auch explizit in Art. 25 Abs. 1 DSGVO genannt werden, besteht eine Möglichkeit der Umsetzung, sich für jeden Datenschutzgrundsatz zu überlegen, welche technischen und organisatorischen Maßnahmen zum Einsatz kommen sollen, um die Umsetzung in der Verarbeitung zu gewährleisten oder zumindest zu unterstützen.[65]

Im Datenschutzgrundsatz „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“ (Art. 5 Abs. 1 Buchst. a) versammeln sich verschiedene allgemeine Anforderungen an die Verarbeitung. Bezüglich der Rechtmäßigkeit der Verarbeitung muss dem Verantwortlichen klar sein, dass technische und organisatorische Maßnahmen eine Verarbeitung, die einer Rechtsgrundlage entbehrt, nicht in eine rechtmäßige Verarbeitung verwandeln kann. Solche Maßnahmen können aber notwendig für die Rechtmäßigkeit sein und eine solche auch dadurch unterstützen, indem der Verantwortliche Vorgaben an die Einführung einer Verarbeitung erstellt und durchsetzt, dass z. B. zunächst eine Rechtsgrundlage festzustellen und zu dokumentieren ist und ein geordneter Freigabeprozess durchgeführt werden muss. Im Falle einer Einwilligung kämen beispielsweise technische und organisatorische Maßnahmen zu einem Einwilligungsmanagement, einschließlich praxistauglicher Funktionen zum Widerruf der Einwilligung, infrage.

Die Verarbeitung nach Treu und Glauben, in der englischen Fassung der DSGVO „Fairness“, beinhaltet die faire Gestaltung der Verarbeitung. Dies kann so verstanden werden, dass die Perspektive der betroffenen Personen bei der Entwicklung und im Betrieb der Verarbeitung Berücksichtigung findet (siehe vorne: ähnlich der „mehrseitigen Sicherheit“) und ihnen das Wahrnehmen der Betroffenenrechte möglichst einfach möglich ist. Auch eine Unterstützung der

[63] Hoepman (2014, S. 446).

[64] Doty und Gupta (2013); UC Berkeley School of Information, Privacy Patterns, Stand 2020, https://privacypatterns.org/.

[65] Hansen, in: Simitis, Hornung u. a. (2019), Art. 25 Rn. 62 ff.

Verwendung von Selbstdatenschutz-Tools[66] der betroffenen Personen lässt sich aus diesem Datenschutzgrundsatz ableiten.

Der Datenschutzgrundsatz der Transparenz, der durch Artt. 12 ff. DSGVO konkretisiert wird, bedeutet insbesondere, dass „alle Informationen und Mitteilungen zur Verarbeitung“ der personenbezogenen Daten „leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind“ (ErwGr. 39 S. 3). Ein situations- und zielgruppengerechtes Informieren der betroffenen Personen muss angesichts der verschiedenen Einsatzszenarien zu den zur Verfügung stehenden Benutzungsoberflächen passen. Bewährt haben sich Mehr-Ebenen-Formate (Multi-Layer), die gestuft die jeweils nötigen oder von der betroffenen Person gewünschten Informationen darstellen.[67] Auch Bildsymbole (siehe Art. 12 Abs. 7 DSGVO) oder andere nichttextliche Aufbereitungen können für den Einzelfall hilfreich sein. Auch sog. Datenschutz-Dashboards, Datenschutz-Cockpits oder andere Transparency-Enhancing Technologies (TETs, als Ergänzung zu PETs[68]) sollen die Transparenz verbessern.

Bei der Umsetzung des Datenschutzgrundsatzes der Zweckbindung (Art. 5 Abs. 1 Buchst. b) ist auf das sorgfältige Festlegen des Zwecks zu achten. Zweckbindung bedeutet, dass es für die personenbezogenen Daten keine Verarbeitung geben darf, die nicht mit den festgelegten Zwecken vereinbar ist. Unterstützende technische und organisatorische Maßnahmen sind beispielsweise ein Verzicht auf zentrale Datensammlungen und zweckübergreifend nutzbare Identifikatoren, physische oder logische Trennung oder Isolation der Daten, Verschlüsselung der Daten, Kennzeichnung der Zwecke und Verknüpfen mit den Daten (z. B. über sog. „Sticky Policies“).

Art. 25 DSGVO hebt die Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) als wichtigen Datenschutzgrundsatz bezüglich der Gestaltung hervor. Auch ErwGr. 78 S. 3 nennt als erste beispielhafte Maßnahme die Minimierung der Verarbeitung personenbezogener Daten. Das bedeutet zum einen, den Personenbezug von Daten einzuschränken, z. B. durch Trennung von Daten und Verzicht auf zweckübergreifende Identifikatoren, durch Löschung, Anonymisierung[69]

[66] Karaboga, Masur u. a. (2014).

[67] Art.-29-Datenschutzgruppe (2004).

[68] Fischer-Hübner und Berthold (2017, S. 759).

[69] Art.-29-Datenschutzgruppe (2014).

oder Pseudonymisierung[70] zum frühestmöglichen Zeitpunkt. Zum anderen ist die Verarbeitung an sich zu minimieren, beispielsweise durch Beschränkung der Erhebung und Erfassung von Daten sowie bereits der Erhebungs- und Erfassungsmöglichkeit, indem beispielsweise nicht erforderliche Video-, Audio- und Sensorfunktionalität nicht Bestandteil der verwendeten Hardware sind.[71] Auch auf zusätzliche Verarbeitungen ist zu verzichten, und die Zahl der betroffenen Personen ist zu minimieren.

Technische und organisatorische Maßnahmen des Integritätsschutzes für die Daten und die Verarbeitung unterstützen den Datenschutzgrundsatz der Richtigkeit (Art. 5 Abs. 1 Buchst. d DSGVO). Auch das Aufsetzen eines Verfahrens zur Berichtigung oder Vervollständigung der personenbezogenen Daten kann hier helfen.

Der mit der Datenminimierung verwandte Datenschutzgrundsatz der Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e DSGVO) lässt sich mit ähnlichen Maßnahmen umsetzen. Die Pseudonymisierung als eine Maßnahme wird bereits in Art. 25 Abs. 1 DSGVO genannt. Ebenfalls können Anonymisierung oder Löschen zur Speicherbegrenzung beitragen. All diese Maßnahmen sind so früh wie möglich durchzuführen. Dies kann vielfach automatisch geschehen, z. B. durch eincodierte Löschfristen oder zumindest durch definierte Prüffristen, damit dann über eine weitere etwa erforderliche Aufbewahrung entschieden wird und andernfalls die Löschfreigabe erfolgt.

Der Datenschutzgrundsatz der Integrität und Vertraulichkeit (Art. 5 Abs. 1 Buchst. f DSGVO) zielt auf sämtliche technische und organisatorische Maßnahmen der Informationssicherheit in Bezug auf personenbezogener Daten, um eine unbefugte oder unrechtmäßige Verarbeitung zu verhindern. Hier liegt eine Parallelität zu den Anforderungen des Art. 32 DSGVO vor. Dies umfasst laut ErwGr. 78 S. 3 Maßnahmen, die den Verantwortlichen in die Lage versetzen, Sicherheitsfunktionen zu schaffen und zu verbessern. Dazu ist es notwendig, die Anforderungen gemäß dem vorliegenden Schutzbedarf zu erfüllen und die getroffenen Maßnahmen regelmäßig zu überprüfen und ggf. zu aktualisieren.

Auch der Datenschutzgrundsatz der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) erfordert ein regelmäßiges Prüfen, inwieweit die datenschutzrechtlichen Anforderungen erfüllt sind, verbunden mit einem Nachsteuern und Anpassen an möglicherweise veränderte Bedingungen. Hier können technische

[70] Siehe auch Schwartmann und Weiß (2017); Hansen und Walczak (2019), S. 53; ENISA (2018a); ENISA (2019); ENISA (2021).

