DuD-Fachbeiträge

RESEARCH

Michael Friedewald · Michael Kreutzer
Marit Hansen *Hrsg.*

Selbstbestimmung, Privatheit und Datenschutz

Gestaltungsoptionen für einen europäischen Weg

OPEN ACCESS

DuD
Datenschutz und Datensicherheit

Springer Vieweg

DuD-Fachbeiträge

Reihe herausgegeben von

Gerrit Hornung, Institut für Wirtschaftsrecht, Universität Kassel, Kassel, Hessen, Deutschland

Helmut Reimer, Erfurt, Thüringen, Deutschland

Karl Rihaczek, Bad Homburg vor der Höhe, Deutschland

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

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.

Michael Friedewald · Michael Kreutzer · Marit Hansen
(Hrsg.)

Selbstbestimmung, Privatheit und Datenschutz

Gestaltungsoptionen für einen europäischen Weg

Springer Vieweg

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

Michael Kreutzer
Fraunhofer-Institut für Sichere Informationstechnologie
Darmstadt, Deutschland

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

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

ISSN 2512-6997 ISSN 2512-7004 (electronic)
DuD-Fachbeiträge
ISBN 978-3-658-33305-8 ISBN 978-3-658-33306-5 (eBook)
https://doi.org/10.1007/978-3-658-33306-5

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

Planung/Lektorat: Carina Reibold
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

Vorwort

Um im interdisziplinären Dialog die technischen, wirtschaftlichen und politischen Gestaltungsmöglichkeiten für Selbstbestimmung und Privatheit in einer zunehmend von Digitalisierung und Datafizierung geprägten Gesellschaft auszuloten und zu diskutieren, veranstaltete das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte „Forum Privatheit und selbstbestimmtes Leben in der Digitalen Welt“ (https://www.forum-privatheit.de) am 12. und 13. November 2020 seine interdisziplinäre Jahrestagung zum Schwerpunktthema „Selbstbestimmung und Privatheit – Gestaltungsoptionen für einen europäischen Weg“. Ursprünglich war geplant, zum Abschluss der zweiten Förderperiode des „Forum Privatheit“ eine große Veranstaltung in Berlin auszurichten. Infolge der SARS-CoV-2-Pandemie musste diese letztlich als Online-Veranstaltung durchgeführt werden. Aufgrund der professionellen technischen Organisation und einer niedrig gehaltenen Zugangsschwelle für Interessierte lag die Zahl der Teilnehmer sogar über den Werten der vorherigen Jahrestagungen. Erfreulicherweise blieb die Zahl der online zugeschalteten und auch aktiv an den Diskussionen teilnehmenden Personen an beiden Tagen konstant hoch. Der vorliegende Band präsentiert ausgewählte Beiträge und reflektiert auch die dort angestoßenen Diskussionen.

Das „Forum Privatheit“ arbeitet seit nunmehr sieben Jahren – ausgehend von technischen, juristischen, ökonomischen sowie geistes- und gesellschaftswissenschaftlichen Ansätzen – an einem interdisziplinär fundierten, zeitgemäßen Verständnis von Privatheit und Selbstbestimmung. Hieran anknüpfend werden Konzepte zur (Neu-)Bestimmung und Gewährleistung der informationellen Selbstbestimmung und des Privaten in der digitalen Welt erstellt. Es versteht sich über seine Kerndisziplinen hinaus als eine Plattform für den fachlichen Austausch und erarbeitet Orientierungswissen für den öffentlichen Diskurs in Form

wissenschaftlicher Publikationen, Tagungen, White-Papers und Policy-Papers. Mitglieder des „Forum Privatheit“ sind

- das Fraunhofer-Institut für System- und Innovationsforschung (ISI), Karlsruhe,
- das Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt,
- das Fachgebiet Soziologische Theorie an der Universität Kassel,
- die Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel,
- das Fachgebiet Sozialpsychologie der Universität Duisburg-Essen,
- das Internationale Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen,
- das Institut für Wirtschaftsinformatik und neue Medien der Ludwig-Maximilians-Universität München und
- das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel.

Die inhaltliche Ausrichtung und Organisation der Konferenz standen in der Verantwortung der Fraunhofer-Institute für System- und Innovationsforschung ISI und für Sichere Informationstechnologie SIT, sowie des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. Als Herausgeber:innen freuen wir uns stellvertretend für das „Forum Privatheit“ insgesamt, nun diesen Konferenzband präsentieren zu können. Wir danken insbesondere den Autorinnen für die Beisteuerung der jeweiligen Fachartikel. Ebenso zum Dank verpflichtet sind wir allen Beteiligten am „Forum Privatheit“. Die Konferenz „Selbstbestimmung und Privatheit – Gestaltungsoptionen für einen europäischen Weg“ wäre ohne die vielfältige Unterstützung durch das interdisziplinäre Kollegium nicht möglich gewesen. Wir danken insbesondere all jenen, die organisatorisch oder inhaltlich an der Durchführung der Konferenz und ihrer verschiedenen Sektionen mitgewirkt haben, darunter vor allem Johanna Mittermeier (Fraunhofer SIT) und Susanne Ruhm (Fraunhofer ISI). Bei Barbara Ferrarese bedanken wir uns für ihre hervorragende Öffentlichkeitsarbeit sowie bei Uwe Jean Heuser (Die ZEIT) für die professionelle und fachkundige Moderation.

Dieser Tagungsband wäre nicht ohne tatkräftige Unterstützung bei der Manuskriptbearbeitung und -korrektur zustande gekommen. Insbesondere möchten wir uns sehr herzlich bei Johanna Mittermeier (Fraunhofer SIT) für ihre koordinierende Tätigkeit bei der Erstellung des Tagungsbandes bedanken. Wir danken Andreas Baur, Tamer Bile, Benjamin Bremert, Barbara Büttner, Christian Geminn, Murat Karaboga, Judith Meinert, Carsten Ochs, Pauline Scheidemann,

Linda Schreiber, Ingrid Stapf und Mena Teebken aus dem Team des „Forum Privatheit“ für die kritische Begutachtung der eingereichten Beiträge. Für die allfälligen Formatierungs- und Korrekturarbeiten danken wir Wilma Gießen (Fraunhofer ISI).

Schließlich möchten wir uns auch bei Frau Dr. Heike Prasse und Herrn Ingo Höllein vom Bundesministerium für Bildung und Forschung (BMBF) bedanken, das den Projektverbund unterstützt, sowie bei Dr. Jan-Ole Malchow, der für den Projektträger VDI/VDE-IT die Forschungsarbeiten des „Forum Privatheit“, die Durchführung der Konferenz und das Erscheinen des Bandes begleitet hat.

Karlsruhe — Michael Friedewald
Darmstadt — Michael Kreutzer
Kiel — Marit Hansen
im Januar 2021

Inhaltsverzeichnis

Herausgeber- und Autorenverzeichnis

Über die Herausgeber

Dr. Michael Friedewald leitet am Fraunhofer Institut für System- und Innovationsforschung ISI in Karlsruhe das Geschäftsfeld „Informations- und Kommunikationstechnik“. Er studierte Elektrotechnik, Wirtschaftswissenschaften und Technikgeschichte an der Rheinisch-Westfälischen Technischen Hochschule Aachen. Er beschäftigt sich mit Voraussetzungen, Prozessen und Folgen der Digitalisierung. Er ist Koordinator des vom BMBF geförderten Projekts „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt“.

Dr. Michael Kreutzer forscht und publiziert seit mehr als 20 Jahren zu Fragestellungen des technischen Privatsphärenschutzes und der IT-Sicherheit. Bereits 2002 publizierte er in Mitautorschaft zu „Pervasive privacy with identity management“ und 2003 entwickelte er das Angreifermodell „The Freiburg Privacy Diamond: An Attacker Model for a Mobile Computing Environment” mit. Er engagierte sich für die Ringvorlesung „‚Privacy by Design‘ als technisches und gesellschaftliches Konstruktionsprinzip“. Seit 2015 verantwortet er beim Fraunhofer-Institut für Sichere Informationstechnologie (SIT) den Bereich Internationalisierung und strategische Industriebeziehungen. Michael Kreutzer leitete 2017–2019 das interdisziplinäre Forschungsprojekt „DORIAN - Desinformation aufdecken und bekämpfen“.

Marit Hansen ist seit 2015 die Landesbeauftragte für Datenschutz Schleswig-Holstein und leitet das Unabhängige Landeszentrum für Datenschutz (ULD). Davor war die Diplom-Informatikerin sieben Jahre lang stellvertretende Landesbeauftragte für Datenschutz Schleswig-Holstein. Im ULD hat sie den Bereich

der Projekte für technischen Datenschutz aufgebaut. Die gesellschaftlichen Herausforderungen, die aus der zunehmenden Digitalisierung resultieren, betrachten und bearbeiten Frau Hansen und ihr Team interdisziplinär und in Kooperation mit Forschung und Wissenschaft. Seit 1995 arbeitet Frau Hansen zu Themen des Datenschutzes und der Informationssicherheit. Ihr Schwerpunkt liegt auf der grundrechtskonformen Gestaltung von Systemen, insbesondere durch Datenschutz „by Design“ und „by Default“.

Autorenverzeichnis

Prof. Dr. Hartmut Aden ist seit 2009 Professor an der Hochschule für Wirtschaft und Recht Berlin, seit 2016 Professur für Öffentliches Recht, Europarecht, Politik- und Verwaltungswissenschaft. Er war von 2016 bis 2020 stv. Direktor des Forschungsinstituts für Öffentliche und Private Sicherheit (FÖPS Berlin) der HWR, bevor er 2020 Vizepräsident für Forschung und Transfer der HWR Berlin wurde. Er lehrt und forscht zu rechts- und verwaltungswissenschaftlichen Themen sowie zur vergleichenden Policy-Forschung. Themenschwerpunkte: Accountability, Menschenrechte, Datenschutz, Polizei-, Versammlungs- und Umweltrecht. Seine Forschungsprojekte befassen sich vorwiegend mit den Schnittstellen zwischen Recht, Politik und Verwaltung, auch aus europäischer und internationaler Perspektive.

Prof. Dr. Clemens Arzt ist Professor für Staats- und Verwaltungsrecht mit dem Schwerpunkt Polizei- und Ordnungsrecht an der HWR Berlin und Direktor des Forschungsinstituts für öffentliche und private Sicherheit (FÖPS Berlin). Seine Forschungsgebiete sind insbesondere deutsches und ausländisches Polizei- und Versammlungsrecht, Schutz kritischer Infrastrukturen und Recht der Fahrzeugautomatisierung. Am interdisziplinär ausgerichteten FÖPS Berlin leitet er die rechtswissenschaftliche Beteiligung mehrerer Drittmittelvorhaben.

Torben Jan Barev ist wissenschaftliche Mitarbeiter an der Universität Kassel am Fachgebiet für Wirtschaftsinformatik. Er absolvierte er ein Masterstudium an der University of Melbourne im Bereich Marketingmanagement. Seine Forschungsinteresse liegt insbesondere auf dem Decision-making in digitalen Umgebungen und seine Forschung wurde unter anderem im Journal Datenschutz und Datensicherheit (DuD) oder auf Konferenzen wie der International Conference on Design

Science Research in Information Systems and Technology (DESRIST) veröffentlicht. Für seine Forschung rund um Privacy Nudging gewann er den Best Paper Award der Hawaii International Conference on System Sciences (HICSS) 2020.

Jan Bartsch is a research associate in the Critical Information Infrastructures (cii) research group at the Institute of Applied Informatics and Formal Description Methods (AIFB) of the Karlsruhe Institute of Technology (KIT) in Germany. He earned his bachelor's degree in 2016 and his master's degree in 2020 in computer science at KIT. Jan Bartsch is interested in schemes for access control and other aspects of IT security and its application. He is also interested in the behavior of distributed and decentralized systems with heterogeneous agents.

Dr. Peter Biniok hat Informatik und (Technik-)Soziologie an der Technischen Universität Berlin studiert und an der Universität Luzern promoviert. Er war lange Zeit in grenzüberschreitenden Hochschulprojekten und als freier Mitarbeiter tätig und widmet sich aktuell sozialwissenschaftlicher Praxisforschung. Seine Forschungsschwerpunkte sind Digitalisierung und gesellschaftlicher Wandel, Wissenschafts- und Technikentwicklung sowie Mensch-Maschine-Interaktionen. Die letzten Veröffentlichungen behandelten die Themen „digitale Solidarität", „digitale Dienstbarkeit" und „holistischer Datenschutz".

Aline Blankertz ist Datenökonomin mit umfassender Erfahrung in der Analyse digitaler Märkte und Erarbeitung von Handlungsempfehlungen. Sie leitet wirtschaftswissenschaftliche Analysen bei dem Beratungsunternehmen Oxera und ist Mitgründerin und Co-Vorstand der SINE Foundation, einem gemeinnützigen Think-and-Do-Tank, der Datenkollaborationen ermöglicht. Aline arbeitet seit einigen Jahren zu verschiedenen Themen der Datenökonomie, u. a. zu Datentreuhändern, Plattformökonomie, Datenschutz, Algorithmen, Fairness in E-Commerce und Intermediärshaftung.

Arvid Butting ist Doktorand und wissenschaftlicher Mitarbeiter am Lehrstuhl für Software Engineering der RWTH Aachen. Seine Forschungsschwerpunkte umfassen die modellgetriebene Softwareentwicklung, die Entwicklung von kompositionalen Modellierungssprachen, sowie modellbasierte Softwarearchitekturen.

Dr. Niël Conradie is a postdoctoral researcher at RWTH Aachen University, working within the Applied Ethics Group of the Department of Society, Technology, and Human Factors. His current research focus is divided between the topic of

collective responsibility and how this relates to AI and other emergent technologies and – under the umbrella of the InviDas project – the topic of digital sovereignty as this notion pertains to digital wearable technologies. Work output has covered questions of moral enhancement, socially-responsive AI, and digital sovereignty. He earned his PhD in philosophy, focused on the intersection of responsibility and action theory, at the University of St Andrews, Scotland. His MA in philosophy and BA(PPE) were earned at the University of Stellenbosch, South Africa.

Jutta Croll ist Vorstandsvorsitzende der Stiftung Digitale Chancen, einer gemeinnützigen Organisation unter der Schirmherrschaft des BMWi und des BMFSFJ. Sie ist verantwortlich für das auf internationale Zusammenarbeit ausgerichtete Projekt Kinderschutz und Kinderrechte in der digitalen Welt. Als Wissenschaftlerin befasst sich Jutta Croll mit den Themen Medienpolitik und Mediennutzung, Förderung der Medienkompetenz und Entwicklung eines zeitgemäßen Kinder- und Jugendschutzes im Internet unter Berücksichtigung der Rechte von Kindern einerseits und aktueller technischer Entwicklungen andererseits sowie Usability und Accessibility im Bereich der Informations- und Kommunikationstechnologien, Fragen des Datenschutzes und der Nutzung von Social Media zur Förderung gesellschaftlicher Prozesse. Sie arbeitet zusammen mit dem Council of Europe, der Europäischen Kommission, der UNESCO, den Vereinten Nationen und ICANN.

Sunny Dass ist seit Januar 2021 als Berater für IT-Sicherheit tätig und erwarb davor den Bachelor of Science (B.Sc.) Informatik an der Technischen Universität Darmstadt.

Dr. Martin Degeling ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Systemsicherheit des Horst Görtz Instituts für IT Sicherheit der Ruhr Universität Bochum. In seinen Forschungsarbeiten im Bereich Usable Privacy and Security untersucht er die Vor- und Nachteile verschiedener Transparenz- und Kontrollmechanismen. Zuletzt hat er an mehrere Studien mitgewirkt, die die Auswirkungen der Datenschutzgrundverordnung auf Webseiten untersucht haben.

Tobias Dehling is a postdoctoral researcher at the Institute of Applied Informatics and Formal Description Methods (AIFB) of the Karlsruhe Institute of Technology (KIT) in Germany. His research interests are information privacy in consumer information systems, information systems for patient-centered health care, and distributed ledger technologies. Tobias received his PhD in Information

Systems in 2017 at the University of Kassel, Germany, and his master's degree (Diploma) in Information Systems in 2012 at the University of Cologne, Germany. His research has been published in renowned international outlets (e.g., ACM Computing Surveys, Electronic Markets, JMIR mHealth uHealth, Journal of the American Medical Informatics Association).

Ernestine Dickhaut ist Doktorandin und wissenschaftliche Mitarbeiterin am Fachgebiet Wirtschaftsinformatik und dem Wissenschaftlichen Zentrum für Informationstechnikgestaltung (ITeG) an der Universität Kassel. In ihren Forschungsschwerpunkten beschäftigt sie sich mit der Kodifizierung von konfliktärem, domänenspezifischem Wissen und wie dieses für Systementwickler zugänglich gemacht werden kann. Sie studierte an der TU Darmstadt den interdisziplinären Studiengang Psychologie in IT.

Dr. Jan Fährmann ist Jurist und Kriminologe. Nach einer Tätigkeit in der Strafverteidigung arbeitet er aktuell im Forschungsinstitut für öffentliche und private Sicherheit (FÖPS Berlin) an der HWR Berlin, an der er auch als Dozent tätig ist. Seine Forschungsschwerpunkte liegen im Polizei-, Strafprozess-. Strafvollzugs-, Datenschutz- und Betäubungsmittelrecht. In Forschungsprojekten befasst er sich vorwiegend mit den Schnittstellen zwischen Recht und Technik.

Manuel Fehler ist Informatiker und Head of Area X (Innovationsmanagement) bei Garmin Würzburg GmbH.

Dr. Michael Friedewald leitet am Fraunhofer Institut für System- und Innovationsforschung ISI in Karlsruhe das Geschäftsfeld „Informations- und Kommunikationstechnik". Er studierte Elektrotechnik, Wirtschaftswissenschaften und Technikgeschichte an der Rheinisch-Westfälischen Technischen Hochschule Aachen. Er beschäftigt sich mit Voraussetzungen, Prozessen und Folgen der Digitalisierung. Er ist Koordinator des vom BMBF geförderten Projekts „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt".