[71] Dies kann zusätzlich ein Sicherheitsrisiko darstellen, vgl. Hansen, in: Hornung und Schallbruch (2021), Rn. 42 ff.

und organisatorische Maßnahmen ein umfassendes Datenschutzmanagementsystem unterstützen. Dazu gehören z. B. die Erstellung und Anpassung der Dokumentation von Prozessen und informationstechnischen Systemen sowie das Protokollieren von Änderungen oder anderen nachzuweisenden Ereignissen, um dauerhaft die Erfüllung der Anforderungen der Verordnung zu gewährleisten.[72]

4.1.2 Das Standard-Datenschutzmodell mit sieben Gewährleistungszielen

In der Informationssicherheit ist man seit Jahrzehnten gewohnt, mit Schutzzielen (protection goals) zu arbeiten. Zwar gibt es vielfältige Ansätze für mehr oder weniger komplexe Schutzzielkanons, aber als fundamental für Informationssicherheit werden die Schutzziele Vertraulichkeit (confidentiality), Integrität (integrity) und Verfügbarkeit (availability) angesehen. Weil diese nicht ausreichen, um sämtliche Datenschutzanforderungen zu beschreiben, für die technische und organisatorische Maßnahmen getroffen werden sollten, gleichzeitig aber eine Kommunikation mit den Zuständigen für die Gestaltung von Technik und Prozessen anschlussfähig an die klassischen Schutzziele der Informationssicherheit sein sollte, wurden im Jahr 2009 weitere Schutzziele vorgeschlagen.[73] Die von der deutschen Datenschutz-Diskussion ausgehenden, teilweise auch international[74] weitergeführten Debatten mit Beteiligung von Wissenschaft und Datenschutzaufsicht haben schließlich das Standard-Datenschutzmodell mit sieben Gewährleistungszielen hervorgebracht: Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Intervenierbarkeit, Nicht-Verkettung von personenbezogenen Verfahren sowie die übergreifende Anforderung der Datenminimierung. Diese Gewährleistungsziele ähneln den Schutzzielen der Informationssicherheit; wichtig ist dabei stets die Anwendung aus der Perspektive der betroffenen Personen, wie dies auch bei der Bestimmung des Risikos für die Rechte und Freiheiten (siehe vorne) notwendig ist.

Beim „Standard-Datenschutzmodell“ (SDM) handelt es sich um eine Methode für die Beratungs- und Prüfpraxis im operativen Datenschutz. Das SDM wird von den deutschen Datenschutzaufsichtsbehörden zur Anwendung empfohlen.[75]

---

[72] Hansen, in: Simitis, Hornung u. a. (2019), Art. 25 Rn. 69.

[73] Rost und Pfitzmann (2009).

[74] Hansen, Jensen u. a. (2015); Danezis, Domingo-Ferrer u. a. (2015).

[75] Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2016).

Dieses Werkzeug unterstützt die risikoadäquate Auswahl und Bewertung technischer und organisatorischer Maßnahmen und ist hilfreich bei der Erfüllung der Rechenschaftspflichten der Datenschutz-Grundverordnung.[76]

Die ersten Versionen des SDM sind lange vor Geltung der DSGVO entstanden und konnten daher auch noch nicht auf die Datenschutzgrundsätze eingehen. Mit der Version 2.0 wurde das SDM überarbeitet, um sich besser in die Terminologie und die Konzepte der DSGVO einzufügen und damit die Verwendung für die Verantwortlichen und Auftragsverarbeiter zu erleichtern. Auch eine englische Fassung steht zur Verfügung.

Maßnahmenkataloge mit generischen Bausteinen zu Referenz-Schutzmaßnahmen befinden sich in der Entwicklung oder sind bereits verfügbar. Beispielsweise gehören dazu die Bausteine „Aufbewahren", „Dokumentieren", „Protokollieren", „Trennen", „Löschen und Vernichten", „Berichtigen" und „Einschränken der Verarbeitung".[77] Weitere Bausteine sind in Bearbeitung. Bei der Überarbeitung werten die Datenschutzaufsichtsbehörden das Feedback der Verantwortlichen und Auftragsverarbeiter beim Einsatz des SDM aus, um das Werkzeug zu verbessern und die Praxistauglichkeit zu erhöhen.

Zunächst setzt das SDM bei der Umsetzung der Anforderungen nach Art. 32 DSGVO an; es geht aber durch die deutliche Datenschutzausrichtung über die bestehenden technischen Regelwerke hinaus und umfasst generell technische und organisatorische Maßnahmen zum Einbauen der Anforderungen der DSGVO (und damit auch Art. 25 DSGVO). Das SDM orientiert sich in seiner Methodik an den Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI), die Grundlage für einen IT-Grundschutz sind und deren Maßnahmenbeschreibungen ständig aktualisiert werden. Dagegen etwas weniger konkret sind die internationalen ISO/IEC 27001-Normen, die sich z. B. um den Maßnahmenkatalog der ISO/IEC 27002 ergänzen lassen, oder die Common Criteria, ISO/IEC 15408, mit denen man Sicherheitseigenschaften von IT-Produkten prüfen und bewerten kann.

Mit dem SDM und den Gewährleistungszielen lassen sich insgesamt die Datenschutzgrundsätze und die weiteren Anforderungen der DSGVO abbilden.[78] Bezüglich der Betroffenenrechte legt das SDM mit dem Gewährleistungsziel der Intervenierbarkeit sogar einen deutlicheren Fokus, als dies beim (zumindest

[76] https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/, https://www.datenschutzzentrum.de/sdm/.

[77] Stand: Herbst (2020).

[78] Vgl. auch Bieker, (im Erscheinen, S. 222 ff.).

flüchtigen) Lesen der Datenschutzgrundsätze in Art. 5 DSGVO vermittelt wird. Auch im Rahmen der Datenschutz-Folgenabschätzung kann das SDM eingesetzt werden, wie in verschiedenen Muster- und realen Beispielen erprobt.[79]

4.2 Datenschutz durch datenschutzfreundliche Voreinstellungen

Auch bei der Anforderung des Datenschutzes durch datenschutzfreundliche Voreinstellungen trifft die Pflicht den Verantwortlichen (Art. 25 Abs. 2 DSGVO). Im Gegensatz zum ersten Absatz des Art. 25 sieht die DSGVO keine (möglicherweise relativierenden) Faktoren vor, die bei der Auswahl der zu treffenden Maßnahmen zu berücksichtigen sind.[80] Vielmehr müssen die geeigneten technischen und organisatorischen Maßnahmen getroffen werden, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Damit wird der Maßstab der Erforderlichkeit, der sich auch in den Datenschutzgrundsätzen der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO) und der Speicherbegrenzung (Art. 5 Abs. 1 Buchst. e DSGVO) findet, betont und im Folgenden spezifiziert: „Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit." (Art. 25 Abs. 2 S. 2 DSGVO). Die Voreinstellung muss also gewährleisten, dass keine überschießenden Daten verarbeitet werden, dass die Verarbeitung sich auf das notwendige Maß beschränkt, dass die Speicherdauer möglichst gering ist und dass die Daten keinen zu weitgehenden Zugriffsmöglichkeiten ausgesetzt sind. Besonders der letzte Punkt verdeutlicht, dass damit auch Gestaltungsoptionen verschränkt sein können, beispielsweise bezüglich des Orts einer Speicherung (lokal oder in der Cloud, sodass die Daten einem Betreiber oder den dortigen Behörden zugänglich werden könnten), der Zugriffsrechte oder einer Verschlüsselung, die den Klartext dem Zugang entzöge.[81]

Nicht immer sind die datenschutzfreundlichsten Voreinstellungen für jede Nutzerin und jeden Nutzer gleich oder eindeutig im Vorfeld erkennbar.

[79] Siehe beispielsweise Martin u. a. (2020).

[80] Bieker und Hansen (2017, S. 165); Hansen, in: Simitis, Hornung u. a. (2019), Art. 25 Rn. 39 ff.

[81] ENISA (2018b); ENISA (2019).

Beispielsweise wäre es in Bezug auf Bezahlverfahren in einem E-Commerce-Dienst verbraucherfreundlich und sinnvoll, eine Reihe von unterstützten Verfahren zur freien Auswahl für die Nutzenden anzubieten und keines davon vorauszuwählen, selbst wenn darunter eines als objektiv am datenschutzfreundlichsten zu identifizieren wäre.[82] Dies ergibt sich schon aus der Tatsache, dass üblicherweise die Nutzenden eigene Benutzerkonten bei den Bezahldienstleistern eingerichtet haben müssen und ein vorkonfiguriertes Verfahren nicht in jedem Fall den Nutzenden auch zur Verfügung steht. Besser wäre es, wenn bei einem Kauf die Nutzenden eine bewusste Entscheidung darüber treffen müssten, welches Verfahren sie für diesen Fall präferieren. Dies kann sich auch je nach Produkt oder Anbieter unterscheiden.

Die Anforderung des Datenschutzes durch datenschutzfreundliche Voreinstellungen – Datenschutz „by Default“ – erscheint durch die Formulierung als sehr mächtig: Stets sollte also eine Verarbeitung (und ebenso eine Kundenbeziehung) auf Basis personenbezogener Daten maximal datenschutzfreundlich beginnen; wenn später die betroffene Person bereit ist, zu weiteren Zwecken zusätzliche personenbezogene Daten zu offenbaren oder in weitere Verarbeitungen einzuwilligen, kann dies geschehen. Allerdings deckt sich dies nicht mit der Praxis, in der zumindest einige der großen Anbieter ein datengieriges Verhalten an den Tag legen und demnach eher nach dem Motto „Datenabgreifen by Default“ verfahren wird.[83]

5 Ganzheitliche Betrachtungsweise: Bewusstsein über Spannungsfelder

So wie für spezifische datenschutzrechtliche Sachverhalte unterschiedliche grundrechtliche Interessen miteinander abgewogen werden, geschieht dies auch im Verhältnis des Datenschutzes zu anderen geschützten Interessen. Datenschutzrechtliche Erwägungen können hier dazu führen, dass andere rechtlich geschützte Ansprüche reduziert oder abgelehnt werden, genauso wie sie dazu führen können, dass die Konsequenzen in benachbarte Rechtsgebiete ausstrahlen. Auch Anforderungen, die nicht rechtlich im selben Maße festgeschrieben sind,

[82] Hansen (2013, S. 4).

[83] Forbrukerrdet (2018).

können eine Rolle spielen, wenn es um eine faire und verträgliche Gestaltung von Systemen geht. Dazu sollten sich sowohl die Verantwortlichen als auch die Hersteller oder Entwickler der Systeme die verschiedenen Anforderungen samt möglicher Interdependenzen und Auswirkungen bewusst machen, selbst wenn sie in der Praxis oft nicht expliziert werden. Eine datenschutzkonforme Verfahrensgestaltung muss nicht in einem unauflösbaren Widerspruch zu anderen wichtigen Erwägungen stehen, sondern häufig können Lösungen gefunden werden, die nicht nur sämtliche rechtlichen Bedingungen, sondern auch die verschiedenen zusätzlichen Anforderungen in ausreichendem Maße berücksichtigen.[84]

Neben den bekannten und immer wieder genannten vermeintlichen Gegensätzen „Datenschutz und Sicherheit", „Datenschutz und Freiheit" und „Datenschutz und Nutzbarkeit" bestehen beispielsweise Spannungsfelder in Bezug auf Informationsfreiheit, Umweltschutz, Datenzugang, Wirtschaftlichkeit und Kartellrecht. Auf diese Spannungsfelder soll im Folgenden das Augenmerk gelenkt werden.

5.1 Informationsfreiheit

Ein Bereich der häufig im Zusammenhang mit dem Datenschutzrecht genannt wird und in der behördlichen Zuständigkeit mit ihm zusammenfällt, ist das Informationsfreiheitsrecht. Nur im ersten Moment stehen beide Rechtsgebiete in einem Konkurrenzverhältnis, denn im Kern geht es um Ansprüche gegenüber Organisationen, Datenschutz auf der einen Seite und Informationszugang zu behördlichen Informationen auf der anderen Seite. Am Beispiel der Informationsfreiheit lässt sich aber auch zeigen, dass durch eine optimierte Verfahrensplanung und –gestaltung ein sinnvoller Ausgleich zwischen kollidierenden Interessen stattfinden kann. Denn gerade dort, wo aus datenschutzrechtlicher Sicht eine umfassende Betrachtung der Risiken stattfindet, kann auch der Aspekt der Informationsfreiheit bereits im Stadium der Verfahrensplanung Berücksichtigung finden. Das schließt einerseits ein, dass entsprechende Voraussetzungen und der Ablauf etwaiger Anfragen zur besseren Auffindbarkeit bereits dann eingeplant werden, wenn behördliche Informationen angelegt werden und andererseits eine Einbeziehung der betroffenen Personen stattfindet. Konkret bedeutet das, dass bei der Planung der Verarbeitungsverfahren hinsichtlich der erhobenen Daten eine

[84] Hansen und Bremert (2020a, b).

Relevanzprüfung für Sachverhalte im Bereich der Informationsfreiheit stattzufinden hat. Hier ist zu bestimmen, ob Daten abstrakt Gegenstand einer Anfrage nach Informationsfreiheitsgesetz fallen können, ob einer Herausgabe dieser Daten etwaige Rechte Dritter entgegenstehen (also im Falle personenbezogener Daten, die Rechte der betroffenen Personen) und wie das Ergebnis einer Interessenabwägung aussehen könnte. Das kann im nächsten Schritt dazu führen, dass für komplexere Informationen bereits im Zeitpunkt der Erhebung Metadaten angelegt werden, um im Falle einer Anfrage nach Informationsfreiheitsgesetz eine zügige Schwärzung der Unterlagen vornehmen zu können. Hierbei kann also eine Schwärzung bereits vorab stattfinden, wenn es wahrscheinlich erscheint, dass später entsprechende Herausgabebegehren eintreffen werden. Das beinhaltet allerdings auch, dass betroffene Personen bereits im Zeitpunkt der Erhebung in die Entscheidung über das Maß der Schwärzung einbezogen werden und dies nicht erst im Zeitpunkt der Anfrage über die Herausgabe dieser Informationen geschehen muss. Das bietet sich insbesondere dann an, wenn andernfalls eine Verzögerung der Bearbeitung zu erwarten wäre, also etwa, weil die betroffenen Personen nicht mehr ohne Weiteres kontaktiert werden können oder sich der Sachbearbeiter der Anfrage erst wieder umfassender mit der Materie beschäftigen müsste.

5.2 Umweltschutz

Datenverarbeitung per Computer verbraucht Energie.[85] Eine Reduktion des Energieverbrauchs ist häufig nicht nur aus Umweltschutzgründen angestrebt, sondern wird auch untersucht, damit Akkus weniger häufig aufgeladen und mobile Systeme nicht mit großen oder schweren Akkus ausgestattet werden müssen. Datenschutzfunktionalität wie Verschlüsselung erhöht den Energieverbrauch.[86] Auch datenschutzfreundliche Konzepte, die weitere technische Komponenten oder zusätzliche elektronische Kommunikation erfordern, um auf diese Weise als Treuhänder oder im Sinne einer Abschottung eine Vertraulichkeit oder Nichtverkettung von personenbezogenen Daten gewährleisten können, führen zu einem Mehr an Energieverbrauch.

Es gibt aber auch Effekte der Verringerung des Energieverbrauchs. Das Umsetzen der Datenschutzgrundsätze wie Datenminimierung und Speicherbegrenzung kann ebenso wie das Prinzip des Datenschutzes „by Default“ im

[85] Bender, Gebru u. a. (2021).

[86] Potlapally, Ravi u. a. (2003).

Vergleich zur heutigen Praxis eine Reduzierung des Energieverbrauchs erzielen. Auch die nutzerseitige – und damit potenziell besser kontrollierbare – Datenverarbeitung im Endgerät spart Energie im Vergleich zu Cloud-Lösungen, die mit einer dauerhaften elektronischen Kommunikation einhergehen. Virtualisierung und Lastverteilung können zu einer ressourcenschonenden Technikinfrastruktur beitragen. Hier kann eine sorgfältige Konzeption und Planung der Datenverarbeitung, die ohnehin aus Datenschutzsicht notwendig ist, auch zu mehr Ressourcenbewusstsein führen.