Dr. Thomas Grote studierte in Würzburg Philosophie und promovierte dort Ende 2015 im Bereich der Praktischen Philosophie. Seit Juli 2016 ist er Wissenschaftlicher Mitarbeiter in Tübingen, zunächst am IZEW und seit April 2019 am Exzellenzcluster Maschinelles Lernen, wo er Teil der AG Ethik & Philosophie ist. Der Schwerpunkt seiner Forschung liegt auf der Philosophie der medizinischen KI. Hier arbeitet er insbesondere an ethischen und erkenntnistheoretischen Fragen zum Zusammenspiel von klinischen Experten und KI Systemen, Fragen der

Fairness bei algorithmischen Entscheidungen sowie forschungsethischen Fragen. Seine Forschung ist dabei dezidiert interdisziplinär.

Clemens Gruber ist Diplom-Psychologe und Projektverantwortlicher für das Projekt InviDas bei der Stiftung Digitale Chancen. Er ist befasst mit der Partizipation unterschiedlicher Nutzergruppen in der Entwicklung digitaler Lösungen und der Analyse der sozialen und ethischen Implikationen. Die Stiftung Digitale Chancen erforscht als gemeinnützige Organisation die gesellschaftlichen Folgen der Digitalisierung. Sie setzt sich ein für den chancengleichen Zugang aller Menschen zum Internet und fördert ihre Medienkompetenz.

Marit Hansen ist seit 2015 die Landesbeauftragte für Datenschutz Schleswig-Holstein und leitet das Unabhängige Landeszentrum für Datenschutz (ULD). Davor war die Diplom-Informatikerin sieben Jahre lang stellvertretende Landesbeauftragte für Datenschutz Schleswig-Holstein. Im ULD hat sie den Bereich der Projekte für technischen Datenschutz aufgebaut. Die gesellschaftlichen Herausforderungen, die aus der zunehmenden Digitalisierung resultieren, betrachten und bearbeiten Frau Hansen und ihr Team interdisziplinär und in Kooperation mit Forschung und Wissenschaft. Seit 1995 arbeitet Frau Hansen zu Themen des Datenschutzes und der Informationssicherheit. Ihr Schwerpunkt liegt auf der grundrechtskonformen Gestaltung von Systemen, insbesondere durch Datenschutz „by Design“ und „by Default“.

Prof. Dr. Dominik Herrmann ist seit Oktober 2017 ordentlicher Professor für Datenschutz und Sicherheit in der Informationstechnik an der Universität Bamberg. Zuvor war er als Post-Doc in der Gruppe Sicherheit in verteilten Systemen an der Universität Hamburg tätig. Dominik Herrmann hat 2014 an der Universität Hamburg in Informatik promoviert. Seine Dissertation zu Datenschutzfragen im Domain Name System wurde mit dem Dissertationspreis der Gesellschaft für Informatik (GI) für die beste Informatik-Dissertation in Deutschland, Österreich und der Schweiz, dem GI/CAST-Dissertationspreis für Informationssicherheit und dem Forschungspreis der GDD e.V. ausgezeichnet. 2014 wurde Dominik Herrmann zum Junior Fellow der Gesellschaft für Informatik ernannt.

Prof. Dr. Gerrit Hornung studierte Rechtswissenschaften und Philosophie an den Universitäten Freiburg und Edinburgh. 2005 wurde er an der Universität Kassel mit einer Arbeit über Rechtsprobleme von Chipkartenausweisen promoviert. Nach dem Referendariat war er 2006 bis 2011 Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel und

habilitierte sich dort mit der Arbeit „Grundrechtsinnovationen“. 2011 bis 2015 war er Professor für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau. Seit 2015 ist Hornung Professor für Öffentliches Recht, IT-Recht und Umweltrecht an der Universität Kassel und Direktor am dortigen Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG).

Dr. Andreas Janson ist Post-Doc und Projektleiter am Institut für Wirtschaftsinformatik der Universität St.Gallen (IWI-HSG). Dr. Andreas Janson promovierte an der Universität Kassel zu digitalen Lernprozessen. Seine Forschungsinteressen umfassen dabei insbesondere das Decision-making in digitalen Umgebungen und die Gestaltung von digitalen Dienstleistungen. Seine Forschung wurde unter anderem in Journals wie dem Journal of the Association for Information Systems (JAIS), Journal of Information Technology (JIT) und dem Acade Management Learning & Education (AMLE) Journal veröffentlicht. Für seine Forschung rund um Privacy Nudging gewann er den Best Paper Award der Hawaii International Conference on System Sciences (HICSS) 2020.

Murat Karaboga studierte Politikwissenschaften, Philosophie und Pädagogik. Seit 2014 ist er am Fraunhofer-Institut für System- und Innovationsforschung ISI wissenschaftlicher Mitarbeiter im Geschäftsfeld Informations- und Kommunikationstechnologien in der Abteilung Neue Technologien. Seine Arbeitsschwerpunkte liegen in der Policy-Analyse und der Analyse von Governance- und Akteursstrukturen, insb. im Hinblick auf den Schutz personenbezogener Daten im Kontext neuer Technologien. In seiner Dissertation hat er die Entstehung der Datenschutz-Grundverordnung unter Berücksichtigung der Debatten rund um einen individualistischen und kollektivistischen Datenschutz untersucht.

Özlem Karasoy studierte Angewandte Informatik an der Ruhr-Universität Bochum und erlangte 2019 ihren Bachelor-Abschluss. In ihrer Bachelorarbeit beschäftigte sie sich mit den Umsetzungsstrategien für das Recht auf Datenportabilität nach Datenschutzgrundverordnung in Unternehmen. Direkt nach ihrem Abschluss absolvierte sie ein Orientierungspraktikum als Datenschutzkoordinatorin. Aktuell ist Özlem Güdel auf der Suche nach einer Anstellung im Bereich Datenschutz.

Alina Khayretdinova ist wissenschaftliche Mitarbeiterin am Institut für Arbeitswissenschaft und Technologiemanagement (IAT), Universität Stuttgart. Ihre Forschungsschwerpunkte liegen im Bereich Usability und User Experience von Identitätsmanagement-Lösungen und Sprachassistenten. Zuvor absolvierte

sie ihr Masterstudium im Fachbereich Computerlinguistik in Stuttgart und ihr Diplomstudium im Bereich Übersetzungstheorie in Ufa (Russland).

Ralf Kneuper ist seit 2016 Professor für Informatik und Wirtschaftsinformatik an der IUBH Internationale Hochschule im Bereich Fernstudium mit den Schwerpunkten IT-Management, IT-Sicherheit und Datenschutz. Davor hat er ca. 25 Jahre bei verschiedenen IT-Unternehmen sowie als selbstständiger Berater für Qualitätsmanagement und Prozessverbesserung in der IT gearbeitet.

Prof. Dr. Nicole Krämer ist Professorin für Sozialpsychologie – Medien und Kommunikation an die Universität Duisburg-Essen in der Fakultät für Ingenieurwissenschaften.

Dr. Michael Kreutzer forscht und publiziert seit mehr als 20 Jahren zu Fragestellungen des technischen Privatsphärenschutzes und der IT-Sicherheit. Bereits 2002 publizierte er in Mitautorschaft zu „Pervasive privacy with identity management“ und 2003 entwickelte er das Angreifermodell „The Freiburg Privacy Diamond: An Attacker Model for a Mobile Computing Environment” mit. Er engagierte sich für die Ringvorlesung „„Privacy by Design‘ als technisches und gesellschaftliches Konstruktionsprinzip“. Seit 2015 verantwortet er beim Fraunhofer-Institut für Sichere Informationstechnologie (SIT) den Bereich Internationalisierung und strategische Industriebeziehungen. Michael Kreutzer leitete 2017–2019 das interdisziplinäre Forschungsprojekt „DORIAN - Desinformation aufdecken und bekämpfen“.

Dr. Michael Kubach studied politics and administrative science as well as management at the universities of Konstanz, Göttingen and Lille. He received a PhD in economics at the Georg-August-University Göttingen. Since 2013, Michael Kubach is working in the Fraunhofer IAO Team Identity Management on issues around viable security, where he takes a user oriented and a socioeconomic perspective. Michael Kubach has worked in several European and national cooperative research projects such as the EC-funded eSSIF-TRAIN, LIGHTest and FutureID as well as in national projects such as ONCE, ENTOURAGE, and SkIDentity. Moreover, he has been consulting international corporations and NGOs. His research interests focus on the areas of economic aspects of IT-security, privacy and identity management.

Robert Landwirth studierte Soziologie, Psychologie und Philosophie an der Friedrich-Alexander Universität Erlangen-Nürnberg sowie an der Duke University. Seine Forschungsschwerpunkte sind Internetkommunikation und Identitätsbildung mit einem Interessenschwerpunkt in soziologischer Theorie. Momentan arbeitet er als wissenschaftlicher Mitarbeiter im BMBF geförderten, interdisziplinären Forschungsprojekt PANDA (https://panda-projekt.org) am Lehrstuhl für Sicherheit in der Informationstechnik der TU Darmstadt. Im Rahmen des Projekts ist er für die soziologische Erforschung von Darknets zuständig und beschäftigt sich mit den Auswirkungen technischer Anonymität auf die Kommunikationsdynamik online. In seiner Dissertation versucht er die Grundzüge einer Sozialtheorie für Internetkommunikation zu entwickeln.

Florian Lauf is scientist in the department of "Healthcare" at the Fraunhofer Institute for Software and Systems Engineering ISST in Dortmund, Germany. Previously to this, he finished his studies in Applied Computer Science with the emphasis on e-services engineering and robotics at the TU Dortmund. In the context of his master thesis, Mister Lauf modelled a reliable artificial hearth control and thereby discovered his interest in the combination of computer science and medicine. In a digitalizing world, personal data are becoming increasingly important. Therefore, Mister Lauf is engaged in current research topics at Fraunhofer ISST concerning the data sovereignty, the Digital Life Journey and the International Data Spaces.

Prof. Dr. Jan Marco Leimeister ist Leiter des Fachgebietes Wirtschaftsinformatik und Direktor am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel. Er ist zudem Ordinarius für Wirtschaftsinformatik und Direktor am Institut für Wirtschaftsinformatik (IWIHSG) der Universität St.Gallen. Seine Forschungsschwerpunkte liegen im Bereich Digital Business, Digital Transformation, Dienstleistungsforschung, Crowdsourcing, Digitale Arbeit, Collaboration Engineering und IT Innovationsmanagement. Er unterrichtet in diversen Executive Education Programmen zu diesen Themen.

Alexandra Lux ist seit 2017 wissenschaftliche Mitarbeiterin im interdisziplinären Projekt PANDA (Parallelstrukturen, Aktivitätsformen und Nutzerverhalten im Darknet) und promoviert im Fachgebiet Medienpsychologie bei Prof. Sabine Trepte an der Universität Hohenheim. In ihrer Dissertation untersucht sie Kommunikation auf soziale Netzwerkseiten im Darknet. Sie studierte Publizistik- und Kommunikationswissenschaft mit den Nebenfächern Psychologie und Soziologie an der Universität Wien und University of Ottawa.

Dr. Judith Meinert arbeitet als wissenschaftliche Mitarbeiterin am Lehrstuhl für Sozialpsychologie: Medien und Kommunikation an der Universität Duisburg-Essen. Dort forscht sie zu den Themen Social Media Kommunikation sowie Wahrnehmung und Umgang mit Privatheitsrisiken und Schutzansätzen u.a. im Bildungskontext. In ihrer Doktorarbeit untersuchte sie Glaubwürdigkeitsbewertungen von News und politischer Kommunikation in sozialen Medien unter Berücksichtigung zugrundeliegender psychologischer Mechanismen. Zuvor absolvierte Judith Meinert sowohl ihr Master- als auch ihr Bachelorstudium im Fachbereich der angewandte Kognitions- und Medienwissenschaften mit dem Schwerpunkt Psychologie (im Master) an der Universität Duisburg-Essen.

Dr. Sven Meister is heading the department "Healthcare" at the Fraunhofer Institute for Software and Systems Engineering in Dortmund, Germany. He holds a diploma degree and doctorate in computer science, focused on the procession of bio-medical data. Since 15 years, Sven Meister is driving the research on disruptive digital innovation in healthcare forward. As data has become more and more important, actual projects are asking for data-driven solution as well as strategies for real-world implementation of them. He is a board member of MedEcon Ruhr e.V. and SMITH from German Medical Informatics Initiative as well as head of the Medical Data Space at the International Data Spaces Association e.V.

Dr.-Ing. Alexander Mertens ist Abteilungsleiter „Ergonomie und Mensch-Maschine-Systeme" am Institut für Arbeitswissenschaften der RWTH Aachen.

Dr. Judith Michael ist PostDoc und Teamleiterin für Modellbasierte Assistenz- und Informationsservices am Lehrstuhl für Software Engineering der RWTH Aachen sowie Aufsichtsratsvorsitzende der Lakeside Science & Technology Park GmbH in Österreich. Ihre Forschung umfasst die (konzeptuelle) Modellierung von z.B. menschlichen Verhaltenszielen für Assistenzsysteme, Umgebungs- und Kontextinformationen und Datenschutzerklärungen. Zudem beschäftigt sie sich mit der Modellbasierten Entwicklung von Assistenz- und Informationssystemen sowie der Konzeption der entsprechenden Softwarearchitekturen in den Anwendungsgebieten Ambient Assisted Living, Controlling und Finanzen, Energie, Gesundheit, Produktionssysteme, Internet of Things, Industrie 4.0 und Smart Homes.

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.

Prof. Dr. Saskia Nagel arbeitet an der Schnittstelle von Ethik, Philosophie, Lebens- und Technikwissenschaften. Sie hat konzeptuelle und normative Ansätze für individuelle und gesellschaftliche Herausforderungen durch neue Technologien entwickelt. Der Schwerpunkt ihrer Arbeit liegt auf den ethischen, anthropologischen und sozialen Konsequenzen wissenschaftlichen und technologischen Fortschritts. Ihr besonderes Interesse gilt Systemen, in denen Mensch und Technologie interagieren, und die Fragen nach Autonomie, Verantwortung und Vertrauen stellen. In InviDas bringt ihr Team Expertise zu ethischen Fragen digitaler Souveränität ein.

Prof. Dr. Verena Nitsch ist Leiterin des Instituts für Arbeitswissenschaft der RWTH Aachen. Sie ist als Gutachterin und Beraterin in zahlreichen Ausschüssen und Beiräten tätig, u.a. im Programmausschuss „Robotik und Automation“ des DLR Raumfahrtmanagements, im Fachbeirat des Forschungsinstituts für Betriebliche Bildung und im Programmkomitee der Tagung „Mensch und Computer“. Zu ihren Forschungsschwerpunkten zählt die menschengerechte Mensch-Technik Interaktion in teil- und hochautomatisierten Arbeitssystemen sowie die Natural User Interface Gestaltung.

Dr. Carsten Ochs ist seit 2014 Postdoc an der Universität Kassel, Fachgebiet Soziologische Theorie, und Mitarbeiter im Projekt „Forum Privatheit.“ Er befasst sich seit bald zwei Jahrzehnten mit den soziokulturellen Effekten und Implikationen von Digitalisierungsprozessen. Nach dem Studium (Frankfurt/M., London) untersuchte er in seiner Dissertation (Gießen) Digitalisierungsprozesse in Pakistan. Seit 2011 ist er verstärkt mit Privatheit befasst, zunächst an der TU Darmstadt im Projekt „Internet Privacy“, später am European Center for Security and Privacy by Design. Seine Publikationen umfassen sowohl empirische, als auch theoretische und historische Arbeiten zur Anthropologie und Soziologie von Digitalisierung und Privatheit, sowie zu epistemologischen und gesellschaftsstrukturellen Fragen.

Fabian Pittroff ist wissenschaftlicher Mitarbeiter am Fachgebiet Soziologische Theorie der Universität Kassel. Seine Forschungsschwerpunkte sind die Kultur

der Digitalisierung, Soziologien der Subjektivierung und die Zukunft des Privaten. Dafür forscht er zum NSA-Untersuchungsausschuss, dem Internet der Dinge, der modernen Freundschaft und den Praktiken der Selfie-Fotografie. Er ist ehemaliger Mitarbeiter des Forum Privatheit und aktuell assoziierter Doktorand der Forschungsgruppe „Gender/Diversity in Informatics Systems“ (GeDIS) und des DFG- Graduiertenkollegs „Privatheit und Vertrauen für mobile Nutzende“.

Florian Platzer ist wissenschaftlicher Mitarbeiter in der Abteilung Media Security und IT Forensics am Fraunhofer Institut für Sichere Informationstechnologie. Er arbeitet seit Anfang 2019 im interdisziplinären Projekt PANDA (Parallelstrukturen, Aktivitätsformen und Nutzerverhalten im Darknet) für die Disziplin Informatik. Florian Platzer studierte IT-Sicherheit an der Technischen Universität Darmstadt.

Sebastian Pütz ist Doktorand und wissenschaftlicher Mitarbeiter in der Abteilung Ergonomie und Mensch-Maschine-Systeme am Lehrstuhl und Institut für Arbeitswissenschaft der RWTH Aachen. In seiner Forschung untersucht er, wie die digitale Souveränität von Nutzern digitaler Technologien durch die nutzerzentrierte Aufbereitung von datenschutzrelevanten Informationen gefördert werden kann.

Tilla Reichert studierte Deaf Studies und Gebärdensprachdolmetschen an der Humboldt Universität zu Berlin. Neben ihrer Tätigkeit als Gebärdensprachdolmetscherin wirkt sie als wissenschaftliche Mitarbeiterin im Institut für praktische Interdisziplinarität (Institut PI, Berlin) schwerpunktmäßig im Bereich Accessibility-Aspekte digitaler Technologien sowie Digitale Teilhabe und Inklusion. Ihre Promotion beschäftigt sich mit den Herausforderungen des Dolmetschens für taube Akademiker*Innen bzw. Professionelle.