Dieser adaptive Ansatz kann selbst beim Vernichten von mehr oder weniger vertraulichen Papierunterlagen eine Rolle spielen. Denn die Recyclingfähigkeit des Schredderguts ist eingeschränkt, wenn die Papierfasern zu klein gehäckselt werden. Dies spricht dafür, dass man den Hochsicherheitsschredder nicht für jeglichen Papiermüll verwendet, sondern risikoadäquat prüft, welche Art der Vernichtung gewählt werden soll.

5.3 Datenzugang

In zahlreichen Anwendungen fallen Daten an, für die sich die Frage stellt, inwieweit sie von wem zu weiteren Zwecken ausgewertet werden dürfen. Beispielsweise könnte man sich in einer datenbasierten Smart City oder für Internet-of-Things (IoT)-Anwendungen vorstellen, dass die entstehenden Daten verwendet würden, um Verfahren zum Nutzen des Gemeinwohls zu optimieren, die Planung der Infrastruktur zu verbessern, die Wissenschaft teilhaben zu lassen oder Start-ups die Daten für neue Geschäftsmodelle anzubieten. Nicht jede datenschutzgerechte Lösung ist aber gleichermaßen für die Bereitstellung der Daten für andere geeignet. Dies sieht man beispielsweise in Szenarien, in denen große Anbieter Daten ihrer Kundinnen und Kunden – Privatpersonen oder auch andere Unternehmen, personenbezogene oder nicht-personenbezogene Daten – sammeln und auf Basis der bestehenden Rechtsgrundlagen im Einklang mit den Anforderungen der Datenschutz-Grundverordnung an den Verantwortlichen weiterverwenden. Es gibt hier jedoch Bedenken von unerwünschten Monopolisierungen und Innovationshindernissen, wenn kein fairer Zugang zu solchen „Datenschätzen“ gewährt wird.

So problematisiert die Bundesfachgruppe Freie Werkstätten des Deutschen Kfz-Gewerbes, dass die bisherigen Konzepte der Autohersteller, die aus den zunehmend vernetzten Fahrzeugen Daten erhalten, den Werkstätten keinen

fairen Zugang zu den Daten bieten.[87] Ähnliches kritisieren die Versicherungen, die ihre Angebote auf Autofahrerinnen und –fahrer erstrecken. Die Datenethikkommission hat sich dieses Problems angenommen und Vorschläge für einen Interessenausgleich unterbreitet, der die Interessen aller – selbstverständlich auch der betroffenen Personen – berücksichtigen muss.[88] Dies kann bedeuten, nicht auf eine abgesicherte Zentralspeicherung bei einem einzigen Verantwortlichen zu setzen, sondern mit rechtlichen, technischen und organisatorischen Maßnahmen ein ebenfalls datenschutzkonformes föderiertes System zu entwickeln, in dem beispielsweise mit der Hilfe von Treuhändern die definierten Regeln implementiert und durchgesetzt werden können.

5.4 Wirtschaftlichkeit

Datenschutzgerechte Gestaltung verringert nicht nur das Risiko, dass die Rechte und Freiheiten natürlicher Personen verletzt werden, sondern hat auch den Effekt, dass der Verantwortliche seine Datenschutzpflichten leichter erfüllen kann. Finanzielle Schäden können dem Unternehmen durch Bußgelder der Datenschutzaufsichtsbehörde, Schadensersatzforderungen von betroffenen Personen oder Abmahnungen von datenschutzwidrigem Verhalten drohen. Für die meisten noch wichtiger ist aber, dass das Vertrauen der Kunden oder Kooperationspartner nicht durch Datenpannen, negative Schlagzeilen oder Shitstorms in den sozialen Medien gestört wird und mühsam wiederaufgebaut werden muss. Der Schutz der personenbezogenen Daten ist laut einer Umfrage in sämtlichen Märkten das zweitwichtigste Auswahlkriterium nach der Qualität von Produkten und Dienstleistungen.[89]

5.5 Kartellrecht

Ein weiterer Aspekt sind die kartellrechtlichen Auswirkungen datenschutzrechtlicher Sachverhalte. Dass das für kartellrechtliche Maßnahmen gegen miss-

[87] https://www.kfzgewerbe.de/presse/pressemeldungen/freie-werkstaetten-fordern-fairen-zugang-zu-daten.html.

[88] Datenethikkommission (2019).

[89] The Harris Poll, IBM Cybersecurity and Privacy Research, 13.04.2018, S. 13, abrufbar unter: http://newsroom.ibm.com/Cybersecurity-and-Privacy-Research.

bräuchliches Verhalten marktbeherrschender Unternehmen gilt, hat der BGH jüngst in seiner Facebook-Entscheidung dargelegt[90], womit vermutlich auch der Streit zur Anwendbarkeit lauterkeitsrechtlicher Normen neben datenschutzrechtlichen Regelungen entschieden wurde.

Die möglichen Probleme erschöpfen sich im Zusammenhang mit dem Kartellrecht aber nicht nur in missbräuchlichem Verhalten, sondern stellen sich schon im Stadium der Technikgestaltung, so ist für den Bereich der Missbrauchskontrolle denkbar, dass etwa marktbeherrschende Stellungen von Anbietern dadurch entstehen, dass Zugangshindernisse gerade durch Technikgestaltung geschaffen werden. Der Umstand ist besonders relevant, wenn die öffentliche Hand Kooperationen eingeht oder auf Produkte und/oder Leistungen setzt und dadurch den Wettbewerb im konkreten Bereich faktisch entscheidet. Hier kann, gerade in einem Bereich, in dem es um hoheitliche Aufgabenerfüllung auf Grundlage dieser Kooperationen, Produkte und Leistungen angeht, der Wettbewerb auf dem relevanten Markt oder angrenzenden Märkten praktisch ausgeschaltet werden. Daher müssen auch diese Auswirkungen von vornherein berücksichtigt werden und es muss sichergestellt werden, dass nicht nur der Wettbewerb nicht unzulässigerweise beschränkt, sondern auch die (zukünftige) Entwicklung datenschutzfreundlicherer Produkte und Leistungen auf dem relevanten Markt nicht verhindert wird.

5.6 Allgemeines Zivilrecht, Gewährleistung

Ein weiterer Bereich, in dem Risikoerwägungen in Zukunft eine größere Rolle spielen könnten, ist das Zivilrecht bzw. spezieller das Kaufrecht. Hier stellt sich in der Praxis oft die Frage, ob ein Kaufgegenstand frei von Sachmängeln ist. Wenn die Parteien keine Individualvereinbarung über die Beschaffenheit des Kaufgegenstandes getroffen haben, dann ist diese Frage am Gesetz zu beantworten. In § 434 S. 2 2 BGB wird dafür entweder auf die Geeignetheit für die nach dem Vertrag vorausgesetzte Verwendung (Nr. 1) oder auf die Eignung für die gewöhnliche Verwendung und einer Beschaffenheit, die bei Sachen gleicher Art üblich ist und die der Käufer nach der Art der Sache erwarten kann (Nr. 2) abgestellt. Im Falle von neuen Technologien dürfte in diesem Zusammenhang auch die Situation auftreten, dass neue Technologien nicht nur mit gewünschten Effekten einhergehen, sondern womöglich auch Angreifern neue Angriffsszenarien öffnen. Hier würde sich z. B. die Frage stellen, ob bauartbedingte Angriffsvektoren bereits einen Sachmangel

[90] BGH, Beschluss vom 23.06.2020 – KVR 69/19 („Facebook“).

implizieren, oder dies nur bei besonders gefahrengeneigter Nutzung und insoweit besonders hoher Schutzbedürftigkeit des Käufers (die dem Verkäufer auch bekannt sein muss) angenommen werden kann. Jedenfalls ohne entsprechende individuelle Vereinbarungen, wird man aktuell wohl zu dem Ergebnis kommen müssen, dass, sofern der Verkäufer oder der Hersteller (in dem Verkäufer zurechenbarer Weise[91]) nicht gerade mit datenschutzfreundlicher Technikgestaltung werben, eine Kundenerwartung im Sinne einer Eignung zur gewöhnlichen Verwendung beim Käufer nicht geweckt werden kann, wenn es sich nicht schon aus den Besonderheiten des Kaufgegenstandes ergibt. Aber auch diese Frage lässt sich aus Herstellersicht bereits im Stadium der Konzeption der Datenverarbeitung von hergestellten Produkten berücksichtigen. Damit können spezifische Angriffsszenarien jedenfalls beim Verkauf von Produkten beachtet werden, wenn der Käufer im konkreten Fall aus Hersteller- oder Verkäufersicht erkennbar aufgrund seiner individuellen Umstände gefährdet erscheint.

Eine andere Frage stellt sich im Falle von IoT-Geräten, also Hardware die jedenfalls mittelbar an das Internet angeschlossen ist. In diesen Geräten ist häufig ein kleiner aber vollständiger Computer integriert, auf dem ein Betriebssystem läuft. Die Software kann dabei im Laufe der Zeit Sicherheitslücken aufweisen, die meist nur durch entsprechende Updates des Hardware-Herstellers geschlossen werden können. Die Hersteller wiederum haben im Anschluss an den Verkauf häufig allerdings ein geringes Interesse, die Software der verwendeten Hardware noch über Jahre aktuell zu halten. Hier würde sich ebenfalls die Frage stellen, ob eine entsprechende Einstellung der Software-Updates durch den Hersteller Auswirkungen auf die Mangelhaftigkeit der Hardware haben könnten und dies zu Ersatzansprüchen des Kunden führen könnte und inwieweit entsprechende Risiken der Kunden, die aus dem Betrieb ungeschützter Hardware resultieren, durch den Hersteller zu berücksichtigen sind.

5.7 Berücksichtigung von Risiken bei Gesetzesvorhaben

Eine ganzheitliche Berücksichtigung wird auch bei dem Ansatz der Überwachungs-Gesamtrechnung gefordert. Dabei sollen Risiken staatlicher Überwachung über die individuellen Auswirkungen einer konkreten Maßnahmen hinaus Berücksichtigung finden und so die Auswirkungen der Gesamtheit staatlicher Maßnahmen auf die

[91] Saenger, in: Schulze (2019), § 434 Rn. 15 f.

individuelle Freiheitsausübung untersucht werden.[92] Dieser Ansatz wird mit dem zulässigen Maße an Gesamtüberwachung und der Verfassungsidentität begründet, die eine gesamte Erfassung der individuellen Freiheitsausübung verbiete.[93]

Als eine mögliche Operationalisierung der Überwachungs-Gesamtrechnung wird eine Gesetzes-Datenschutz-Folgenabschätzung vorgeschlagen.[94] Dabei könnten die möglichen Risiken für die Grundrechtsausübung nicht nur im Rahmen eines formalisierten Prozesses berücksichtigt werden, sondern der iterative Prozess der Datenschutz-Folgenabschätzung könnte auch im Rahmen von späteren Gesetzes-Evaluationen Anwendung finden.[95]

6 Fazit und Schlussfolgerungen

Systemgestaltung hat einen erheblichen Einfluss darauf, wie die Verarbeitung von Daten geschieht und ob die in der EU-Grundrechte-Charta festgelegten Rechte und Freiheiten auch in unserer zunehmend digitalisierten Gesellschaft gewährleistet werden. Hier gibt es keinen Universalansatz, der die Grundrechte technisch garantieren kann, und es wäre auch verfehlt, anzunehmen, dass „One size fits all" erfolgversprechend wäre. Maßstab für einen angemessenen Datenschutz und Privatheitsschutz ist das Risiko für die Rechte und Freiheiten.

Oft wurde nach Inkrafttreten der DSGVO durch Verantwortliche Kritik am risikobasierten Ansatz geäußert: Die Risikoerkennung sei für sie nicht handhabbar und eine umfassende Bewertung, wie die DSGVO sie vorsieht, sei ihnen nicht zuzumuten. Verantwortliche werden die Risikoidentifikation und Risikobewertung nur dann durchführen können, wenn sie die sonstigen Anforderungen der DSGVO an die Ausgestaltung und Dokumentation von Verarbeitungsverfahren einhalten. Das bedeutet nicht nur, dass neu zu implementierte Verfahren diesen Maßstäben gerecht werden müssen, auch alte Verarbeitungsverfahren müssen durch die Verantwortlichen auf die neue Rechtslage angepasst werden, wenn sie auch heute noch – mit Geltung der DSGVO – weiter betrieben werden sollen.

Probleme im Umgang mit den neuen Anforderungen der DSGVO hängen nach Erfahrung des Autorenteams häufig damit zusammen, dass Verantwortliche nicht

[92] Roßnagel (2010).

[93] BVerfG, Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08, Rn. 218.

[94] Bieker, Bremert u. a. (2018a, b, S. 148); Bieker und Bremert (2019, S. 35).

[95] Bremert (2021).

das Wissen über die eigene Datenverarbeitung haben, das für eine richtige Einschätzung notwendig wäre. Problematisch ist dies besonders dann, wenn in der Datenverarbeitung Software- oder Hardware-Komponenten, über die dem Verantwortlichen keine ausreichenden Kenntnisse vorliegen, zum Einsatz kommen. In solchen Fällen kann der Verantwortliche oft eine (unbefugte) Offenbarung der personenbezogenen Daten an Dritte nicht ausschließen[96], z. B. wenn derartige Komponenten Mängel in ihrer Funktionsweise aufweisen oder sogar über undokumentierte Funktionen verfügen, die zu einem Datenabfluss führen können[97].

Die datenschutzrechtlichen Anforderungen treffen jeden Verantwortlichen, sodass eine übergreifende und lückenlose Compliance für jede Verarbeitung personenbezogener Daten einzufordern ist, auch bei der Auswahl von Produkten oder Dienstleistern. Wirksame Informationssicherheitsmaßnahmen sind zudem auch aufgrund der eigenen Organisationsinteressen – z. B. zum Schutz von Betriebs- und Geschäftsgeheimnissen – nötig. Es zeigt sich jedoch, dass die Verantwortlichen Schwierigkeiten haben können, wenn Hersteller von Produkten, Diensten und Anwendungen sie nicht in ihrer Rechenschaftspflicht unterstützen, z. B. durch Bereitstellung der notwendigen Dokumentation, oder – noch schlimmer – eine Konformität mit den in Europa geltenden datenschutzrechtlichen Anforderungen womöglich gar nicht erst anstreben geschweige denn erfüllen. Faktisch besteht in vielen Fällen eine Abhängigkeit von den Herstellern: Selbst wenn ein Wechsel der Anbieter durch ein Herauslösen der personenbezogenen Daten und das Bereitstellen alternativer Angebote technisch möglich ist, verursacht dies in den meisten Fällen einen erheblichen Aufwand, zumal die Alternativen meist nicht identisch in Funktionalität und Bedienbarkeit sind.

Dies zeigte sich im Jahr 2020 in Bezug auf die Entscheidung des Europäischen Gerichtshofs (EuGH) zum „Privacy Shield“, auf den vielfach der grenzüberschreitende Transfer personenbezogener Daten in die USA gestützt wurde. Nachdem der EuGH mit Urteil vom 16. Juli 2020 (Rechtssache C-311/18) den „Privacy Shield“ (Beschluss 2016/1250) der Europäischen Kommission zur Übermittlung personenbezogener Daten in die USA für unwirksam erklärt hatte,[98] erhob sich ein massives Drängen der Industrieverbände in Europa auf

[96] Vgl. im Falle von Facebook-Apps: Feiner (2019).

[97] Wagner und Salzmann (2019); Lischka, Hartmann u. a. (2012, S. 9 ff.).