Dr. Irmhild Rogalla ist Leiterin des Instituts für praktische Interdisziplinarität (Institut PI, Berlin). Das Institut PI forscht, entwickelt und berät zum Thema Digitalisierung und Arbeit, – zu Entwicklungs- und Innovationsprozessen ‚in‘ der IT, insbesondere durch Technikfolgenabschätzung; – zu Anwendungs- und Einsatzbereich ‚von‘ IT, insbesondere in High-Tech-Bereichen (aktuell: Internet of Things, cyberphysische Systeme, Data Science und Analytics), aber auch in Alltag und Gesellschaft; – zur Gestaltung ‚mit‘ IT, insbesondere von Arbeitsprozessen, Kompetenzentwicklung sowie „Digitaler Teilhabe und Inklusion“. Frau Dr. Rogalla ist ertaubt und verfügt über vielfältige eigene Erfahrungen mit der Nutzung digitaler Technologien zur Teilhabe in allen Lebensbereichen.

Dr. Heiko Roßnagel is head of the Competence Team Identity Management at the Fraunhofer Institute for Industrial Engineering IAO. He studied computer science at the TU Darmstadt. He received a PhD in business administration and economics at the Goethe-University Frankfurt. He is currently coordinating the EC-funded H2020 project LIGHTest and has coordinated the FP7 project FutureID. He has been participating in several European and national cooperative research projects such as the EC-funded projects WiTness, FIDIS, SSEDIC, SECUR-ED and national projects such as VeRSiert, VERTRAG, SkIDentity, SANDRA, CUES, IDS and ENTOURAGE. His research interests are in the areas of security, privacy and identity management with a focus on human factors and technology development and adoption.

Prof. Dr. Bernhard Rumpe leitet den Lehrstuhl Software Engineering der RWTH Aachen. Er beschäftigt sich mit domänenspezifischer Modellierung und ihrer Anwendung im Software und Systems Engineering, in der wissenschaftlichen Modellbildung oder auch der Vertragsgestaltung. Mehrere dafür geeignete Sprachen, u.a. Derivate der UML und der SysML, wurden für den praktischen Einsatz auf Basis der Language Workbench MontiCore entwickelt. Prof. Rumpe ist unter anderem Mitglied im Center for Systems Engineering (CSE) und des Exzellenzclusters Internet of Production „der RWTH. Prof. Rumpe hat eine Reihe von Tagungen organisiert und ist Autor und Editor von 34 Büchern sowie Editor-in-Chief und Gründer des internationalen Journals on Software and Systems Modeling SSoSyM“.

Alexander Schäfer ist studierter Wirtschaftsingenieur mit der Vertiefungsrichtung Elektro- und Informationstechnik. Er arbeitete in mehrere Unternehmen im Bereich der Digitalisierung. In den letzten Jahren setzte er sich verstärkt mit den Themen der langfristigen Unternehmensgestaltung hinsichtlich des Innovationsmanagements auseinander.

Elisabeth Schauermann ist Referentin für Politik bei der Gesellschaft für Informatik e.V. und koordiniert dort unter anderem das Projekt InviDas (= Interaktive, visuelle Datenräume zur souveränen, datenschutzrechtlichen Entscheidungsfindung) und das Digital Autonomy Hub, im Zuge Projekte und Initiativen vernetzt werden, die sich mit individueller digitaler Souveränität und der Mündigkeit von Nutzer*innen befassen. Ihr fachlicher Fokus liegt auf offener Governance, Chancengerechtigkeit und Datendemokratie.

Diana Schneider studierte Philosophie und Germanistik an der Universität Potsdam sowie Kultur und Technik an der Brandenburgisch Technischen Universität Cottbus- Senftenberg. Seit 2018 ist sie wissenschaftliche Mitarbeiterin am Fachbereich Sozialwesen der FH Bielefeld University of Applied Sciences und Promovendin des Forschungsverbundes NRW Digitale Gesellschaft im Projekt „Maschinelle Entscheidungsunterstützung in wohlfahrtsstaatlichen Institutionen: Nutzungsoptionen, Implikationen und Regulierungsbedarfe (MAEWIN)". In ihrer Promotion untersucht sie, was plausible Zukunftsbilder für den Einsatz von algorithmischen Entscheidungsunterstützungssystemen am Beispiel der Teilhabeplanung in Deutschland sein können.

Dr. Sofia Schöbel ist Juniorprofessorin für Wirtschaftsinformatik an der Universität Osnabrück. Zuvor war sie Postdoktorandin am Fachbereich Wirtschaftsinformatik der Universität Kassel. Sofia Schöbel hat im Bereich Gamification im digitalen Lernen promoviert. Ihre Forschung konzentriert sind auf Aspekte wie persuasives Systemdesign, die Gestaltung smarter und persönlicher Assistenten, die digitale Transformation von Dienstleistungen und die Gestaltung von interaktiven Prozessen beim digitalen Lernen. Ihre Forschungsergebnisse wurden in verschiedenen Fachzeitschriften wie dem European Journal of Information Systems (ECIS), Communications of the AIS oder auf führenden Konferenzen im Bereich der Informationssysteme veröffentlicht wie ICIS oder ECIS veröffentlicht.

Prof. Dr. Johannes Schöning ist Lichtenberg-Professor und Leiter der Arbeitsgruppe Mensch-Technik-Interaktion der Universität Bremen, Mitglied des Technologie-Zentrums für Informatik und Informationstechnik der Universität Bremen sowie Co-Direktor des Bremen Spatial Cognition Centers. Seine Forschung umfasst MenschComputer-Interaktion, Geoinformatik und ubiquitäre Computertechnologien, die nachweislich das Leben ihrer Anwender*innen verbessern, indem sie deren Interaktionen mit der Umgebung unterstützen.

Sabrina Schomberg ist seit 2019 wissenschaftliche Mitarbeiterin des Fachgebiets Öffentliches Recht, IT-Recht und Umweltrecht am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel, in dem Projekt „Nudging Privacy in der digitalisierten Arbeitswelt – Systematische Konzeptentwicklung und Pilotierung"(Nudger). Von 2016-2018 absolvierte sie den Juristischen Vorbereitungsdienst am LG Kassel mit Stationen in Speyer und Berlin und schloss diesen mit dem Zweiten Juristischen Staatsexamen ab. „Zuvor studierte sie Rechtswissenschaften an der Georg-August-Universität Göttingen

und der Université de Genève mit dem Abschluss des Ersten Juristischen Staatsexamens und dem Schwerpunkt Internationales und Europäisches öffentliches Recht“.

Linda Schreiber ist wissenschaftliche Referentin in der Geschäftsstelle des Nationalen Forschungszentrums für angewandte Cybersicherheit am Fraunhofer SIT. Sie hat Informationsrecht (LL.B.) und Internationales Lizenzrecht (LL.M.) an der Hochschule Darmstadt, sowie Innovation, Technology and the Law an der University of Edinburgh studiert. Sie verfügt über Erfahrungen im Bereich IT-Vertragsgestaltung und Open Source Compliance.

Rachelle Sellung is a senior scientist the Fraunhofer Institute for Industrial Engineering IAO. She achieved a Master's of Science in Economics at the University of Hohenheim in Stuttgart, Germany. As well as, a Bachelor's of Business Administration in Marketing at the University of Mississippi in the USA. She contributed a socio-economic perspective in the large-scale EU FP7 project FutureID, which developed an identity management infrastructure for Europe. She led University Stuttgart's contribution in the EU Horizon 2020 project, LIGHTest, which aimed to create a global cross-domain trust infrastructure. Her research interests include the areas of security, identity management, and trust services in emerging technologies (e.g. Blockchain, and SSI).

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. Konkret geht es ihm darum, neue Technologien zur Verbesserung der Privatsphäre und Transparenz für mobile und verteilte Systeme zu entwickeln und in die Praxis umzusetzen. Hervais hat an der Technischen Universität Darmstadt Informatik studiert und ist Mitglied im Forum Privatheit.

Prof. Dr. Matthias Söllner ist Professor und Lehrstuhlinhaber für Wirtschaftsinformatik und Systementwicklung sowie Direktor des interdisziplinären Forschungszentrums für IS-Design (ITeG) an der Universität Kassel. Seine Forschung konzentriert sich auf das Verständnis und die Gestaltung erfolgreicher digitaler Innovationen in Bereichen wie der Hochschul- und Berufsbildung sowie Hybrid Intelligence. Seine Forschung wurde von Zeitschriften wie MIS Quarterly (Research Curation), Journal of the Association for Information Systems, Academy of Management Learning & Education, Journal of Information Technology,

European Journal of Information Systems und Business & Information Systems Engineering veröffentlicht.

Martin Steinebach studierte Informatik an der TU Darmstadt. 1999 wurde er Doktorand am GMD IPSI, 2003 promovierte er an der TU Darmstadt zum DoktorIngenieur im Fachbereich Informatik mit dem Thema digitaler Audiowasserzeichen. Im Jahre 2007 wechselte er nach der Auflösung des IPSI an das SIT, wo er 2010 die Abteilungsleitung Media Security and Forensics übernahm. Seit November 2016 ist er Honorarprofessor der TU Darmstadt und hält dort unter anderem eine Vorlesung zur Multimedia-Sicherheit. Er ist Autor von über 170 Fachpublikation. Mit seinen Arbeiten am ForBild Projekt erzielte Herr Steinebach gemeinsam mit seinen Kollegen den zweiten Platz beim IT-Sicherheitspreis 2012 der Horst-Görtz Stiftung. Er leitet zahlreiche Projekte zu IT-Forensik und Big-Data Sicherheit für Industrie und die öffentliche Hand.

Carolin Stellmacher ist Doktorandin und wissenschaftliche Mitarbeiterin in der Arbeitsgruppe Mensch-Technik-Interaktion der Universität Bremen. In ihrer Forschung entwickelt sie interaktive Technologien, die komplexe Datenräume von Fitness- und Gesundheitsanwendungen für Nutzer*innen verständlich kommunizieren und die Motivation zur Auseinandersetzung mit dem eigenen Datenschutz erhöhen.

Prof. Dr. Ali Sunyaev is Director of the Institute of Applied Informatics and Formal Description Methods (AIFB) and Professor at the Karlsruhe Institute of Technology (KIT) in Germany. His research interests are reliable and purposeful software and information systems within the scope of internet technologies, distributed ledger technology, trustworthy AI, auditing/certification of IT, and innovative health IT applications. His research accounts for the multifaceted use contexts of digital technologies with research on human behavior affecting IT and vice versa. Ali Sunyaev has received several awards for his research. At KIT, Ali Sunyaev is leading the Critical Information Infrastructures (cii) research group and acts as a mentor for numerous start-ups.

Dr. Sabine Theis ist PostDoc und wissenschaftliche Mitarbeiterin am Institut für Arbeitswissenschaften der RWTH Aachen. Ihre Forschung umfasst die Evaluation und Charakterisierung von Daten- und Informationsvisualisierungssystemen und -techniken aus einer Human Factors Perspektive.

Laura Friederike Thies promoviert an der Universität Kassel zu einem datenschutzrechtlichen Thema und war bis Juli 2020 wissenschaftliche Mitarbeiterin im Projekt AnEkA (Anforderungs- und Entwurfsmuster zur rechtsverträglichen und qualitätszentrierten Gestaltung kontextsensitiver Applikationen) in der Projektgruppe verfassungsverträgliche Technikgestaltung – provet – am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel.

Gülcan Turgut absolvierte 2020 ihren Bachelor-Abschluss in Angewandter Informatik an der Ruhr-Universität in Bochum. In ihrer Bachelorarbeit mit dem Titel „Die Umsetzung der Datenportabilität nach der Datenschutzgrundverordnung und ihre Tauglichkeit aus Sicht des Betroffenenüntersuchte sie die Tauglichkeit des Rechtes in ihrer Umsetzung für die EU Bürger. Derzeit ist sie auf der Suche nach einem Einstieg ins Arbeitsleben“.

Sandra Wittmer schloss ihr Studium der Rechtswissenschaften an der Johann Wolfgang von Goethe-Universität Frankfurt am Main mit dem ersten juristischen Staatsexamen ab. Seit Oktober 2018 ist sie als wissenschaftliche Mitarbeiterin im interdisziplinären Forschungsprojekt „PANDA: Parallelstrukturen, Aktivitätsformen und Nutzerverhalten im Darknet“ tätig und promoviert derzeit an der Universität Osnabrück zum Thema Straftaten und Strafverfolgung im Darknet.

Einleitung: Selbstbestimmung und Privatheit – Gestaltungsoptionen für einen europäischen Weg

Michael Friedewald, Michael Kreutzer und Marit Hansen

Digitalisierung stößt umfassende Wandlungsprozesse auf gesellschaftlicher, wirtschaftlicher und rechtlicher Ebene an. Übergreifend sind es vor allem fünf miteinander verschränkte, technologiegetriebene Trends, welche die zurzeit tiefgreifenden soziotechnischen Transformationsprozesse vorantreiben: Die Allgegenwart von Smartphones als dominierende Endgeräte der Informations- und Kommunikationstechnik, die Ausbreitung des Internet of Things, die Plattformökonomie, die Verbreitung von Social Networks und Fortschritte im Bereich künstlicher Intelligenz.

Diese Trends durchdringen alle Lebensbereiche. Vor dem Hintergrund der rasanten Entwicklungen entstehen Spannungen zwischen Erwartungen an den technologischen Fortschritt und einer sich wandelnden Kultur von Privatheit und Öffentlichkeit. Längst haben wir es nicht mehr nur mit einer isolierten Neuerung mit begrenzten und prognostizierbaren Wirkungen zu tun. Digitalisierung hat mittlerweile soziotechnische Infrastrukturen (Netze, Kommunikationsräume, Arbeitsorganisation, rechtliche Regelungen usw.) hervorgebracht, ohne die der Alltag kaum noch zu bewältigen ist und die so zum Rückgrat unserer modernen Gesellschaft

M. Friedewald (✉)
Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe, Deutschland
E-mail: michael.friedewald@isi.fraunhofer.de

M. Kreutzer
Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt, Deutschland
E-mail: michael.kreutzer@sit.fraunhofer.de

M. Hansen
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kiel, Deutschland
E-mail: marit.hansen@datenschutzzentrum.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_1

geworden sind. Heute sind wir am Übergang zu einer Phase, in der diese Entwicklungen globale Auswirkungen haben, indem sie zur Grundlage der vorherrschenden Wirtschaftsweise werden und bisherige Grundannahmen und Werte in Frage stellen. Die konkreten Wirkungen sind breit gestreut und bringen dabei zahlreiche neue Möglichkeiten hervor: Digitale Technologien ermöglichen Individuen neue Formen der Mitbestimmung und der verteilten Kommunikation, digitale Medien erlauben den orts- und zeitunabhängigen Zugriff auf weltweite Inhalte, und eine Vielzahl von Apps unterstützen zahlreiche Routine-Tätigkeiten und geben Individuen ein Mehr an Informationen und Kontrolle, beispielsweise über die eigene Gesundheit [3]. Jedoch können mit der zunehmenden Digitalisierung auch Fehlentwicklungen und Unsicherheit auf Seiten der Nutzer:innen entstehen: Digitale Plattformen können dazu genutzt werden, den Abbau von Rechten von Arbeitnehmenden voranzutreiben oder Digitalarbeiter:innen mehr und mehr in Richtung „Gig Economy" – in einer prekären Variante – zu drängen, klassische Medienöffentlichkeiten drohen von zahlreichen Echokammern überlagert zu werden, es gibt die Versuchung in Schulen und Krankenhäusern neue Überwachungstechnologien einzuführen usw. Prominente internationale Autor:innen [1, 2, 4] sehen diese Entwicklungen im Rahmen eines (uneingelösten) Versprechens von deren Protagonist:innen in Richtung einer besseren Steuerbarkeit von Wirtschaft, Politik und Gesellschaft einerseits, während gleichzeitig zur Realisierung des Versprechens großräumig Mechanismen der Verhaltenssteuerung eingesetzt werden, auf deren Wirkungsweise und Ziele weder die betroffenen Personen noch die Öffentlichkeit nennenswert Einfluss nehmen können. Dies hat Auswirkungen auf die Freiheitsrechte von Individuen im gesamten Lebensverlauf, darunter aber besonders für vulnerable Gruppen wie Menschen mit Beeinträchtigungen oder Kinder, die nicht über alle Fähigkeiten verfügen, um die entstehenden Risiken zu erkennen und sich selbst zu schützen.

Wir beobachten, dass die Europäische Union und Deutschland – angesichts der Fülle an Herausforderungen und in Folge der genannten Entwicklungen – einen sogenannten „dritten" bzw. „europäischen Weg" voranbringen möchten, der auf eine gemeinwohlorientierte Technikentwicklung europäischer Prägung abzielt. Dieser Ansatz versteht sich als Alternative zu einem rein profitorientierten Digitalkapitalismus, bzw. Digitalautoritarismus. Wir verstehen den europäischen Weg so, dass die Idee eines freien Digitalmarktes mit den demokratischen Werten und Grundrechten in Einklang gebracht wird, sodass die Potenziale erhalten bleiben, während nachteilige Auswirkungen minimiert werden. Nicht nur die Verabschiedung der Datenschutz-Grundverordnung (DSGVO), auch die weiteren Debatten in diesem Zusammenhang spiegeln diese Entwicklung wider: Darunter fallen die Daten- sowie die Blockchain-Strategie der Bundesregierung, die Empfehlungen der Datenethik-

kommission, ambitionierte Großprojekte wie GAIA-X, aber auch Bestrebungen der EU hinsichtlich einer europäischen Datenstrategie oder zur Plattformregulierung.

Im Bereich der Wissenschaft finden sich zudem zahlreiche Forschungsunternehmungen, die sich der Frage nach dem Status robuster demokratischer Formen der Öffentlichkeit und der Privatheit, der individuellen und kollektiven Selbstbestimmung, der Gewährleistung fairer Arbeitsbedingungen und des Gemeinwohls, der gesellschaftlichen Integration und der Gewährleistung weiterer Werte unter den Bedingungen der digitalen Gesellschaft widmen. Gleichzeitig sind digitale Problemlagen Dauerthema der Feuilletons und beschäftigen auch Kunst und Literatur in hohem Maße. Die Diskussion über Daten und Selbstbestimmung hat folglich mittlerweile einen festen Platz im politischen und gesellschaftlichen Diskurs eingenommen.