[98] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2020).

neue Verhandlungen der Europäischen Kommission mit den USA und auf ein Moratorium der Datenschutzaufsicht.[99] Dies ist deswegen erstaunlich, weil zumindest den kundigen Juristinnen und Juristen der Industrieverbände schon viele Monate oder sogar Jahre vor dem Urteil klar war (oder hätte klar sein müssen), dass der „Privacy Shield" als Rechtslage infrage stand und nicht als stabiles Fundament taugte. Zeit für Anpassungen hätte es gegeben, aber die Verantwortlichen scheuten die fristgerechten Änderungen, die bei ihnen zu Aufwänden, Kosten oder anderen Unbequemlichkeiten geführt hätten.

Trotz einiger Hemmnisse in der Umsetzung ist das Prinzip, durch Systemgestaltung für eine Verbesserung von Datenschutz und Privatheitsschutz zu sorgen, richtig und erfolgversprechend. Die Datenschutz-Grundverordnung hat dies nun stärker ins Bewusstsein von Verantwortlichen und Dienstleistern gerückt, sodass nach vielen Jahren und Jahrzehnten Fortschritte zu erwarten sind. Eng damit verbunden ist der Umgang mit dem Risikobegriff, insbesondere bei neuen Technologien mit personenbezogener Datenverarbeitung, bei deren Einführung die Notwendigkeit einer Datenschutz-Folgenabschätzung zu prüfen ist. Wünschenswert – oder sogar notwendig angesichts des Hypes um Algorithmen bis hin zu „Künstlicher Intelligenz" – ist die Betrachtung der Risiken für Rechte und Freiheiten von Individuen ebenso wie für unsere demokratische Gesellschaft auch für solche technischen Systeme, in denen der Personenbezug keine Rolle spielt. Generell sind Folgenabschätzungen angeraten, die zu adäquaten Maßnahmen einer Risikoeindämmung und zu einer fairen und am Gemeinwohl orientierten Gestaltung der Digitalisierung führen, die eine zukunftsfähige und nachhaltige Entwicklung unserer Gesellschaft unterstützt.

Literatur

AK Technik der Datenschutzbeauftragten des Bundes und der Länder. (1997a). *Arbeitspapier „Datenschutzfreundliche Technologien"*. AK Technik der Datenschutzbeauftragten des Bundes und der Länder.

AK Technik der Datenschutzbeauftragten des Bundes und der Länder. (1997b). *Arbeitspapier „Datenschutzfreundliche Technologien in der Telekommunikation"*. AK Technik der Datenschutzbeauftragten des Bundes und der Länder.

[99] https://www.bitkom.org/sites/default/files/2020-07/draft-joint-industry-statement-on-privacy-shield-and-sccs-july-28-2020.pdf.

Alexy, R. (2003). Die Gewichtsformel. In J. Jickeli, P. Kreutzer & D. Reuter (Hrsg.), *Gedächtnisschrift für Jürgen Sonnenschein* (S. 771–792). DeGruyter.

Art.-29-Datenschutzgruppe. (2004). *Stellungnahme 10/2004 zu einheitlicheren Bestimmungen über Informationspflichten, 04/DE WP 100.* Brüssel.

Art.-29-Datenschutzgruppe. (2014). *Stellungnahme 5/2014 zu Anonymisierungstechniken, 14/DE WP 216.* Brüssel.

Bender, E., Gebru, T., McMillan-Major, A., & Shmitchell, S. (2021). On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? *Proceedings of the 2021 ACM Conference on Fairness, Transparency and Accountability*. https://doi.org/10.1145/3442188.3445922.

Bieker, F. (2017). Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell. *Datenschutz und Datensicherheit, 41,* 27–31.

Bieker, F., & Bremert, B. (2019). Rote Linien im Sand, bei Sturm: Die Überwachungs-Gesamtrechnung. *FIfF-Kommunikation, 4*(19), 34.

Bieker, F., & Bremert, B. (2020). Identifizierung von Risiken für die Grundrechte von Individuen. *Zeitschrift für Datenschutz, 10,* 7–14.

Bieker, F., Bremert, B., & Hagendorff, T. (2018a). Die Überwachungs-Gesamtrechnung, oder: Es kann nicht sein, was nicht sein darf. In A. Roßnagel, M. Friedewald & M. Hansen (Hrsg.), *Die Fortentwicklung des Datenschutzes* (S. 140–150). Springer.

Bieker, F., Bremert, B., & Hansen, M. (2018b). Verantwortlichkeit und Einsatz von Algorithmen bei öffentlichen Stellen. *Datenschutz und Datensicherheit, 42,* 608–612.

Bieker, F., & Hansen, M. (2017). Datenschutz „by Design" und „by Default" nach der neuen europäischen Datenschutz-Grundverordnung. *Recht der Datenverarbeitung, 33*, 165–170.

Bieker, F., Hansen, M., & Friedewald, M. (2016). Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung nach der neuen europäischen Datenschutz-Grundverordnung. *Recht der Datenverarbeitung, 32,* 188–197.

Bieker, F. (im Erscheinen). *The Right to Data Protection – Individual and Structural Dimensions of Data Protection in EU Law*. Asser Press/Springer.

Bremert, B. (2021). Stellungnahme im Rahmen der öffentlichen Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages am 22. Februar 2021, Ausschussdrucksache 19(4) 732 F, abrufbar unter: https://www.bundestag.de/resource/blob/823356/95ff16908f0b33b1d69a0697e5e77af7/ADrs-19-4-732-F-data.pdf.

Borking, J. (1996). Der Identity-Protector. *Datenschutz und Datensicherheit, 20,* 654.

Borking, J. (1998). Einsatz datenschutzfreundlicher Technologien. *Datenschutz und Datensicherheit, 22,* 636.

Cavoukian, A. (2011). *Privacy by Design – The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario, Canada. Originally published: August 2009. Revised: January 2011.

Chaum, D. (1985). Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM, 28,* 1030.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Métayer, D., Tirtea, R., & Schiffner, S. (2015). *Privacy and Data Protection by Design – from Policy to Engineering*. European Union Agency for Network and Information Security (ENISA). https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design. Zugegriffen: 8. Dez. 2021.

Datenethikkommission. (2019). *Gutachten der Datenethikkommission*. https://www.bmjv.de/DE/Themen/FokusThemen/Datenethikkommission/Datenethikkommission_node.html. Zugegriffen: 8. Dez. 2021.

Doty, N., & Gupta, M. (2013). Privacy Design Patterns and Anti-Patterns – Patterns Misapplied and Unintended Consequences. In *A Turn for the Worse: Trustbusters for User Interfaces Workshop, Symposium On Usable Privacy and Security (SOUPS) 2013*. http://cups.cs.cmu.edu/soups/2013/trustbusters2013/Privacy_Design_Patterns-Anti-patterns_Doty.pdf. Zugegriffen: 8. Dez. 2021.

Europäische Kommission. (2007). *Privacy Enhancing Technologies (PETs)*, MEMO/07/159. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_07_159. Zugegriffen: 2. Mai 2007.

European Data Protection Board. (2020). *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0*. abrufbar unter: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

European Union Agency for Network and Information Security (ENISA). (2015). *Readiness Analysis for the Adoption and Evolution of Privacy Enhancing Technologies, Methodology, Pilot Assessment, and Continuity Plan*. https://www.enisa.europa.eu/publications/pets. Zugegriffen: 8. Dez. 2021.

European Union Agency for Network and Information Security (ENISA). (2018a). *Recommendations on shaping technology according to GDPR provisions – An overview on data pseudonymisation*. https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions. Zugegriffen: 8. Dez. 2021.

European Union Agency for Network and Information Security (ENISA). (2018b). *Recommendations on shaping technology according to GDPR provisions – Exploring the notion of data protection by default*. https://www.enisa.europa.eu/publications/recommendations-on-shaping-technology-according-to-gdpr-provisions-part-2. Zugegriffen: 8. Dez. 2021.

European Union Agency for Cybersecurity (ENISA). (2019). *Pseudonymisation techniques and best practices – Recommendations on shaping technology according to data protection and privacy provisions*. https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices. Zugegriffen: 8. Dez. 2021.

European Union Agency for Cybersecurity (ENISA). (2021). *Data Pseudonymisation: Advanced Techniques & Use Cases – Technical analysis of cybersecurity measures in data protection and privacy*. https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases. Zugegriffen: 8. Dez. 2021.

Feiner, L. (2019). *Facebook reportedly gets deeply personal info, such as ovulation times and heart rate, from some apps, CNBC*. https://www.cnbc.com/2019/02/22/facebook-receives-personal-health-data-from-apps-wsj.html. Zugegriffen: 22. Febr. 2019.

Felber, W. (2020). Europäischer Datenschutz. In R. Schulze, A. Janssen, & S. Kadelbach (Hrsg.). *Europarecht – Handbuch für die deutsche Rechtspraxis* (S. 2561–2609) (4. Aufl.). Nomos.

Fischer-Hübner, S., & Berthold, S. (2017). Privacy Enhancing Technologies. In J. R. Vacca (Hrsg.). *Computer and information security Handbook* (S. 759–778). Morgan Kaufmann.

Flores, A. W., Bechtel, K., & Lowenkamp, C. T. (2016). False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks". *Federal Probation, 80*(2), 38–46.

Forbrukerrdet. (2018). *Deceived by Design – How tech companies use dark patterns to discourage us from exercising our rights to privacy*, Oslo, abrufbar unter: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

Friedewald, M., Bieker, F., Martin, N., Obersteller, H., Nebel, M., Rost, M., & Hansen, M. (2017). *Datenschutz-Folgenabschätzung: Ein Werkzeug für einen besseren Datenschutz* (3. Aufl.). Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. https://www.forum-privatheit.de/datenschutz-folgenabschaetzung/.

Guyan, K. (2022). *Queer Data – Using Gender, Sex and Sexuality Data for Action*. Bloomsburg Academic.

Hansen, M. (2013). Risk analysis of identity management approaches employing privacy protection goals. In S. Fischer-Hübner, E. de Leeuw & C. Mitchell (Hrsg.). *Policies and research in identity management. IDMAN 2013: Bd. 396. IFIP advances in information and communication technology*. Springer. https://doi.org/10.1007/978-3-642-37282-7_10.

Hansen, M., & Walczak, B. (2019). Pseudonymisierung à la DSGVO und verwandte Methoden. *Recht der Datenverarbeitung, 35*, 53–57.

Hansen, M., & Bremert, B. (2020a). Mehr (als) Datenschutz: Plädoyer für planvolles Vorgehen für Datenschutz by Design. *BvD News, 2*, 30–34.

Hansen, M., & Bremert, B. (2020b). Mit Tracing-Apps in eine Healthy New World. *Privacy in Germany, 5*, 141–145.

Hansen, M., Jensen, M., & Rost, M. (2015). Protection Goals for Privacy Engineering. In *Proceedings 2015 IEEE Security and Privacy Workshops (SPW 2015),* San Jose, Calif., 21 May 2015 (S. 159–166). IEEE Computer Society.

Hansen, M. (2021). Private Haushalte. In Hornung, G., & Schallbruch, M. (Hrsg.). *IT-Sicherheitsrecht*. Nomos. 620–644.

Hoepman, J.-H. (2014). Privacy design strategies. In N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, & T. Sans (Hrsg.). *ICT systems security and privacy protection. SEC 2014: Bd. 428. IFIP advances in information and communication technology* (S. 446–459). Springer. https://doi.org/10.1007/978-3-642-55415-5_38.

Hornung, G., & Schallbruch, M. (2021). *IT-Sicherheitsrecht*. Nomos.

Jarass, H. D. (2021). *Charta der Grundrechte der Europäischen Union* (4. Aufl.). Beck.

Karaboga, M., Masur, P., Matzner, T., Mothes, C., Nebel, M., Ochs, C., Schütz, P., & Simo Fhom, H. (2014). *Whitepaper Selbstdatenschutz*. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Karlsruhe: Fraunhofer ISI. https://www.forum-privatheit.de/download/selbstdatenschutz-2-auflage-2014/.

Kersten, J. (2017). Anonymität in der liberalen Demokratie. *Juristische Schulung, 2017,* 193–203.

Kingreen, T. (2016). Art. 8 GrCh. In Callies, C., & Ruffert, M. (Hrsg.). *EUV/AEUV – Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta* (6. Aufl.). Beck.

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder. (2016). *Das Standard-Datenschutzmodell: Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele, V.1.0 – Erprobungsfassung*.

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. (2018). *Kurzpapier Nr. 18: Risiko für Rechte und Freiheiten natürlicher Personen*. https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_18_Risiko.pdf.

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. (2020). *Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II") stärkt den Datenschutz für EU-Bürgerinnen und Bürger*, Pressemitteilung vom 28.07.2020. https://www.datenschutzkonferenz-online.de/media/pm/20200616_pm_schrems2.pdf.

Kühling, J., & Buchner, B. (Hrsg.). (2020). *DS-GVO BDSG* (3. Aufl.). Beck.

Lischka, B., Hartmann, M., Zypries, B. et al. (2012). *Kleine Anfrage von Abgeordneten der Fraktion der SPD zum „Einsatz der Quellen-Telekommunikationsüberwachung"*. BT-Drs, 17/11598, Berlin.

Lopez Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. (2019). 'Internet of Things': How Abuse is Getting Smarter. *Safe – The Domestic Abuse Quarterly 63*(6), 22–26.

Martin, N., Friedewald, M., Schiering, I., Mester, B., Hallinan, D., & Jensen, M. (2020). *Die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO: Ein Handbuch für die Praxis*. Fraunhofer Verlag.

Meyer, J., & Hölscheidt, S. (Hrsg.). (2019). *Charta der Grundrechte der Europäischen Union* (5. Aufl.). Nomos.

Müller, G., & Rannenberg, K. (1999). *Multilateral security in communications: Technology, infrastructure, economy*. Addison-Wesley.

Paal, B. P., & Pauly, D. A. (Hrsg.). (2018). *DS-GVO BDSG* (2. Aufl.). Beck.

Pfitzmann, A. (2006). Multilateral security: Enabling technologies and their evaluation. In G. Müller (Hrsg.). *Emerging Trends in Information and Communication Security. ETRICS 2006: Bd. 3995. Lecture notes in computer science* (S. 1–13). Springer. https://doi.org/10.1007/11766155_1.

Pfitzmann, B., Waidner, M., & Pfitzmann, A. (1990). Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. *Datenschutz und Datensicherheit, 14,* 243–253, 305–315.

Potlapally, N. R., Ravi, S., Raghunathan, A., & Jha, N. K. (2003). Analyzing the energy consumption of security protocols. *Proceedings ISLPED '03*, ACM.

Roßnagel, A. (2010). Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung. *Neue Juristische Wochenschrift, 63,* 1238.

Roßnagel, A. (Hrsg.). (2003). *Handbuch Datenschutzrecht*. Beck.

Roßnagel, A. (2019). Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht. *Neue Juristische Wochenschrift, 72,* 1.

Rost, M. (2018). Risiken im Datenschutz. *Vorgänge, 221*(222), 79–91.

Rost, M., & Pfitzmann, A. (2009). Datenschutz-Schutzziele – revisited. *Datenschutz und Datensicherheit, 33*(6), 353–358.

Schulze, R. (Hrsg.). (2019). *Handbuch Bürgerliches Gesetzbuch* (10. Aufl.). Nomos.

Schwartmann, R., & Weiß, S. (Hrsg.). (2017). *Whitepaper zur Pseudonymisierung der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2017 – Leitlinien für die rechtssichere Nutzung von Pseudonymisierungslösungen unter Berücksichtigung der Datenschutz-Grundverordnung – Digital Gipfel*. Version 1.0. https://www.gdd.de/downloads/whitepaper-zur-pseudonymisierung. Zugegriffen: 8. Dez. 2021.