Das zentrale Thema, mit dem sich die Beiträge in diesem Band aus unterschiedlicher Perspektive befassen lautet daher: „Welche Gestaltungsoptionen sind geeignet, um Selbstbestimmung und Privatheit auch im Digitalzeitalter zu gewährleisten?"

Der vorliegende Band enthält Untersuchungen zu solchen Themen und Fragen. Er präsentiert eine Auswahl von Vorträgen der interdisziplinären Konferenz „Selbstbestimmung und Privatheit – Gestaltungsoptionen für einen europäischen Weg", die das „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt" am 12. und 13. November 2020 durchgeführt hat. Die Beiträge analysieren im interdisziplinären Dialog die Herausforderungen des digitalen Wandels für die informationelle Selbstbestimmung. Sie diskutieren verschiedene Aspekte für ein zukunftsfähiges Konzept des Datenschutzes in einer digitalen Gesellschaft und erörtern konstruktive Bausteine für eine zukunftsgerechte Gewährleistung von Selbstbestimmung.

Bei dem ersten Thema im Konferenzband steht im Fokus, wie der **Datenschutz unter den Rahmenbedingungen der existierenden Daten- und Plattformökonomie** realisiert werden kann.

So befasst sich *Aline Blankertz* (SINE Foundation e. V.) in ihrem Beitrag mit der Frage, welche Funktion Instrumente wie das Wettbewerbsrecht bei der Einhegung von Risiken spielen kann. Sie betrachtet dazu die Auswirkungen, die (fehlender) Wettbewerb auf den Schutz der Privatsphäre hat. Dabei geht es zunächst um die Frage, inwieweit konkrete Wirkungen von Wettbewerb auf die Privatsphäre belegt sind und Gegenmaßnahmen erfordern, bevor die Frage beleuchtet wird, inwieweit Wettbewerb auch ein Instrument für den besseren Schutz von personenbezogenen Daten und Privatsphäre darstellen kann. Abschließend werden Maßnahmen vorgestellt, die dies befördern können.

Der zweite Themenkomplex behandelt, was **Privatheit in Zeiten der umfassenden Digitalisierung** ausmacht und wie diese geschützt werden kann.

Carsten Ochs (Universität Kassel) reflektiert in seinem Beitrag die gesellschaftsstrukturellen Bedingungen im Bereich der Privatheit. Mittels der Rekonstruktion von strukturhistorischen Konstellationen stellt er vier prototypische Formen der informationellen Privatheit, die sich in unterschiedlichen Vergesellschaftungsphasen der Moderne herausgebildet haben, vor. Darauf aufbauend wird erläutert, welche Anforderungen sich aus den unterschiedlichen Formen der Privatheit für die Technikgestaltung ergeben.

Der Beitrag von *Michael Kreutzer* und *Johanna Mittermeier* (Fraunhofer SIT) ordnet die technischen Möglichkeiten zu Selbstanalysen, Selbstoptimierungsvorschlägen und Prognosen durch Maschinelles Lernen ein und verknüpft diese mit einer philosophischen Betrachtung entlang folgender Fragestellung: Wie steht es um die Freiheit der Entscheidung, ob das Individuum durch Maschinelles Lernen berechnete, auf sich bezogene Analysen wissen sollen muss oder ob es sich dazu entschließen darf, dies nicht wissen zu wollen.

Fabian Pittroff (Universität Kassel) leistet einen Beitrag zur Analyse zeitgenössischer Formen der Personalisierung unter den Bedingungen der Digitalisierung. Um die Herausforderungen für Privatheit und Selbstbestimmung durch Personalisierung zu identifizieren, stellt er Ergebnisse einer autoethnografischen Studie zur Herstellung von Selfie-Fotografien, eine mögliche Form der Personalisierung auf Seite der Nutzer:innen unter digitalen Bedingungen, vor.

Der dritte Themenblock knüpft thematisch an die Frage nach der Privatheit unter geänderten Bedingungen an und diskutiert, welchen Wert und welche Funktion **Anonymität** in unserer Gesellschaft hat und wie diese gewährleistet werden kann.

Der Beitrag von *Robert Landwirth* (Technische Universität Darmstadt) beleuchtet das Konzept der Anonymität und seine Bedeutung für demokratische Gesellschaften und diskutiert diese am Beispiel des Tor-Netzes bzw. Darknets.

Alexandra Lux und *Florian Platzer* (Fraunhofer SIT und Technische Universität Darmstadt) erstellen eine Anonymitätsmetrik unter Verwendung des Tor-Browsers und legen ihren Fokus auf die Verbindung der technischen und psychologischen Komponenten der Betrachtung. Ziel dieses Beitrags ist es, die Tor-Nutzergruppe in Bezug auf den Grad der Anonymität und Online-Privatheitskompetenz sowie Motive und Zweck der Nutzung zu erforschen.

Sandra Wittmer, Florian Platzer und *Martin Steinebach* (Fraunhofer SIT und Technische Universität Darmstadt) wenden sich in ihrem Beitrag den Möglichkeiten der Strafverfolgung im Tor-Netz zu. Es werden Vorgehensweisen zur Identifizierung tatverdächtiger Personen vorgestellt und aus rechtlicher Perspektive bewertet, ob diese von den derzeit existierenden Ermittlungsbefugnissen der Strafverfolgungsbehörden gedeckt wären.

Ralf Kneuper (IUBH Internationale Hochschule) beschäftigt sich im letzten Beitrag dieses Themenblocks mit der Frage, ob für anonymisierte Daten wirklich kein Datenschutz erforderlich ist. Der Aufsatz gibt zunächst eine Einführung in Problematiken in Zusammenhang mit Anonymisierung, Re-Identifikation und die Notwendigkeit des Schutzes anonymer Daten, gefolgt von einer systematischen Darstellung und Auseinandersetzung von in diesem Zusammenhang in der Literatur diskutierten Lösungsansätzen.

Der vierte thematische Block legt den Fokus auf die Frage, inwieweit Privatheit und Datenschutz eine Rolle bei der **Verwirklichung von sozialer Teilhabe** spielen können. Dies geschieht zum einen am Beispiel des medial gestützten Lernens und zum anderen im Rahmen von Bemühungen zur Eingliederung von gesellschaftlich benachteiligten Gruppen.

Judith Meinert und *Nicole C. Krämer* (Universität Duisburg-Essen) beschäftigen sich in ihrem Beitrag mit der Frage, inwiefern Kinder und Jugendliche die Bedrohung ihrer Privatsphäre bei der Nutzung von Lernsoftware wahrnehmen. Im Rahmen einer empirischen Befragung wurde untersucht, in welchem Umfang Lernsoftware in den Schulen und zu Hause genutzt wird, ob Kenntnisse über potenzielle Bedrohungen der persönlichen Daten bei der Nutzung von Lernsoftware vorhanden sind und welche Schutzmaßnahmen ergriffen werden, um die eigenen Daten zu schützen.

Im Rahmen ihres Beitrags untersuchen *Hervais Simo Fhom, Michael Kreutzer* und *Linda Schreiber* (Fraunhofer SIT), inwieweit Android Learning Apps vor dem Hintergrund der DSGVO die Privatheit ihrer Nutzenden gewährleisten und Anforderungen an Datensicherheit erfüllen. Die zunächst vorgestellte grobgranulare Analyse befasst sich mit Beobachtungen und statistischen Erkenntnissen, welche direkt aus den bereits gesammelten Metadaten der Applikationen ersichtlich sind. Bei der folgenden feingranularen Analyse wird die App-Software mittels Tools zur statistischen und dynamischen Auswertung genauer betrachtet.

Diana Schneider (Fraunhofer ISI und FH Bielefeld) untersucht in ihrem Artikel, ob und wie ein algorithmisches System zur Entscheidungsunterstützung im Prozess der Teilhabeplanung behilflich sein kann. Zwanzig leitfadengestützte Interviews geben Anhaltspunkte darüber, welches Konzept von Privatheit die interviewten Personen vertreten und welche Auswirkungen dies auf potentielle Datenanalysen hat.

Irmhild Rogalla und *Tilla Reichert* (Institut für praktische Interdisziplinarität) zeigen in ihrem Beitrag strukturelle Lösungen für den Konflikt zwischen Accessibility und Privacy für Menschen mit Behinderungen in der digitalen Welt auf. Eine Lösung dafür bietet der Europäische Standard EN 16234-1:2019 „e-Competence Framework (e-CF)“, in welchem seit neuem Accessibility und Privacy als „trans-

versal aspects“ besonders hervorgehoben und alle IT-Fach- und Führungskräfte zu ihrer Berücksichtigung verpflichtet werden.

Der fünfte Abschnitt des Konferenzbandes nimmt einen perspektivischen Blick ein und befasst sich mit den Notwendigkeiten und Möglichkeiten einer **Fortentwicklung des Datenschutzrechts.**

Murat Karaboga (Fraunhofer ISI) diskutiert in seinem Beitrag anhand ausgewählter Teilbereiche des Datenschutzrechts Lösungsansätze, die über die Fokussierung auf das Individuum hinausgehen und die als eine Art Mittelweg zwischen individualistischen und kollektivistischen Ansätzen verstanden werden können.

Der Beitrag von *Jan Fährmann, Hartmut Aden* und *Clemens Arzt* (Hochschule für Wirtschaft und Recht Berlin) untersucht aus einer rechts- und verwaltungswissenschaftlichen Perspektive, inwiefern Transparenzdefizite bei der Ausgestaltung der polizeilichen Datenerhebung und weiteren Datenverarbeitung bestehen. Am Ende des Beitrags werden mögliche Instrumente zur Steigerung von Transparenz analysiert.

Özlem Karasoy, Gülcan Turgut und *Martin Degeling* (Ruhr-Universität Bochum) analysieren in ihrem Beitrag die Nutzung/Anwendung des in Art. 20 DSGVO formulierten Rechts auf Datenübertragbarkeit. Mittels Forschungsergebnissen aus zwei empirischen Studien (Unternehmens- und Nutzerperspektive) gibt dieser Beitrag Handlungsempfehlungen, damit das Recht in der Praxis stärkere Anwendung finden kann.

Der sechste Abschnitt befasst sich mit den praktischen Möglichkeiten wie **Datenschutz durch Technikgestaltung** und durch datenschutzfreundliche Voreinstellungen Nutzer:innen in ihrer Handlungsautonomie stärken kann.

Peter Biniok (Kompetenzzentrum Innung SHK Berlin) behandelt in seinem Kapitel schwerpunktmäßig die Debatte um Privatheit und Autonomie in Verbindung mit digitalen Technologien. Der Fokus des Beitrags liegt auf der Selbstermächtigung der Nutzer:innen. Dafür stellt er die Frage nach den Voraussetzungen von Selbstbestimmung und Privatheit in einer digitalen Welt, um anschließend die Herausforderungen und Chancen digitaler Selbstermächtigung zu diskutieren.

Der Beitrag von *Sofia Schöbel, Sabrina Schomberg, Torben Jan Barev, Thomas Grote, Andreas Janson, Gerrit Hornung* und *Jan Marco Leimeister* (Universität Kassel, Universität Tübingen bzw. Universität St. Gallen) stellt eine interdisziplinäre Perspektive auf das Thema „Privacy Nudges“ vor. Sie untersuchen die Möglichkeiten und Grenzen bei der Gestaltung von Privacy Nudges, um, ausgehend davon, Gestaltungsempfehlungen für eine rechtlich, ethisch und soziotechnisch konforme Gestaltung von Privacy Nudges zu geben.

Der Beitrag von *Alina Khayretdinova, Michael Kubach, Rachelle Sellung* und *Heiko Roßnagel* (Universität Stuttgart sowie Fraunhofer IAO) analysiert mittels

einer empirischen Studie die Nutzbarkeit und praktische Anwendbarkeit einiger Decentralized Identity Management (DIdM)-Lösungen und stellt ihre Ergebnisse und die daraus gewonnenen Schlüsse vor. Neue Ansätze für das Identitätsmanagement auf der Grundlage von Technologien wie verteilten Ledgern werden als Chance gesehen, den Nutzer:innen die volle Kontrolle über ihre eigenen Identitätsdaten zu geben. Eine große Herausforderung hierbei stellt die Gebrauchstauglichkeit dar.

Im siebten und letzten thematischen Abschnitt geht es schließlich darum, wie unterschiedliche **technische Ansätze** Privatheit und Datenschutz in verschiedenen Anwendungen verbessern können und dadurch die digitale Souveränität der Nutzer:innen stärken.

Martin Steinebach (Fraunhofer SIT) legt in seinem Beitrag eine strukturierte Ausarbeitung zum Einsatz von Uploadfiltern vor. Er zeigt Möglichkeiten und Risiken von Uploadfiltern auf und trägt damit zu einer differenzierten Sichtweise über die Thematik bei.

Alexander Schäfer (Darmstadt) stellt in seinem Beitrag ein Modell und Handlungsempfehlungen vor, um die existierenden Problemfelder der Gewährleistung einer digitalen Souveränität zu lösen. Nach seiner Ansicht ist der Kern des Problems die nicht ausreichende Reichweite gesetzlicher Initiativen wie der DSGVO, da diese oft international an der Durchsetzung scheitern.

Jan Bartsch, Tobias Dehling, Florian Lauf, Sven Meister und *Ali Sunyaev* (Karlsruher Institut für Technologie bzw. Fraunhofer ISST) betrachten in ihrem Beitrag die Datensouveränität aus einer technischen Forschungsperspektive. Sie propagieren die Verwendung von Policy-Definitionssprachen als maschinenlesbaren und durchsetzbaren Mechanismus zur Förderung der Datenhoheit.

Ernestine Dickhaut, Laura Friederike Thies, Andreas Janson, Jan Marco Leimeister und *Matthias Söllner* (Universität Kassel bzw. Universität St. Gallen) stellen ein Projekt vor, das den Lösungsansatz interdisziplinärer Anforderungs- und Entwurfsmuster verfolgt. Durch die Bereitstellung bewährter Lösungen für wiederkehrende Probleme in der Systementwicklung unterstützt es Entwickler:innen in ihrer Konzeption. Ziel des Beitrags ist es, mittels eines multimethodischen Ansatzes aufzuzeigen, welchen Beitrag diese Muster für die Entwicklung rechtsverträglicher und qualitativ hochwertiger KI-basierter Systeme leisten können. Um die Wirksamkeit der Muster zu untersuchen, wurde mithilfe der Muster ein Lernassistent entwickelt und durch eine Simulationsstudie evaluiert.

Judith Michael (RWTH Aachen) und ihre Co-Autor:innen diskutieren im abschließenden Beitrag die gesellschaftlichen Herausforderungen der digitalen Souveränität hinsichtlich Wearables. Der Beitrag skizziert Möglichkeiten zur Visualisierung rechtlicher und datenschutzrechtlicher Informationen und diskutiert Ideen für einen erlebbaren Datenschutz mit Gamifizierungskonzepten.

So wie es dem Forum Privatheit auch schon in den letzten Jahren gelungen ist, die interdisziplinäre Community zu Datenschutz, Selbstbestimmung und Privatheit zusammenzubringen, präsentiert dieser Konferenzband vielfältige Ansätze, Methoden und vor allem Ideen und Impulse. Das Team vom Forum Privatheit wünscht viel Spaß beim Lesen und hofft darauf, dass die zahlreichen spannenden Punkte und guten Anregungen in Wissenschaft, Praxis und Politik aufgegriffen und weiterentwickelt werden.

Literatur

1. Daum, T.: Das Kapital sind wir: Zur Kritik der digitalen Ökonomie. Edition Nautilus, Hamburg (2017)
2. Mau, S.: Das metrische Wir: Über die Quantifizierung des Sozialen. Suhrkamp, Berlin (2017)
3. Schwab, K.: Die Vierte Industrielle Revolution. Pantheon, München (2016)
4. Zuboff, S.: Das Zeitalter des Überwachungskapitalismus. Campus, Frankfurt (2018)

Datenschutz unter den Rahmenbedingungen der existierenden Daten- und Plattformökonomie

Warum Wettbewerbspolitik auch die Privatsphäre berücksichtigen muss

Aline Blankertz

Zusammenfassung

Europäische und deutsche Gesetzgeber:innen und Behörden sind sich einig, dass sie die negativen Folgen von Marktkonzentration begrenzen wollen. Doch inwieweit wirkt sich fehlender Wettbewerb auf den Schutz der Privatsphäre aus? Im Kontext des Facebook-Verfahrens werden v. a. zwei verschiedene Ansätze beleuchtet – einerseits, inwiefern Konzentration den Umfang der gesammelten bzw. genutzten Daten beeinflusst, und andererseits, wie Konzentration sich auf die Verhandlungsposition der Nutzer:innen auswirkt. Dieser Beitrag zeigt auf, dass der erste Ansatz nur spärlich empirisch gestützt ist, während der zweite weiterer konzeptioneller Ausarbeitung bedarf. Im Anschluss wird untersucht, inwieweit nicht nur Marktkonzentration, sondern fehlende Befähigung von Verbraucher:innen dazu führt, dass es keinen wirksamen Wettbewerb um besseren Datenschutz gibt. Beide Teile schließen mit politischen Handlungsempfehlungen ab.

Schlüsselwörter

Wettbewerb • Datenmacht • Privatsphäre • Regulierung • Wahlfreiheit

Die Privatsphäre von Individuen ist ein Thema für Datenschutzbehörden – so wird vielfach argumentiert, um zu begründen, wer für die Untersuchung der oftmals hochgradig bedenklichen Datenpraktiken von digitalen Plattformen zuständig

A. Blankertz (✉)
SINE Foundation e. V., Berlin, Deutschland
E-Mail: aline@sine.foundation

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_2

sei.[1] Doch es häufen sich Konstellationen, in denen Datenschutz- und Wettbewerbsbedenken miteinander verknüpft scheinen. Beispielsweise befasst sich der Facebook-Fall[2] des Bundeskartellamtes mit der Frage, ob und inwieweit Datenpraktiken der Plattform einen Missbrauch von Marktmacht darstellen. Allerdings gibt es bisher keinen Konsens darüber, inwiefern das Vorliegen von Marktmacht den Schutz der Privatsphäre beeinflusst, und welche weiteren Faktoren neben der Marktkonzentration die Intensität des Wettbewerbs um den Parameter Datenschutz treiben.

Dieses Kapitel befasst sich mit den Auswirkungen, die (fehlender) Wettbewerb auf die Privatsphäre hat insbesondere in den im Facebook-Verfahren untersuchten Zusammenhängen. Zunächst geht es um die Fragen, in Abschn. 1, inwieweit sich Wettbewerb auf die Privatsphäre auswirkt und, in Abschn. 1.1, ob es sich dabei um Auswirkungen auf den Umfang der gesammelten bzw. genutzten Daten handelt, oder, in Abschn. 1.2, ob es Auswirkungen auf die Verhandlungsposition der Nutzer:innen gibt, und in Abschn. 1.3, welche Gegenmaßnahmen zu erwägen sind. In Abschn. 2 wird die Frage beleuchtet, auf welche Faktoren neben der Marktkonzentration der wenig effektive Wettbewerb um besseren Datenschutz zurückzuführen ist und, erneut, welche Gegenmaßnahmen sinnvoll erscheinen.

1 Wann der Schutz der Privatsphäre auch vom Wettbewerb abhängt

Behörden befassen sich, wenn auch zögerlich, mit dem Einfluss von Wettbewerb auf Datenschutz. Der erste Fall, der sich ausdrücklich mit wettbewerbswidrigen Auswirkungen auf den Datenschutz befasst, ist der des deutschen Bundeskartellamtes gegen Facebook. In diesem argumentiert die Behörde, dass die Auferlegung schlechter Datenschutzbestimmungen einen Missbrauch von Marktmacht darstellt. Dieses Verfahren begann 2016, seither gab es weitere Fälle, die sich mit dem Zusammenhang zwischen Wettbewerb und Datenschutz befassen. Beispielsweise hat die geplante Übernahme von Fitbit, einem Hersteller von Smartwatches und Fitness-Trackern, durch Google Bedenken über die Zusammenführung sensibler Gesundheitsdaten mit vorhandenen Google-Profilen aufgeworfen.[3] Auch

[1] Siehe Körber, T. (2018) [30], „‚Ist Wissen Marktmacht?' Überlegungen zum Verhältnis von Datenschutz, ‚Datenmacht' und Kartellrecht – Teil 1".

[2] Bundeskartellamt (2019) [10], Beschluss des Bundeskartellamts zu B6-22/16 (Facebook).

[3] Siehe z. B. Bria, Francesca et al. (2020) [8], „Europe must not rush Google-Fitbit deal", Politico, 23. Juli, und Kemp, K. (2020b) [28], „Every step you take: why Google's plan to buy Fitbit has the ACCC's pulse racing", The Conversation, 23. Juni.

Tab. 1 Übersicht über die Zusammenhänge, über die Wettbewerb die Privatsphäre beeinflusst

	Zusammenhang	Evidenz
1	Wenn weniger Wettbewerb herrscht, können Unternehmen mehr personenbezogene Daten sammeln	Begrenzter Zusammenhang in App-Märkten [29] und vorläufige Belege eines Zusammenhangs in Werbemärkten [13]
2	Wenn weniger Wettbewerb herrscht, haben Verbraucher:innen weniger Wahlfreiheit in Bezug auf die Privatsphäre [20, 25]	Konzeptionelles Argument, offene Frage für die Wettbewerbsbehörden: Was ist der Maßstab für die Feststellung wettbewerbswidrigen Verhaltens und die Wiederherstellung der Wahlfreiheit?
3	Wenn Unternehmen fusionieren, können Unternehmen mehr Daten sammeln und verwenden [3]	Offensichtlich und Angelegenheit für Wettbewerbsbehörden, wenn die Privatsphäre ein relevanter Wettbewerbsfaktor ist
4	Personenbezogene Daten in den Händen marktbeherrschender Unternehmen verursachen mehr Schaden	Keine basierend auf den (theoretischen) Beweisen für die Auswirkungen der Preispersonalisierung: kein Zusammenhang zwischen Marktmacht und negativen Ergebnissen für Verbraucher:innen [41]
5	Wenn weniger Wettbewerb herrscht, können Unternehmen den Wettbewerb um die Privatsphäre untergraben [27]	Bisher beschränkt auf die Lesbarkeit von Datenschutzbestimmungen, die mit zunehmender Unternehmensgröße abnimmt
6	Marktmächtige Unternehmen können sich quasi-regulatorische Befugnisse über personenbezogene Daten aneignen, die den Wettbewerb behindern [1, 7, 32]	Wettbewerbsschäden erwiesen, unklar, ob es Vorteile für die Privatsphäre gibt

Quelle: Stiftung Neue Verantwortung

bei Praktiken von Apple wird geprüft, ob es zulässig ist, dass bestimmte personenbezogene Daten nicht weitergegeben werden, während sie für eigene Dienste verwendet werden.[4]

Sechs mögliche Zusammenhänge, über die der Wettbewerb die Privatsphäre beeinflussen kann, sind in Tab. 1 zusammengefasst. Sie stellen Hypothesen dar, durch die weniger Wettbewerb die Privatsphäre entweder auf unterschiedliche Weise beeinträchtigen (Zusammenhänge 1 bis 5) oder sie sogar fördern könnte

[4] Albergotti, Reed (2020) [1], „Calls grow for European regulators to investigate Apple, accused of bullying smaller rivals“, The Washington Post, 28. Mai.

(Zusammenhang 6). Die Tabelle fasst auch die verfügbare Evidenz dafür zusammen, ob und inwieweit sich die hypothetischen Auswirkungen tatsächlich auf Märkten beobachten lassen.

In diesem Beitrag liegt der Fokus auf den Hypothesen 1 und 2, die im Facebook-Fall relevant sind und sich der Frage annähern, ob Marktkonzentration das Verhalten des Unternehmens beeinflusst (Hypothese 1) und/oder die Beziehung zu anderen Marktteilnehmenden (Hypothese 2).[5]

1.1 Hypothese 1: Wenn weniger Wettbewerb herrscht, können Unternehmen mehr personenbezogene Daten sammeln

Können Unternehmen, die weniger Wettbewerb ausgesetzt sind, mehr personenbezogene Daten sammeln und somit weniger Privatsphäre gewähren? Diese Frage stellt sich im Facebook-Verfahren. Das Bundeskartellamt argumentiert, dass der Mangel an alternativen sozialen Netzwerken die Verbraucher:innen dazu zwänge, Datenschutzbestimmungen zu akzeptieren, die dieselben Verbraucher:innen ablehnen würden, wenn es Wettbewerb im Markt der sozialen Netzwerke gäbe. Der Bundesgerichtshof schlussfolgert aus den vom Bundeskartellamt vorgelegten Daten über Nutzer:innenpräferenzen, dass sich durch mehr Wettbewerb Angebote mit weniger eingreifenden Datenpraktiken hätten herausbilden können.[6] Allerdings ist die Frage nicht prinzipiell auf Facebook beschränkt. Wenn weniger Wettbewerb problematische Datenpraktiken eher ermöglicht, sind Bedenken auch in anderen stark konzentrierten digitalen Märkten, von Suchmaschinen bis hin zu App-Stores, gerechtfertigt.

Unterschiedliche Argumente stehen im Raum zur Frage, ob marktmächtige Unternehmen mehr oder sensiblere Daten sammeln. Einige argumentieren, dass Unternehmen unabhängig von ihrer Marktstellung ähnlichen Anreizen und Zwängen ausgesetzt sind, innerhalb der gesetzlichen Grenzen so viele Daten wie möglich zu erheben. Dies erleichtere die Monetarisierung und wird von Verbraucher:innen kaum bei der Auswahl ihrer Produkte berücksichtigt.[7] Andere

[5] Für eine vollständige Analyse siehe Blankertz, Aline (2020b) [5], „How competition impacts privacy. And why competition authorities should care".

[6] Bundesgerichtshof (2020) [9], Beschluss zu KVR 69/19, 23. Juni, Para 86.

[7] Siehe z. B. Körber (2018) [30], op. cit., und Information Technology und Innovation Foundation (2018) [26], Response to „The intersection between privacy, big data and competition, Data as a dimension of competition, and/or as an impediment to entry into or expansion within a relevant market".

argumentieren, dass Marktmacht es den Unternehmen ermögliche, aggressivere Datenpraktiken zu betreiben.[8] Prinzipiell solle der Wettbewerbsdruck die Unternehmen veranlassen, die Preise zu senken und/oder ihre Datenschutzbestimmungen zu verbessern, um die Nachfrage nach ihren Produkten zu steigern.

Die konkreteste Anwendung dieser Argumente erfolgt im Facebook-Verfahren. Nach einer dreijährigen Untersuchung gab das Bundeskartellamt Anfang 2019 bekannt, dass Facebook gegen die DSGVO verstoßen und damit seine marktbeherrschende Stellung missbraucht habe. Der Marktmachtmissbrauch bestehe darin, dass Facebook Nutzer:innen missbräuchliche Bedingungen auferlegt habe, die sie nicht ablehnen konnten, wenn sie die Plattform nutzen wollten. Diese unfairen Bedingungen ermöglichten es Facebook, Daten über Nutzer:innen aus verschiedenen Quellen über die eigene Plattform hinaus zu sammeln, einschließlich den übernommenen Netzwerken WhatsApp und Instagram sowie Websites von Drittanbietern, die „Gefällt mir" oder „Teilen"-Buttons enthielten oder die Analysedienste von Facebook nutzten. Nach Angaben des Bundeskartellamtes erlitten die Verbraucher einen Kontrollverlust über ihre Daten, der durch die Verletzung verschiedener Grundsätze der DSGVO durch Facebook verursacht wurde. Das Bundeskartellamt argumentierte, dass die Verbraucher weder eine gültige Einwilligung in dem nötigen Umfang gegeben hätten,[9] noch hätten sie zu erwarten, so umfassend überwacht zu werden.[10] Das Bundeskartellamt erlegte Facebook deshalb die Verpflichtung auf, die freiwillige Zustimmung der Nutzer zur Zusammenführung von Daten aus verschiedenen Quellen einzuholen, was faktisch eine „interne Entflechtung" der Daten erfordert.[11]

Wie in Abb. 1 zusammengefasst, setzte das Oberlandesgericht (OLG) Düsseldorf das Urteil aus, weil das OLG befand, dass das Bundeskartellamt keine ausreichenden Beweise dafür vorgelegt habe, dass das angeblich missbräuchliche Verhalten – der Verstoß gegen die DSGVO- durch die Marktbeherrschung von Facebook ermöglicht worden sei.[12] Das Bundeskartellamt legte gegen die Aussetzung Beschwerde beim Bundesgerichtshof (BGH) ein, der die Entscheidung des Bundeskartellamtes wieder einsetzte. Der BGH befand, dass die Aussetzung nicht gerechtfertigt war, verlagerte aber auch den Schwerpunkt der Untersuchung von der Frage, ob ein DSGVO-Verstoß einen Missbrauch der marktbeherrschenden

[8] Siehe Bundesgerichtshof (2020) [9], op. cit. und Kemp (2020a) [27], op. cit.

[9] Bundeskartellamt (2019) [10], op. cit., Para 639.

[10] Ebd., Para 848.

[11] Zeit (2019) [43], „Kartellamt bremst Facebook beim Sammlen von Nutzerdaten", 7. Februar.

[12] Oberlandesgericht Düsseldorf (2019) [36], Beschluss zu Vi-Kart 1/19 (V), 26. August.

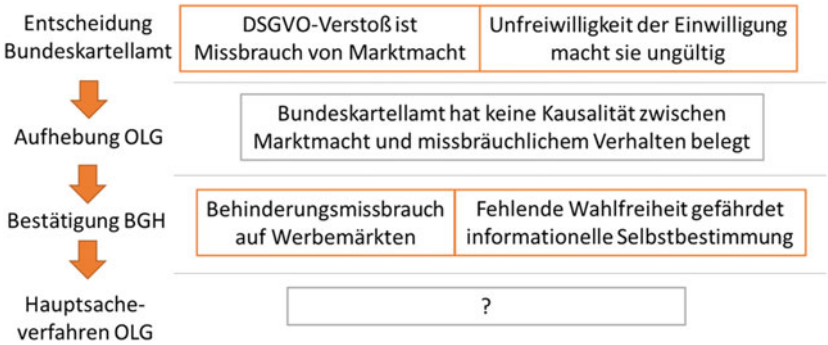


Abb. 1 Die Hauptargumente in den verschiedenen Stadien des Facebook-Falls. (Quelle: Stiftung Neue Verantwortung)

Stellung darstellt, auf die Frage, ob möglicherweise Behinderung von Wettbewerbern auf Werbemärkten vorgelegen haben und ob die Praktiken von Facebook die Wahlfreiheit der Verbraucher:innen unangemessen eingeschränkt haben.

1.1.1 Evidenz

Im Prinzip können diese Hypothesen empirisch getestet werden: Sammeln Unternehmen in einem Wettbewerbsumfeld weniger Daten und/oder weniger sensible Daten als marktbeherrschende Unternehmen? Ein erster Ansatzpunkt ist die Fallstudie Facebook selbst. Manche stellen dar, wie mit der zunehmenden Marktmacht von Facebook die Plattform immer weniger um die Privatsphäre der Nutzer besorgt sei.[13] Allerdings zeichnen die verfügbaren Daten ein komplexeres Bild: Abb. 2 veranschaulicht die Entwicklung der Datenschutzeinstellungen der Plattform, gemessen durch unabhängige Forschung, und die Entwicklung ihrer Marktbedeutung, approximiert durch die Anzahl der Nutzer:innen. Es wird deutlich, dass Datenschutz und Wettbewerb nicht, wie oft angenommen, direkt miteinander verknüpft sind, sodass weniger Wettbewerb automatisch zu schlechter geschützter Privatsphäre führe. So besserte sich der Datenschutz deutlich nach dem ersten Tiefpunkt zu Beginn 2009, um dann zwischen 2010 und 2014 stetig abzufallen. Doch ab 2015 gab es trotz weiter steigender Nutzer:innenzahlen eine deutliche Besserung. Weitere Faktoren wie öffentliche Aufmerksamkeit auf den

[13] Siehe z. B. Srinivasan, D. (2019) [39], „The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy".

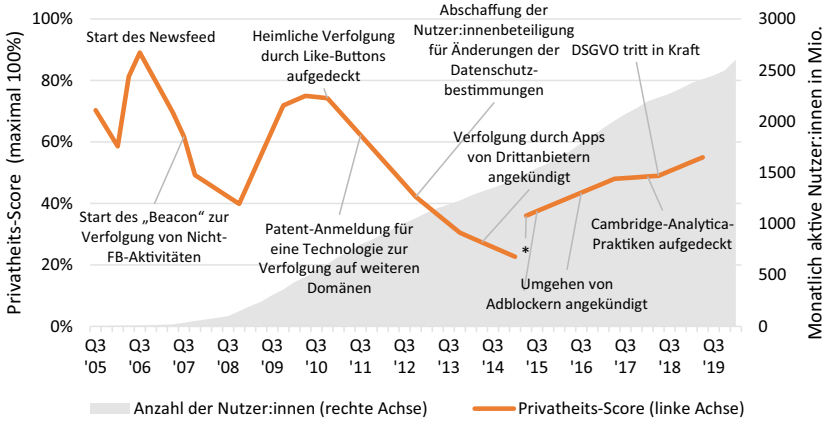


Abb. 2 Der Zusammenhang zwischen Nutzer:innenzahlen und der Datenschutzqualität bei Facebook. Anmerkung: *Wechsel der Datenquelle von Shore und Steinman (2015) [38] zu Ranking Digital Rights. (Quellen: Shore und Steinman [39], Ranking Digital Rights; Srinivasan [39]; Statista)

Datenschutz und rechtliche Vorgaben sind mindestens genauso relevant für die Qualität von Datenschutzbestimmungen.

Abgesehen vom Fall Facebook ist die empirische Evidenz für die Auswirkung der Marktkonzentration auf den Datenschutz sehr begrenzt. Eine aktuelle Studie zeigt, dass Unternehmen in stärker konzentrierten Anwendungsmärkten mehr personenbezogene Daten erheben als Unternehmen in weniger konzentrierten Märkten. Der Zusammenhang ist jedoch gering, sodass ein Unternehmen mit Marktmacht etwa 1–2 % mehr Datentypen sammelt als eines ohne.[14] Betrachtet man eine schrittweise Veränderung des Wettbewerbsumfelds bei Apps, die durch die Einführung neuer App-Kategorien im Android Play Store ausgelöst wurde, steigt der Zusammenhang auf 4–6 %, bleibt aber weiterhin begrenzt.[15]

[14] Kesler et al. (2019) [29], op. cit.

[15] Ergebnisse von App-Märkten sollten mit Vorsicht auf andere Märkte übertragen werden. Die Überforderung der Nutzer:innen durch eine hohe Anzahl von Apps könnte das sog. Privatheitsparadox verstärken, siehe z. B. Savage, S. J., und D. M. Waldman (2015) [37], „Privacy tradeoffs in smartphone applications".