Simitis, S., Hornung, G., & Spiecker gen. Döhmann, I. (Hrsg.). (2019). *Datenschutzrecht.* Nomos.

Taeger, J., & Gabel, D. (Hrsg.). (2019). *DSGVO BDSG* (3. Aufl.). Deutscher Fachverlag.

Tanczer, L., Lopez Neira, I., Parkin, S., Patel, T., & Danezis G. (2018). *Gender and IoT Research Report: The Rise of the Internet of Things and Implications for Technology-Facilitated Abuse*. London: STEaPP, PETRAS IoT Hub, 2018,3 f., abrufbar unter: https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf.

van Rossum, H., Gardeniers, H., Borking, J., Cavoukian, A., Brans, J., Muttupulle, N., & Magistrale, N. (1995). *Privacy-Enhancing Technologies: The Path to Anonymity*. Information and Privacy Commissioner / Ontario, Canada & Registratiekamer, The Netherlands, Den Haag.

Wagner, B., & Salzmann, S. (2019). IT-Sicherheit im Internet of Things: Überwachungspotenzial smarter Küchenhelfer. *ZD-Aktuell,* 06731.

Wybitul, T. (2020). Neue Urteile: Strafschadensersatz wegen DSGVO-Verstößen. *CR-Blog*. https://www.cr-online.de/blog/2020/10/24/neue-urteile-strafschadensersatz-wegen-dsgvo-verstoessen/. Zugegriffen: 24. Okt. 2020.

Marit Hansen ist Landesbeauftragte für Datenschutz Schleswig-Holstein und Leiterin des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein.

Felix Bieker ist juristischer Mitarbeiter beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein.

Benjamin Bremert ist Senior Compliance Manager bei der DZ HYP AG und war zuvor juristischer Mitarbeiter beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein.

Ausgesuchte Veröffentlichungen des „Forum Privatheit“

Bücher

Baumann, J., & Lamla, J. (Hrsg.). (2017). *Privacy Arena: Kontroversen um Privatheit im digitalen Zeitalter.* Kassel University Press.

Büttner, B., Geminn, C. L., Hagendorff, T., Lamla, J., Ledder, S., Ochs, C., & Pittroff, F. (2016). *Die Reterritorialisierung des Digitalen. Zur Reaktion nationaler Demokratie auf die Krise der Privatheit nach Snowden.* Kassel University Press.

Friedewald, M. (Hrsg.). (2018). *Privatheit und selbstbestimmtes Leben in der Digitalen Welt: Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes.* Springer.

Friedewald, M., Kreutzer, M., & Hansen, M. (Hrsg.). (2021). *Selbstbestimmung, Privatheit und Datenschutz: Gestaltungsoptionen für einen europäischen Weg.* Springer Vieweg.

Friedewald, M., Lamla, J., & Roßnagel, A. (Hrsg.). (2017). *Informationelle Selbstbestimmung im digitalen Wandel.* Springer Vieweg.

Hagendorff, T. (2017). *Das Ende der Informationskontrolle: Zur Nutzung digitaler Medien jenseits von Privatheit und Datenschutz.* Transcript.

Johannes, P. C., & Roßnagel, A. (2016). *Der Rechtsrahmen für einen Selbstschutz der Grundrechte in der Digitalen Welt.* Kassel University Press.

Nebel, M. (2021). *Persönlichkeitsschutz in Social Networks: Technische Unterstützung eines grundrechtskonformen Angebots von Social Networks.* Springer Vieweg.

Ochs, C., Friedewald, M., Hess, T., & Lamla, J. (Hrsg.). (2019). *Die Zukunft der Datenökonomie. Digitales Leben zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz.* Springer VS.

Roßnagel, A. (Hrsg.). (2017). *Europäische Datenschutz-Grundverordnung: Vorrang des Unionsrechts – Anwendbarkeit des nationalen Rechts.* Nomos.

Roßnagel, A. (Hrsg.). (2018). *Das neue Datenschutzrecht: Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze.* Nomos.

Roßnagel, A., & Friedewald, M. (Hrsg.). (2021). *Die Zukunft von Privatheit und Selbstbestimmung: Analysen und Empfehlungen zum Schutz der Grundrechte in der digitalen Welt.* Springer Vieweg.

A. Roßnagel und M. Friedewald (Hrsg.), *Die Zukunft von Privatheit und Selbstbestimmung,* DuD-Fachbeiträge,
https://doi.org/10.1007/978-3-658-35263-9

Roßnagel, A., Friedewald, M., & Hansen, M. (Hrsg.). (2018). *Die Fortentwicklung des Datenschutzes: Zwischen Systemgestaltung und Selbstregulierung.* Springer Vieweg.
Roßnagel, A., & Geminn, C. (2020). *Datenschutz-Grundverordnung verbessern: Änderungsvorschläge aus Verbrauchersicht.* Nomos.
Stapf, I., Ammicht Quinn, R., Friedewald, M., Heesen, J., & Krämer, N. C. (Hrsg.). (2021). *Aufwachsen in überwachten Umgebungen: Interdisziplinäre Positionen zur Privatheit und Datenschutz in Kindheit und Jugend.* Nomos.

White und Policy Paper, Arbeitsberichte

Diese Publikationen stehen unter https://www.forum-privatheit.de zum Download zur Verfügung.

2022

- Mehr Fortschritt wagen – durch Stärkung des Datenschutzes. Vorschläge zur Ausgestaltung des Koalitionsvertrags
- Data Protection Authorities under the EU General Data Protection Regulation: A new global benchmark?

2021

- Datenschutz in der Blockchain: Diskussion der Herausforderungen und Lösungsansätze auf Basis der Blockchain-Konsultation der Bundesregierung

2020

- Einwilligung: Möglichkeiten und Fallstricke aus der Konsumentenperspektive
- Privatheit und Kinderrechte
- Risiken Künstlicher Intelligenz für die menschliche Selbstbestimmung

2019

- Evaluation der Datenschutz-Grundverordnung
- Das Sanktionsregime der Datenschutz-Grundverordnung: Auswirkungen auf Unternehmen und Datenschutzaufsichtsbehörden

2018

- Tracking: Beschreibung und Bewertung neuer Methoden
- Desinformation aufdecken und bekämpfen: Handlungsempfehlungen
- Nationale Implementierung der Datenschutz-Grundverordnung: Herausforderungen – Ansätze – Strategien
- Das Netzwerkdurchsetzungsgesetz
- Datenschutz stärken, Innovationen ermöglichen: Wie man den Koalitionsvertrag ausgestalten sollte

2017

- Privatheit in öffentlichen WLANs: Spannungsverhältnisse zwischen ökonomischen Interessen, gesellschaftlicher Verantwortung und rechtlichen Anforderungen
- Datenschutz-Folgenabschätzung – Ein Werkzeug für einen besseren Datenschutz
- Datensparsamkeit oder Datenreichtum? Zur neuen politischen Diskussion über den datenschutzrechtlichen Grundsatz der Datensparsamkeit
- Fake News
- Privacy attitudes, perceptions, and behaviors of the German population

2016

- Die neue Datenschutz-Grundverordnung: Ist das Datenschutzrecht nun für heutige Herausforderungen gerüstet?
- Privatheitskompetenz: Das Wissen der Bürger über Privatheit und Datenschutz
- Privatheit und informationelle Selbstbestimmung: Trendmonitor zu den Einstellungen, Meinungen und Perspektiven der Deutschen
- Smart-TV und Privatheit: Bedrohungspotenziale und Handlungsmöglichkeiten

2015

- Das versteckte Internet: Zu Hause – Im Auto – am Körper
- Privatheit und Datenflut in der neuen Arbeitswelt – Chancen und Risiken einer erhöhten Transparenz
- Wertschöpfung in Datenmärkten: Eine explorative Untersuchung am Beispiel des deutschen Marktes für persönliche Daten

- Privatheit in den Medien: Berichterstattung zum Thema Privatheit und Internet in deutschen Medien
- Akteure, Interessenlagen und Regulierungspraxis im Datenschutz: Eine politikwissenschaftliche Perspektive

2014

- Selbstdatenschutz