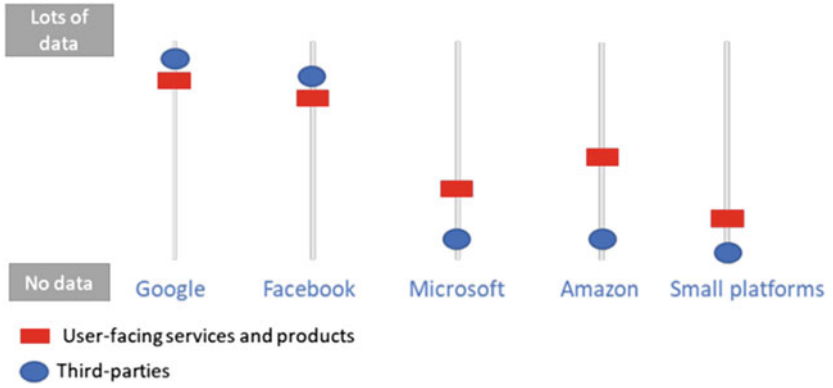


Abb. 3 Umfang der Datenerfassung durch ausgewählte Plattformenüber eigene Dienste und Drittquellen. (Quelle: Competition and Markets Authority [13])

Weitere, wenn auch keine die Kausalität offenlegende Evidenz hat die britische Competition and Markets Authority (CMA) in einer umfassenden Studie über Online-Werbung gesammelt. Darin stellt sie Folgendes fest:[16]

> [w]enn es mehr Auswahl für die Verbraucher gäbe, dann könnte es Spielraum für mehr Wettbewerb zwischen den Plattformen geben, da die Plattformen aktiver konkurrieren müssten, um die Verbraucher von den Vorteilen personalisierter Werbung zu überzeugen. Es gäbe auch Spielraum für andere Plattformen, die auf der Grundlage alternativer Geschäftsmodelle um die Verbraucher konkurrieren und verschiedene Optionen in Bezug auf die Wahl des Datenschutzes und die von ihnen angebotenen Dienste anbieten.

Diese Argumentation stützt sich weitgehend auf die qualitativen Ergebnisse, einschließlich ihrer Komplexität und der Wahrnehmung der Verbraucher:innen, „dass sie keine andere Wahl hatten, als sich trotz Bedenken für Dienste anzumelden“.[17] Bei der Bewertung der plattformübergreifenden Datenpraktiken stellt die CMA fest, dass Google und Facebook Zugang zu wesentlich mehr Daten haben als andere Plattformen, die Daten sammeln; siehe Abb. 3.

Darüber hinaus sind Google und Facebook die einzigen Plattformen, die der Studie zufolge noch mehr Daten über Drittquellen als über nutzerorientierte

[16] Competition and Markets Authority (2020) [13], „Online platforms and digital advertising. Market study final report“, Para 4.121. Eigene Übersetzung.

[17] Ebd., Para 4.117. Eigene Übersetzung.

Dienste und Produkte sammeln. Obwohl aus diesen Ergebnissen nicht auf einen kausalen Effekt der Konzentration auf die Datenerhebungspraktiken geschlossen werden kann, sind die Ergebnisse mit der Existenz eines solchen Effekts vereinbar.

Für ein besseres Verständnis der Wirkungsweise des Mechanismus z. B. auf verschiedenen Märkten sind weitere Studien erforderlich, die Marktkonzentration und Umfang der Datenerfassung empirisch untersuchen. Bei der Durchführung dieser Art von Studien ist bei der umgekehrten Kausalität besondere Vorsicht geboten. So könnte z. B. eine positive Korrelation zwischen Datenerlaubnissen und Konzentration auch durch die zunehmende Monetarisierung datenintensiver Anwendungen bedingt sein, die es ihnen wiederum ermöglichen könnte, mehr in die Verbesserung ihres Produkts zu investieren.

1.2 Hypothese 2: Wenn weniger Wettbewerb herrscht, haben Verbraucher:innen weniger Wahlfreiheit in Bezug auf die Privatsphäre

Haben Verbraucher:innen weniger Wahlfreiheit beim Datenschutz, wenn sie es mit einem Unternehmen zu tun haben, das nur wenige bzw. schwache Wettbewerber hat? Auch diese Frage stellte sich im Facebook-Verfahren spätestens seit dem Urteil des BGH. Die Antwort liegt auf der Hand: Weniger Wettbewerb bedeutet weniger Auswahl. Die Herausforderung besteht allerdings darin, klar zu konzeptualisieren, wann der Mangel an Wahlmöglichkeiten auch einen wettbewerbspolitischen Schaden darstellt. Konkret stellen das Bundeskartellamt[18] und der BGH[19] im Fall Facebook fest, dass die mangelnde Wahlfreiheit gegenüber einem marktbeherrschenden Unternehmen die informationelle Selbstbestimmung gefährdet und einen ausbeuterischen Missbrauch der Nutzer:innen darstellt. Wie bereits im vorigen Abschnitt ausgeführt, dürfte diese Feststellung auch für andere konzentrierte Märkte neben Facebook von hoher Relevanz sein.

Die Konzeptualisierung von Wahlfreiheit im Kontext von Privatsphäre und Wettbewerb baut auf dem Konzept der informationellen Selbstbestimmung und Wahlmöglichkeiten zwischen verschiedenen Optionen als Triebkraft des Wettbewerbs auf. Dies bedeutet, dass ein Mangel an Alternativen das Verhalten eines Unternehmens schon allein deshalb problematisch machen kann, weil das

[18] Bundeskartellamt (2019) [10], op. cit., Para 876.

[19] Bundesgerichtshof (2020) [9], op. cit., Para 103.

Unternehmen marktbeherrschend ist – selbst wenn sich sein Verhalten nicht systematisch von dem kleinerer Unternehmen unterscheidet (d. h. selbst dann, wenn der Zusammenhang aus dem vorherigen Abschnitt nicht gegeben ist). Insbesondere kann eine starke Marktstellung die Wahlfreiheit von Verbraucher:innen in Bezug auf den Datenschutz untergraben, weil diese der Möglichkeit beraubt werden, den Anbieter zu wechseln, um andere Datenschutzbestimmungen zu erhalten, und den Markt nur ganz „verlassen" können.

1.2.1 Evidenz

Um diesen Zusammenhang auf die tatsächlichen Märkte anwendbar zu machen, ist es wichtig zu definieren, was es für ein Unternehmen bedeutet, ausreichende Wahlmöglichkeiten hinsichtlich des Datenschutzes zu bieten, die dann das Mindestmaß an Wahlfreiheit gewährleisten. Erst dann ist klar, ob ein Unternehmen Schritte einleiten bzw. Aufsichtsbehörden eingreifen müssen, um die Wahlfreiheit zu erhöhen. Es ist z. B. nicht plausibel, dass marktmächtige Unternehmen mit hohen Datenschutzstandards verpflichtet werden sollten, den Verbrauchern mehr Wahlmöglichkeiten zu bieten, um mehr Daten zu teilen. Konkret sollte z. B. ein kostenpflichtiger Dienst nicht dazu verpflichtet werden, eine datenintensivere Variante ohne Bezahlung anzubieten.

Erstens ist ein Referenzpunkt nötig, um zu definieren, wann der Wettbewerb keine ausreichende Auswahl mehr bietet, sodass eine zusätzliche Prüfung der Datenschutzpraktiken erforderlich sei. Ein Ansatzpunkt könnte Marktmacht sein, ein etabliertes Konzept im Wettbewerbsrecht, allerdings sollte es möglicherweise verknüpfen mit der „Tracking-Intensität" verknüpft werden. Denn einige Unternehmen können „Datenmacht" erlangen, bevor sie die Schwelle zur Marktbeherrschung erreicht haben, während andere Unternehmen Marktmacht haben können, ohne nennenswert personenbezogene Daten zu erheben. Obwohl die Definition einer relevanten Schwelle nicht einfach ist, zeigen die aktuellen Diskussionen über Sonderregeln für Unternehmen mit Gatekeeper-Macht[20] oder

[20] Europäische Kommission (2020a) [21], „Digital Services Act package – ex ante regulatory instrument of very large online platforms acting as gatekeepers: open public consultation" und Europäische Kommission (2020b) [22], „Single Market – new complementary tool to strengthen competition enforcement: open public consultation".

marktübergreifender Bedeutung[21], dass es möglich ist, neue Konzepte zu entwickeln, die der Dynamik digitaler Märkte besser gerecht werden als etablierte Begriffe.

Zweitens ist es nötig zu definieren, welche Anforderungen das Verhalten dieser Firmen erfüllen muss, um eine ausreichende Wahlfreiheit zu bieten. Im Fall Facebook stellt der BGH fest, dass es eine wettbewerbswidrige Beschränkung der Wahlfreiheit darstellt, wenn Verbraucher:innen keine Wahl haben, ob sie eine Personalisierung auf der Grundlage von nur auf facebook.com oder auch von anderen Domains erhobenen Daten wünschen.[22] Implizit scheint in dieser Feststellung die Vorstellung enthalten, dass die Einwilligung der Verbraucher zur Legitimierung der Verarbeitung durch die Unternehmen nicht so freiwillig ist, wie sie sein sollte, um echte Wahlfreiheit zu ermöglichen. Andere schlagen vor, die Einwilligung als Rechtsgrundlage für die Verarbeitung von Daten durch datenmächtige Unternehmen aufzugeben, und meinen, dass „das Vorhandensein von Marktmacht im Sinne des Wettbewerbsrechts als Indikator dafür dienen kann, dass die Gültigkeit der Einwilligung als legitimer Grund für die Verarbeitung personenbezogener Daten infrage gestellt wird".[23] Ein ähnliches Argument wurde auch vom Europäischen Datenschutzbeauftragten vorgebracht.[24]

Es scheint angemessen, Wahlfreiheit gegenüber Firmen mit Datenmacht als zusätzliche Anforderung zur Einholung der Einwilligung zu konzipieren. Dieser Ansatz würde es Wettbewerbs- und Datenschutzbehörden ermöglichen, zu prüfen, ob solche Anforderungen erfüllt sind. Die Wahlfreiheit sollte die Verbraucher:innen in die Lage versetzen, klare Entscheidungen zu treffen. Wenn Unternehmen beispielsweise Nutzer:innen die Möglichkeit geben, die Datenschutzeinstellungen an ihre Präferenzen anzupassen (wobei alle Daten mit Ausnahme der für die Bereitstellung eines Dienstes erforderlichen Daten optional sind), profitieren Verbraucher:innen von der Datenschutzbestimmung, die ihren Präferenzen am besten entspricht.

---

[21] Siehe Furman, Jason et al. (2019) [24], „Unlocking digital competition" und Bundesministerium für Wirtschaft und Energie (2020) [11], „Gesetzentwurf: Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0", Artikel 19a.

[22] Bundesgerichtshof (2020) [9], op. cit., Para 58.

[23] Graef et al. (2018) [25], op. cit., 207.

[24] EDPS (2014) [20], op. cit., 35.

1.3 Handlungsoptionen

Es wird deutlich, dass ein Effekt von Marktkonzentration auf die Datenpraktiken eines Unternehmens nur unzureichend empirische untersucht und gestützt ist. Das konzeptionelle Argument, dass Verbraucher:innen weniger Wahlfreiheit haben, ist prinzipiell plausibel, erfordert allerdings eine weitere Ausarbeitung. Daraus lassen sich eine Reihe von Handlungsempfehlungen ableiten.

1.3.1 Mehr empirische Forschung

Es gibt nur begrenzte empirische Belege dafür, ob Unternehmen weniger personenbezogene Daten erheben, wenn sie einem stärkeren Wettbewerb ausgesetzt sind, und mit der derzeit verfügbaren Datenmenge sind Belege nur schwer zu erhalten. Wissenschaftler:innen sollten verstärkt untersuchen, ob Unternehmen mit Marktmacht mehr oder sensiblere Daten sammeln als Unternehmen ohne Marktmacht. Diese Untersuchung ist nur möglich, wenn Zugang zu wesentlich mehr Daten über die Praktiken der Plattformen besteht. Behörden und statistische Ämter sollten digitale Plattformen verpflichten, mehr Daten auszutauschen, um eine systematische Analyse ihrer Auswirkungen auf die Privatsphäre zu ermöglichen.[25]

1.3.2 Austausch zwischen Wettbewerbs- und Datenschutzaufsicht

Datenschutz- und Wettbewerbsexpert:innen sollten gemeinsam den Begriff der Wahlfreiheit stärker ausarbeiten. Da sie ein gemeinsames Ziel der Wettbewerbs- und Datenschutzpolitik ist, ist es wichtig, zu einem klareren gemeinsamen Verständnis dessen zu gelangen, was es für ein Unternehmen bedeutet, Wahlfreiheit in Bezug auf den Datenschutz anzubieten. Dies erfordert die Einbeziehung von Datenschutz- und Wettbewerbsexpert:innen, zum Beispiel auf der Grundlage der Vorstellung, dass der Anwendungsbereich des Wettbewerbsrechts auch breitere soziale Auswirkungen von Märkten einschließen sollte,[26] sowie einen kooperativen Ansatz zwischen den Behörden.[27]

[25] Expert Group for the Observatory on the Online Platform Economy (2020) [23], „Progress Report Expert Group for the Observatory on the Online Platform Economy Work stream on Measurement & Economic Indicators“.

[26] Lianos, Ioannis (2018) [33], „Polycentric Competition Law“.

[27] Binns und Bietti (2020) [3], op. cit.

1.3.3 Sicherstellung der Wahlfreiheit

Aufbauend auf einem klareren Begriff der Wahlfreiheit können Mechanismen entwickelt werden, die gegenüber marktbeherrschenden Unternehmen eine Wahlfreiheit gewährleisten. Diese Wahlfreiheit sollte eine Alternative darstellen zu der aktuellen Einwilligung in zahlreiche Datensammelpraktiken eines einzelnen Anbieters. Stattdessen können zusätzliche Anforderungen an marktbeherrschende Unternehmen, die sich auf die Einwilligung als rechtliche Grundlage für die Datenverarbeitung stützen, formuliert werden. Dies wäre Ausdruck der besonderen Verantwortung mächtiger Unternehmen, dafür zu sorgen, dass die Nutzer:innen bei Entscheidungen über ihre Privatsphäre weiterhin Wahlfreiheit haben. Es gibt verschiedene Optionen:

- Einbeziehung der Verbraucher:innen in die Entwicklung von Datenschutzbestimmungen: Dies würde einen Teil der Last der Einwilligung in ein früheres Stadium verlagern, in dem den Verbraucher:innen ein wirklicher Einfluss auf das Ergebnis gegeben werden müsste. Facebook versuchte in der Vergangenheit demokratische Entscheidungsfindung bezüglich der Verwendung persönlicher Daten, gab diese Praxis jedoch auf. Alternativen oder Ergänzungen können Formen der Zustimmung der Gemeinschaft sein, z. B. durch die Einbeziehung von Ethikkommissionen, Bürgerjurys, Umfragen oder offene Diskussionen über die Bewertung legitimer Interessen[28] oder auch bestehende Repräsentanten wie Verbraucherzentralen.
- Entflechtung der Einwilligung und Entflechtung von Daten: Wie das Bundeskartellamt von Facebook verlangte, könnten marktbeherrschende Unternehmen verpflichtet werden, eine detailliertere Einwilligung der Verbraucher:innen einzuholen. Konkret könnte dies bedeuten, dass Verbraucher:innen die Möglichkeit eingeräumt wird, nur die Daten weiterzugeben, die für die Erbringung eines Dienstes erforderlich sind, wobei die aus anderen Quellen erhobenen Daten optional sind. Dieser Ansatz erfreut sich nicht nur bei Datenschutz, sondern auch bei Wettbewerbsökonom:innen zunehmender Beliebtheit.[29] Dabei ist es jedoch wichtig, eine Intervention so zu gestalten, dass die bekannten Probleme der Einwilligung der DSGVO vermieden werden. So kann die DSGVO die Konzentration verstärken, und die Zustimmung kann von großen und etablierten Unternehmen leichter eingeholt werden, weil sie dazu neigen,

[28] Tennison, Jeni (2017) [40], „Community consent“, 17 Januar.

[29] Condorelli, Daniele und Jorge Padilla (2019) [14], „Data-Driven Predatory Entry with Privacy-Policy Tying“.

größere Marktsegmente zu bedienen,[30] und weil Verbraucher:innen aufgrund der Bekanntheit großer Unternehmen weniger auf deren Datenpraktiken reagieren.[31]

Jede dieser Optionen ist mit geltendem Recht kompatibel und würde eine Verbesserung gegenüber dem Status Quo darstellen. Besonders effektiv werden die Maßnahmen allerdings in Verknüpfung miteinander, also z. B. bessere Kennzahlen, die sowohl von Datenschutz- als auch von Wettbewerbsbehörden konsistent angewandt würden.

2 Was für einen Wettbewerb um verbraucher:innenfreundlichere Datenschutzbestimmungen fehlt

Die Betrachtung der zwei Zusammenhänge zeigt, dass das Fehlen von Wettbewerb den Schutz der Privatsphäre beeinträchtigen kann und dass dies v. a. bei einer Beschränkung der Wahlfreiheit problematisch ist. Allerdings ist Marktkonzentration nicht der einzige Grund für problematische Datenschutzpraktiken. Auch auf stärker wettbewerblichen Märkten gibt es kaum datenschutzfreundliche Angebote, die mit datenintensiven Diensten konkurrieren. Gleichzeitig äußern Verbraucher:innen konsequent und in zunehmendem Maße Sorgen über die weit verbreitete Datenerfassung. Warum versuchen Unternehmen nicht, sich stärker über besseren Datenschutz von ihren Wettbewerbern zu differenzieren?

Es gibt strukturelle Hindernisse für einen stärkeren Wettbewerb um besseren Datenschutz. Diese liegen sowohl auf der Seite der Verbraucher:innen als auch auf der der Unternehmen. Trotz den in der DSGVO festgeschriebenen Datenrechten ist es für Verbraucher:innen immer noch völlig unpraktikabel, umfassend Transparenz und Kontrolle darüber zu erhalten, was mit den oft sehr detaillierten Profilen über sie geschieht. Die Komplexität der Datenmärkte, auf denen personenbezogene Daten gehandelt werden, führt dazu, dass Verbraucher:innen erhebliche Anstrengungen unternehmen müssten, um die Auswirkungen ihrer Einwilligung in selbst eine einzelne Datenschutzbestimmung zu verstehen. Selbst

[30] Campbell et al. (2015) [12], „Privacy regulation and market structure“.

[31] Verbraucher:innen laden allgemein weniger Apps herunter, wenn diese mehr sensible Datenpunkte anfordern; dieser Zusammenhang besteht allerdings nicht für Apps von bekannten Marken. Siehe Kummer, Michael und Patrick Schulte (2019) [31], „When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications“.

wenn sie diese im Einzelfall auf sich nähmen, hätten sie nur dann Aussicht auf erfolgreichen Schutz ihrer Privatsphäre, wenn sie es bei der Vielzahl solcher Bestimmungen tun, die sich auf sie auswirken.

2.1 Hürden für Verbraucher:innen

Dass Verbraucher:innen vor dieser Komplexität oft resignieren, kann nicht als Beleg dafür gesehen werden, dass sie ihrer Privatsphäre keinen hohen Wert beimessen. Die Herausforderung besteht vielmehr darin, überhaupt aussagekräftige Datenpunkte für diesen Wert zu generieren. Es gibt mindestens drei Umstände, die dies verkomplizieren:

- Privatsphäre und Datenschutz sind von Natur aus komplexer und kontextabhängiger als andere Merkmale von Produkten. Das führt zu inkonsistenteren Entscheidungen, als in anderen Kontexten der Fall ist.[32]
- Verbraucher:innen haben das Vertrauen verloren und fühlen sich machtlos, wenn es darum geht, wirksame Datenschutzentscheidungen zu treffen, da die Märkte für personenbezogene Daten sehr intransparent sind, Unternehmen ihre Versprechen in Bezug auf Datenschutz leicht brechen können und es immer wieder zu Datenschutzskandalen kommt.
- (Einige) Unternehmen machen es Verbraucher:innenn absichtlich schwer, wirksame Datenschutzentscheidungen zu treffen, indem sie die ersten beiden Punkte verstärken, z. B. indem sie unnötig obskure Sprache oder sog. Dark Patterns verwenden.

Im Ergebnis sind Verbraucher:innen vielen Datenpraktiken geradezu ausgeliefert. Selbst in relativ einfachen Kontexten zeigen Experimente, dass Verbraucher:innen Schwierigkeiten haben, Entscheidungen zu treffen, die tatsächlich ihren Präferenzen entsprechen, und dass diese Präferenzen kontextabhängig sind.[33]

[32] Siehe Winegar, Angela G. und Cass R. Sunstein (2019) [42], „How much is data privacy worth? A preliminary investigation".

[33] Ein signifikanter Anteil der Testpersonen gibt an, dass ihre gewählten Datenschutzeinstellungen nicht ihren eigentlichen Wünschen entsprechen, siehe Nouwens, Midas et al. (2020) [35], „Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence".

2.2 Hürden für Unternehmen

Auf der Seite der Unternehmen gibt es einen Zielkonflikt zwischen Datenschutz und Monetarisierung, der sie oft davon abhält, datenschutzfreundlichere Produkte anzubieten. Dies ist insbesondere dann der Fall, wenn datenschutzfreundliche Anbieter im Wettbewerb stehen mit etablierten Unternehmen, die eine aggressive Monetarisierung persönlicher Daten verfolgen, insbesondere durch gezielte Werbung (und/oder andere Formen der Personalisierung, wie z. B. personalisierte Empfehlungen). Datenschutzfreundliche Anbieter müssen ein Geschäftsmodell finden, das trotz einer geringeren Rentabilität pro Nutzer:in kommerziell tragfähig ist.

Diese Abwägung zwischen Datenschutz und Monetarisierung gilt für kleine und große Unternehmen gleichermaßen, wobei er prinzipiell besonders herausfordernd ist für Unternehmen, die sich gegen etablierte Datenhändler durchsetzen wollen. Start-ups, die wachsen wollen, entscheiden sich oft gegen Tracking und Werbung, zumindest anfänglich, und sind auf andere Monetarisierungsquellen wie externe Finanzierung angewiesen. Aber auch Facebook wies 2018 nach den Enthüllungen von Cambridge Analytica darauf hin, dass „die Produktentwicklung, bei der die Privatsphäre an erster Stelle steht", „einen gewissen Einfluss auf das Umsatzwachstum" habe.[34]

Zwar können bestimmte Geschäftsmodelle bei geringerer Rentabilität immer noch kommerziell tragfähig sein, doch stehen sie Einschränkungen gegenüber, die für Firmen mit aggressiver Monetarisierung nicht gelten. Wenn zum Beispiel über eine Auktion bestimmt wird, welche Suchmaschinen in einem Menü erscheinen, das die Verbraucher bei der Konfiguration neuer Geräte und Browser sehen, ist es unwahrscheinlich, dass datenschutzfreundliche Suchmaschinen erscheinen.[35] Stattdessen werden Auktionen wahrscheinlich den Wettbewerb zwischen Anbietern, die personenbezogene Daten aggressiv monetarisieren, verschärfen, da sie es sich leisten können, bei einer solchen Auktion mehr für die Akquise weiterer Nutzer:innen auszugeben. Dabei gibt es gerade im Zusammenhang mit Suchmaschinen recht zuverlässig eine Nachfrage nach besserem Schutz der Privatsphäre – rund 30 % der Verbraucher:innen aus Deutschland, dem Vereinigten Königreich, den USA und Australien gaben an, dass eine Suchmaschine, die auf die

[34] The Motley Fool (2018) [34], „Facebook, Inc. (FB) Q2 2018 Earnings Conference Call Transcript". Eigene Übersetzung.

[35] DuckDuckGo Blog (2020a) [18], „Search Preference Menus: No Auctions Please".

Erhebung personenbezogener Daten über Suchanfragen verzichtet, sie dazu motivieren würde, die Suchmaschine zu wechseln, als zweitwichtigster Faktor nach der Qualität der Ergebnisse.[36]

Neben fehlendem Wettbewerb tragen also weitere Faktoren marktübergreifend dazu bei, dass kaum effektiver Wettbewerb um den Parameter Datenschutz entsteht. Verbraucher:innen fehlen Transparenz und Kontrolle, während Unternehmen sich aus kommerziellen Motiven für eine stärkere Datennutzung entscheiden.

2.3 Handlungsoptionen

Welche Schritte sind sinnvoll, um diese Hürden für einen wirksameren Wettbewerb um besseren Datenschutz abzubauen? Es gibt eine Bandbreite an Maßnahmen, die es Verbraucher:innen einfacher machen sollen, effektivere Entscheidungen über ihre Privatsphäre zu treffen, und zugleich Unternehmen Anreize setzen können, einen besseren Schutz der Privatsphäre anzubieten.

2.3.1 Mehr Transparenz

Die DSGVO enthält bereits zahlreiche Klauseln, mit denen mehr Transparenz bei Datenschutzbestimmungen durchgesetzt werden kann. Es ist beispielsweise die Möglichkeit vorgesehen, standardisierte Klauseln,[37] maschinenlesbare Datenschutzsymbole[38] und Zertifizierungen zu entwickeln.[39] Jede Maßnahme für sich hätte vermutlich nur begrenzte Auswirkungen, doch eine Kombination könnte einen ersten Schritt zur Erleichterung des Verständnisses und des Vergleichs von Datenschutzbestimmungen darstellen. Sie bringen Herausforderungen mit sich, wie z. B. die Schwierigkeit, die Komplexität auf eine Art und Weise zu reduzieren, die nicht irreführend oder anfällig für Unterminierung durch Firmen ist.

[36] DuckDuckGo Blog (2020b) [19], „Search Preference Menu Immediately Increases Google Competitors' Market Share by 300–800 %“, https://spreadprivacy.com/search-engine-preference-menu/.

[37] Artikel 28 und 46 DSGVO.

[38] Artikel 12 DSGVO.

[39] Artikel 93 DSGVO.

Möglicherweise könnten sie auch auf Datenschutzmetriken für Expert:innen aufbauen (s. o.).[40] Transparenz kann ein geeigneterer Weg sein, die Privatsphäre zu stärken, statt (nur) auf strengere Vorschriften zurückzugreifen.[41]

2.3.2 Mehr Portabilität

Eine Stärkung der Datenportabilität über das Niveau der DSGVO, Artikel 20, hinaus kann Verbraucher:innen mehr Kontrolle darüber zu geben, wie Daten über sie verwendet werden und einen nutzer:innenzentrierten Wettbewerb anzuregen. Die Datenportabilität sollte in Echtzeit erfolgen, ein breites Spektrum von Daten umfassen (wie z. B. bestimmte Arten inferierter Daten) und Nutzer:innen sollten in der Lage sein, Daten direkt zwischen Plattformen zu portieren. Damit kann datenbedingte Wechselträgheit überwunden werden z. B. für Empfehlungssysteme oder Standorthistorie in Kartenapps. Es ist möglich, dass eine Ausgestaltung der Portabilität an markt- bzw. sektorspezifische Gegebenheiten angepasst werden muss, um ein ausreichendes Maß an Mitsprache für Verbraucher:innen sicherzustellen; dies kann auf einem Spektrum passieren, das von Datenportabilität bis zur Protokoll- und Dateninteroperabilität reicht.[42] Ein möglicher Ansatz besteht darin, über den geplanten Digital Services Act zunächst große Plattformen zu einer Echtzeitportabilität zu verpflichten, um v. a. die Wechselhürden hin zu kleineren Wettbewerbern zu verringern.[43]

2.3.3 Neue Dateninstitutionen/Datentreuhänder

Um langfristig Verbraucher:innen zu entlasten, während gleichzeitig Wettbewerb um besseren Datenschutz zu stärken, bedarf es weitergehender Veränderungen in der Datenökonomie. Ein möglicher Ansatz hierfür können neue Dateninstitutionen

---

[40] Die zentrale Zielgruppe für diese Kennzahlen sollten Expert:innen sein, da Verbraucher:innen oft andere Kennzahlen und Formate benötigen, um die Bedeutung für ihre Privatsphäre zu verstehen. Siehe z. B. Ben-Shahar, Omri und Adam Chilton (2016) [2], „Simplification of privacy disclosures: an experimental test“ und Conpolicy (2018) [15], „Wege zur besseren Informiertheit. Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des OnePager-Ansatzes und weiterer Lösungsansätze im Datenschutz“.

[41] Ökonomische Modelle zeigen, dass Transparenz zu besseren Marktergebnissen führt al sein vorgeschriebenes Maß an Datennutzung, siehe de Cornière, Alexandre und Taylor, Greg (2020) [17], „Data and Competition: a General Framework with Applications to Mergers, Market Structure, and Privacy Policy“.

[42] Crémer, J. et al. (2019) [16], „Competition Policy for the Digital Era“.

[43] Siehe Europäische Kommission (2020a) [21], op. cit., und Blankertz, A. und Julian Jaursch (2020) [6], „Beitrag zur Konsultation der Europäischen Kommission zum Digital Services Act (DSA)“.

sein, insbesondere Datentreuhänder.[44] Eine Form kollektiven Verhandelns über die Bedingungen von Datenaustausch von Individuen und Unternehmen könnte Verbraucher:inneninteressen deutlich effektiver durchsetzen, als es mit aktuellen Datenrechten unter der DSGVO möglich ist, und könnte mehr Unternehmen Zugang gewährleisten, als momentan der Fall ist. Hierzu sind weitere konzeptionelle Arbeit und praktische Erprobung nötig, bevor solche Modelle sich zu realistischen Alternativen auf digitalen Märkten entwickeln können.

Literatur

1. Albergotti, R.: „Calls grow for European regulators to investigate Apple, accused of bullying smaller rivals“, The Washington Post, 28. Mai. https://www.washingtonpost.com/technology/2020/05/28/tile-tells-vestager-investigate-apple-antitrust-violations/ (2020). Zugegriffen: 7. Dez. 2020
2. Ben-Shahar, O., Chilton, A.: Simplification of privacy disclosures: an experimental test. J. Leg. Stud. **45**(S2), 41–67 (2016). https://doi.org/10.1086/688405
3. Binns, R., Bietti, E.: Dissolving privacy, one merger at a time: competition, data and third party tracking. Comput. Law Secur. Rev. **37**, 105369 (2020). https://doi.org/10.1016/j.clsr.2019.105369
4. Blankertz, A.: „Designing data trusts. Why we need to test consumer data trusts now“, Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/designing_data_trusts_d.pdf (2020a)
5. Blankertz, A.: „How competition impacts privacy. And why competition authorities should care“, Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/how_competition_impacts_data_privacy_deu.pdf (2020b)
6. Blankertz, A., Jaursch, J.: „Beitrag zur Konsultation der Europäischen Kommission zum Digital Services Act (DSA)“. https://www.stiftung-nv.de/de/publikation/beitrag-zur-konsultation-der-europaeischen-kommission-zum-digital-services-act-dsa (2020)
7. Bovard, R. „Why Google's new limits on third-party cookies are another attempt to control the web“, the federalist, 17. Februar. https://thefederalist.com/2020/02/17/why-googles-new-limits-on-third-party-cookies-are-another-attempt-to-control-the-web/ (2020)
8. Bria, F., Caffarra, C., Crawford, G., Christl, W., Duso, T., Ryan, J., Valletti, T.: „Europe must not rush Google-Fitbit deal“, Politico, 23. Juli. https://www.politico.eu/article/europe-must-not-rush-google-fitbit-deal-data-privacy/ (2020)
9. Bundesgerichtshof: Beschluss zu KVR 69/19, 23. Juni. https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=109506 (2020)
10. Bundeskartellamt: Beschluss des Bundeskartellamts zu B6-22/16 (Facebook). https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=8 (2019)

[44] Blankertz, Aline (2020a) [4], „Designing Data Trusts. Why We Need to Test Consumer Data Trusts Now“.

11. Bundesministerium für Wirtschaft und Energie: „Gesetzentwurf: Entwurf eines Zehnten Gesetzes zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0“. https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/gesetzentwurf-gwb-digitalisierungsgesetz.pdf?__blob=publicationFile&v=6 (2020)
12. Campbell, J., Goldfarb, A., Tucker, C.: Privacy regulation and market structure. J. Econ. Manag. Strateg. **24**(1), 47–73 (2015). https://doi.org/10.1111/jems.12079
13. Competition and Markets Authority: „Online platforms and digital advertising. Market study final report“, 1. Juli. https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf (2020)
14. Condorelli, D., Padilla, J.: „Data-driven predatory entry with privacy-policy tying“. https://doi.org/10.2139/ssrn.3600725 (2019)
15. Conpolicy: „Wege zur besseren Informiertheit. Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des OnePager-Ansatzes und weiterer Lösungsansätze im Datenschutz“. https://www.conpolicy.de/aktuell/wege-zur-besseren-informiertheit-verhaltenswissenschaftliche-ergebnisse-zur-wirksamkeit-des-one-pag/ (2018)
16. Crémer, J., de Montjoye, Y., Schweitzer, H.: „Competition policy for the digital era“, European Commission. https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf (2019)
17. de Cornière, A., Taylor, G.: „Data and competition: a general framework with applications to mergers, market structure, and privacy policy“, TSE Working Papers 20-1076. https://www.tse-fr.eu/sites/default/files/medias/doc/wp/io/wp_tse_1076.pdf (2020)
18. DuckDuckGo Blog: „Search preference menus: no auctions please“. https://spreadprivacy.com/search-preference-menu-auctions/ (2020a)
19. DuckDuckGo Blog: „Search preference menu immediately increases Google competitors' market share by 300–800 %“. https://spreadprivacy.com/search-engine-preference-menu/ (2020b)
20. EDPS: „Privacy and competitiveness in the age of big data: the interplay between data protection, competition law and consumer protection in the Digital Economy“, European Data Protection Supervisor. https://edps.europa.eu/sites/edp/files/publication/14-03-26_competitition_law_big_data_en.pdf (2014)
21. Europäische Kommission: „Digital Services Act package – ex ante regulatory instrument of very large online platforms acting as gatekeepers: open public consultation“. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12418-Digital-Services-Act-package-ex-ante-regulatory-instrument-of-very-large-online-platforms-acting-as-gatekeepers (2020a)
22. Europäische Kommission: „Single market – new complementary tool to strengthen competition enforcement: open public consultation“. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12416-New-competition-tool/public-consultation (2020b)
23. Expert Group for the Observatory on the Online Platform Economy: „Progress report expert group for the observatory on the online platform economy work stream on measurement & economic indicators“, European Commission. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=68357 (2020)
24. Furman, J., Coyle, D., Fletcher, A., Marsden, P., McAuley, D.: „Unlocking digital competition“, report of the digital competition expert panel. https://assets.publishing.ser

vice.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf (2019)
25. Graef, I., Clifford, D., Valcke, P.: Fairness and enforcement: bridging competition, data protection and consumer law. Int. Data Priv. Law **8**(3), 200–223 (2018). https://doi.org/10.1093/idpl/ipy013
26. Information Technology and Innovation Foundation: Response to „the intersection between privacy, big data and competition, data as a dimension of competition, and/or as an impediment to entry into or expansion within a relevant market". https://www.ftc.gov/system/files/documents/public_comments/2018/08/ftc-2018-0051-d-0036-154929.pdf (2018)
27. Kemp, K.: Concealed data practices and competition law: why privacy matters. Eur. Compet. J. **16**(2–3), 628–672 (2020a). https://doi.org/10.1080/17441056.2020.1839228
28. Kemp, K.: „Every step you take: why Google's plan to buy fitbit has the ACCC's pulse racing", the conversation, 23. Juni. https://theconversation.com/every-step-you-take-why-googles-plan-to-buy-fitbit-has-the-accs-pulse-racing-141052 (2020b)
29. Kesler, R., Kummer, M., Schulte, P.: „Competition and privacy in online markets: evidence from the mobile app industry", ZEW Discussion Paper 19-064. https://madoc.bib.uni-mannheim.de/54510 (2019)
30. Körber, T.: „‚Ist Wissen Marktmacht?' Überlegungen zum Verhältnis von Datenschutz, ‚Datenmacht' und Kartellrecht – Teil 1", Neue Zeitschrift für Kartellrecht 2016, 303–348 (17). https://koerber.jura.uni-koeln.de/sites/koerber/user_upload/Verlinkte_Dateien/Koerber_NZKart_2016__303-310.pdf (2018)
31. Kummer, M., Schulte, P.: When private information settles the bill: money and privacy in Google's market for smartphone applications. Manag. Sci. **65**(8), 3470–3469 (2019). https://doi.org/10.1287/mnsc.2018.3132
32. Lardinois, F.: „Google wants to phase out support for third-party cookies in chrome within two years", TechCrunch, 14. Januar. https://techcrunch.com/2020/01/14/google-wants-to-phase-out-support-for-third-party-cookies-in-chrome-within-two-years/ (2020)
33. Lianos, I.: Polycentric competition law. Curr. Leg. Probl. **71**(1), 161–213 (2018). https://doi.org/10.1093/clp/cuy008
34. The Motley Fool: „Facebook, Inc. (FB) Q2 2018 earnings conference call transcript". https://www.nasdaq.com/articles/facebook-inc-fb-q2-2018-earnings-conference-call-transcript-2018-07-25 (2018)
35. Nouwens, Midas, Liccardi, I., Veale, M., Karger, D., Kagal, L.: Dark patterns after the GDPR: scraping consent pop-ups and demonstrating their influence. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (2020). https://doi.org/10.1145/3313831.3376321
36. Oberlandesgericht Düsseldorf: Beschluss zu Vi-Kart 1/19 (V), 26. August. https://openjur.de/u/2179185.html (2019)
37. Savage, S.J., Waldman, D.M.: Privacy tradeoffs in smartphone applications. Econ. Lett. **137**, 171–175 (2015). https://doi.org/10.1016/j.econlet.2015.10.016
38. Shore, J., Steinman, J.: „Did You Really Agree to That? The Evolution of Facebook's Privacy Policy", Technology Science (2015).
39. Srinivasan, D.: The antitrust case against Facebook: a monopolist's journey towards pervasive surveillance in spite of consumers' preference for privacy. Berkeley Bus. Law J. **16**(1), 39–101 (2019)

40. Tennison, J.: „Community consent“, 17 January. https://www.jenitennison.com/2020/01/17/community-consent.html (2020)
41. Townley, C., Morrison, E., Yeung, K.: Big data and personalised price discrimination in EU competition law. Yearb. Eur. Law **36**, 683–748 (2017). https://doi.org/10.1093/yel/yex015
42. Winegar, A.G., Sunstein, C.R.: How much is data privacy worth? A preliminary investigation. J. Consum. Policy **42**, 425–444 (2019). https://doi.org/10.1007/s10603-019-09419-y
43. Die ZEIT: „Kartellamt bremst Facebook beim Sammlen von Nutzerdaten“, 7. Februar. https://www.zeit.de/news/2019-02/07/kartellamt-bremst-facebook-beim-sammlen-von-nutzerdaten-190207-99-883808 (2019)

Privatheit in Zeiten der umfassenden Digitalisierung

Datenbasierte Sichtbarkeit: Gesellschaftsstrukturelle Bedingungen zeitgenössischer Technikgestaltung

Carsten Ochs

Zusammenfassung

Dass wertorientierte Technikgestaltung kaum umhinkommt, die gesellschaftsstrukturellen Bedingungen mit zu reflektieren, unter denen sie agiert, ist bekannt. Der Vortrag überträgt diese Einsicht auf den Bereich der Privatheit, indem er die strukturhistorischen Konstellationen rekonstruiert, aus denen sich versch. Formen der informationellen Privatheit in unterschiedlichen Vergesellschaftungsphasen der Moderne jeweils herausgeschält haben. Bei den so identifizierten Privatheitsformen handelt es sich um a) *Reputation Management;* b) Rückzug; sowie c) individuelle Informationskontrolle. Basierend auf einer solchen Genealogie informationeller Privatheitspraktiken werden in einem weiteren Schritt die strukturellen Treiber zeitgenössischer Privatheit herausgearbeitet, deren Form solchermaßen als d) Unschärfegarantie erkennbar wird. Abschließend werden Konsequenzen diskutiert, die sich aus den somit herausgearbeiteten gesellschaftsstrukturellen Bedingungen zeitgenössischer Technikgestaltung ergeben.

Schlüsselwörter

Digitalisierung • Geschichte der Privatheit • Datenökonomie

C. Ochs (✉)
Universität Kassel, Kassel, Deutschland
E-Mail: Carsten.ochs@uni-kassel.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_3

1 Einleitung

Dass wertorientierte Technikgestaltung gut daran tut, die gesellschaftsstrukturellen Bedingungen der Technikgenese zu reflektieren, ist bekannt. Das gilt insbesondere im Bereich des Datenschutzes, in dem sich diese Vorstellung schon seit längerem im *Privacy by Design*-Paradigma artikuliert. Die Europäische Datenschutzgrundverordnung etwa spezifiziert in Artikel 25 unter der Überschrift „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen", dass die für das Betreiben digitaler Infrastrukturen Verantwortlichen „geeignete technische und organisatorische Maßnahmen" zu treffen hätten, „die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen" [12, S. 48]. Was unter „geeigneten" Maßnahmen zu verstehen ist, variiert jedoch gesellschaftsgeschichtlich, und das gleiche gilt wohl für angemessene „Datenschutzgrundsätze."

Beim vorliegenden Beitrag handelt es sich um den Versuch, soziologisch Auskunft über diese historische Variabilität zu geben. Das Ziel besteht darin, den eher gestalterisch orientierten Disziplinen und Praktiken der Rechtssetzung und -sprechung, des Datenschutzes, der politischen Regulierung sowie der Informatik und den Technikwissenschaften das *big picture* der kulturhistorischen Genese informationeller Privatheit als Reflexionsfolie für die jeweiligen Gestaltungspraktiken zur Verfügung zu stellen. Zu diesem Zweck rekonstruiert der Beitrag in aller Knappheit die historisch entwickelten strukturellen gesellschaftlichen Konstellationen, aus denen sich verschiedene Formen der informationellen Privatheit in unterschiedlichen Vergesellschaftungsphasen der Moderne jeweils herausgeschält haben. Das historische Narrativ, das in diesem Zuge entfaltet wird, ist ein dezidiert euro-amerikanisches: Ob und inwiefern sich ähnliche sozialhistorische Prozesse auch mit Blick auf andere Weltregionen rekonstruieren lassen, bleibt hier offen, die euro-amerikanische Entwicklungsgeschichte wird also ausdrücklich in ihrer Spezifik betrachtet und *nicht* universalisiert. Solchermaßen kulturhistorisch verortet, wird zunächst im Rahmen einer theoretisch-sozialhistorischen Klärung der geschichtliche Einstiegspunkt der Rekonstruktion identifiziert (2), bevor dann die informationellen Privatheitsformen des 18. (3), 19. (4), 20. (5) und 21. Jahrhunderts (6) sowie deren strukturelle Entwicklungstreiber rekonstruiert werden. Im Schlusskapitel (7) werden schließlich einige Konsequenzen andiskutiert, die sich aus der Rekonstruktion ergeben.

2 Privatheit als Subjektivierungsmodus: Zur Vorgeschichte informationeller Teilhabebeschränkung

Die Frage, worum es sich bei Privatheit genau handelt, und wie eine definitorische Bestimmung aussehen könnte, ist seit Jahrzehnten virulent und, sofern überhaupt beantwortet, so doch sicherlich nicht zur Zufriedenheit aller Diskursteilnehmenden, weshalb manche ihre Definitionsfähigkeit gleich generell anzweifeln [62]. Da hier nicht der Ort ist, um die konzeptuellen Problemlagen zu skizzieren, werde ich im Folgenden auf einer anderen, theoretischen Arbeit aufbauen [43] und einfach axiomatisch feststellen, dass (u. a.) informationelle Privatheit stets darauf abzielt, die *Teilhabe* von Akteur(en) B an den Informationen über (einen) andere(n) Akteur(e) A zu *beschränken,* um A einen *Erfahrungsspielraum* zu sichern, der ansonsten keinen Bestand hätte. Egal ob es sich bei B um Voyeure, Geheimdienste oder Internetkonzerne handelt, sie alle verzerren den Erfahrungsspielraum As, wenn sie aus Daten Informationen über A gewinnen, auf diese Weise also an (Informationen über) A teilhaben, um sich selbst *als Voyeure, Geheimdienste, Internetkonzerne zu konstituieren* (unabhängig davon, ob A davon weiß), und zwar indem sie die vorab nicht festgelegte Gesamtheit möglicher Erfahrungstypen – den Spielraum – beschneiden: Ein Internetkonzern beispielsweise, der mithilfe von Daten Informationen über mich generieren will, um sich so als Verhaltensvorhersager oder -manipulator zu konstituieren, könnte meinen Erfahrungsspielraum beschneiden, indem er mir Flugreisen unmöglich macht, Jobchancen vorbestimmt, Versicherungsoptionen entzieht usw. In diesem Sinne handelt es sich bei informationeller Privatheit um Teilhabebeschränkung zur Gewährleistung von Erfahrungsspielräumen.

Anstatt weiterführende theoretische Überlegungen anzustellen, möchte ich an dieser Stelle nun einen sozialhistorischen Argumentationsgang präsentieren, der der Frage folgt, zu welchen Zeitpunkten informationelle Teilhabebeschränkungen auf welche Weise und aus welchen gesellschaftsstrukturellen Gründen *als informationelle Privatheit* formatiert worden sind. Wo wäre diesbezüglich überhaupt historisch einzusetzen? Und welche gesellschaftlichen Konstellationen und informationellen Privatheitstypen lassen sich identifizieren?

Während Historiker:innen die klassische Sichtweise, dass informationelle Privatheit mit der bürgerlichen Moderne im 18. Jahrhundert entsteht, wiederholt infrage gestellt haben [59], [67], lassen sich doch erhebliche Differenzen zwischen modernen und vorherigen Privatheitsformen ausmachen. Unter vormodernen Bedingungen sind Privatheitsrechte immer an das Wohneigentum gebunden, und nicht an individuelle Einzelpersonen [59, S. 459] [67, S. 6]. Techniken der

informationellen Teilhabebeschränkung dienen m.a.W. erst ab dem 18. Jahrhundert dem Zweck individualistischer Selbst-Konstitution. Vier strukturelle Gründe zeichnen dafür verantwortlich: *Erstens* prämiert das vormoderne Ständesystem statische Reproduktion bestehender Verhältnisse [21], [47], [57], während die Moderne auf dynamische Innovation setzt [51]. *Zweitens* steigt im Zuge der Moderne die gesellschaftliche Komplexität durch Differenzierung, und damit die wechselseitige Abhängigkeit sozialer Gruppen voneinander, massiv an [16, S. 124–125], [36]. *Drittens* kommt es zu einer massiven Ausweitung sozialer Mobilität [21], [57]. Und *viertens* beginnen die Formen der Selbst-Konstitution umso stärker zu „wuchern", je mehr die vorgegebenen ständischen Subjektivierungsformen entsperrt werden: Im Ständesystem gestaltet sich die soziale Existenz einförmig und konsistent, Subjektformen sind nicht wählbar, sondern an Stand und Familie gebunden [36, S. 679, 697]. In der Moderne lassen sich Subjektpositionen hingegen neu erfinden [52] (auch wenn sie an Machtstrukturen gebunden bleiben).

Genau an diesem historischen Punkt wird informationelle Teilhabebeschränkung *in den Dienst des Einzelnen gestellt.* Fortan geht es nicht mehr um informationelle Verheimlichung abweichenden Verhaltens von der vorgegebenen Ordnung, wie noch im Mittelalter [6], sondern um informationelle Privatheit im Sinne einer *positiven* Institution: Es wird nun institutionell zunehmend dem Umstand Rechnung getragen, dass Akteure, um sich überhaupt als Subjekte konstituieren zu können, Erfahrungsspielräume, und daher auch Mittel zur informationellen Teilhabeschränkung benötigen. Ich spreche erst ab diesem Moment von „informationeller Privatheit" und bezeichne alle früheren Praktiken der informationellen Teilhabebeschränkung demgegenüber als „Geheimnis."

Die hier vorgenommene Bestimmung des *Einsatzpunktes* einer gesellschaftsstrukturellen Entwicklungsgeschichte informationeller Privatheit begründet sich soziologisch mit der maximalen „tektonischen" Spannung zwischen zwei Vergesellschaftungsformen, die sich im 18. Jahrhundert gewissermaßen ineinanderschieben: die stratifizierte Ordnung des Ancien Régime einerseits, und die differenzierte Ordnung der Moderne andererseits. Die resultierende Spannung mündet in Konflikte zwischen Repräsentant:innen der alten und der neuen Ordnung, namentlich zwischen Adel und Bürgertum [15], [52], und insoweit die Ablösung der Selbst-Konstitution von der hergebrachten Ständeordnung in diesem Zeitraum entscheidend voranschreitet, erfolgt nun auch nach und nach die Umwertung von informationeller Teilhabebeschränkung, vom negativen Abweichungsverheimlichungs- zum positiven Subjektivierungsmodus der informationellen Privatheit.

Tab. 1 Formen der informationellen Privatheit im gesellschaftlichen Strukturierungsgefüge

Historische Phase	Privatheitstyp	Privatheits-technik	Subjektivie-rungsrahmen	Streitsache	Zentraler Widerspruch
Ancien Régime 18. Jh.	Repräsentative Privatheit	Reputation Management	Ständisches Selbst	Reputation	Soziale Ordnung in Bewegung vs. ständisch fixiertes Selbst
Bürgerliche Moderne 19. Jh.	Bürgerliche Privatheit	Rückzug	Einheitliches Selbst	Individualität	Differenzierte Ordnung vs. Unteilbares Selbst
Organi-sierte/Reflexive Moderne 20. Jh.	Hochmoderne Privatheit	Kontrolle	Projekt-Selbst	Karriere	Feststellende Ordnung vs. Mobiles Selbst
Digitale Moderne 21. Jh.	Vernetzte Privatheit	Unschär-fe-Garantie	‚Blurry Self'	Offene Zukunft	Voraussagende Ordnung vs. zukunftsoffenes Selbst

Von diesem Zeitpunkt an lassen sich unterscheidbare moderne Vergesellschaftungszeiträume identifizieren, die jeweils strukturbedingt eine dominante Form informationeller Privatheit hervorbringen. Einmal hervorgebrachte Privatheitsformen verschwinden dabei nicht, sondern sedimentieren ins Praxisrepertoire der Akteure. Bei den genannten strukturellen Gründen handelt es sich um Vergesellschaftungswidersprüche, mit denen sich die Akteure im Zuge ihrer Subjektivierungspraktiken konfrontiert sehen. Informationelle Privatheit ermöglicht einen Umgang mit diesen Widersprüchen, ohne letztere deshalb auszusöhnen. Holzschnittartig zusammengefasst ist die Entwicklungsgeschichte informationeller Privatheit in Tabelle 1.

Die so zusammengefasste Geschichte wird im Folgenden knapp rekonstruiert.

3 18. Jahrhundert: Repräsentative Privatheit als *Reputation Management*

Unter Historiker:innen gilt das 18. Jahrhundert als transitorische Phase („Sattelzeit"), die eher strukturell als kalendarisch zu bestimmen ist, reichen doch einige

seiner Strukturmuster bis weit ins 19. Jahrhundert hinein [31, S. 14], obgleich das Jahrhundert in anderen Hinsichten sein Ende schon 1789 (Französische Revolution) findet. Der Übergangscharakter dieser Vergesellschaftungssituation prägt auch die Form, die informationelle Privatheit im 18. Jahrhundert annimmt.

Ansetzen lässt sich hier mit Elias' (1997b) [16, S. 230 ff.] Analyse des „Königsmechanismus", den „zentrifugalen" Machtmechanismen, die im Rahmen langewährender Prozesse von der feudalistischen Kleinstaaterei (ebd.: S. 26 ff.) schließlich zur absolutistischen Machtkonzentration (ebd.: S. 151–168) und zum Gewalt- und zum Steuermonopol führten. Die vermehrte Zirkulation von Münzgeld ermöglichte es den Regenten, Gefolgsleute monetär, statt mit Land zu entschädigen (ebd.: S. 233), und erlaubte so die Bildung größerer dauerhafter Territorien. Zudem boten die neu entstandenen Techniken der Demographie [18], [19], Bevölkerungsstatistik und Administration [68] Möglichkeiten der raumzeitlichen Ausweitung von Herrschaftsapparaten [22, S. 97, 98]. Sofern der absolutistische Staatsapparat zum Betreiben der Verwaltungsinfrastruktur auf Schreib- und Rechenfähigkeiten, sowie auf juristische Expertise angewiesen war, wertete dies die Position der zumeist bürgerlichen Gelehrten deutlich auf, und die des praktisch funktionslosen Adels tendenziell ab [16, S. 267]. Die absolutistischen Herrscher hielten die Spannung zwischen diesen Gruppen aufrecht, und auf diese Weise beide in Schach. Der Adel wurde am Hofe räumlich konzentriert, um ihn systematisch zu überwachen (ebd.: S. 281–282). In den Fürstentümern des heutigen Deutschland wurde das Bürgertum weitgehend von politischer Betätigung ausgeschlossen, weshalb sich seine Angehörigen auf die quasi-politische Produktion von Literatur und neuartigen Subjektivierungsweisen verlegten [15, S. 120]. Die Dominanz des Ancien Régime war noch nicht gänzlich gebrochen, aber die Kräfte, die dies bewerkstelligen sollten, bereits in Stellung.

Subjektivierung war nach wie vor an die repräsentative Ordnung der Ständegesellschaft gebunden, an die Logik von prä-fixierter Hierarchie und ständischer Ehre, obwohl gleichzeitig schon andersartige Vergesellschaftungslogiken gewissermaßen unter der Hand dabei waren, sich zu etablieren. Symptom dafür ist etwa der Gebrauch, den die städtische Bevölkerung nach wie vor von der sozialen Maskerade der repräsentativen Ordnung machte. Sie nutzte sie als Schutzvorrichtung, löste die Masken jedoch gleichzeitig von der alten Ordnung ab: In der Interaktion wurden ständisch festgelegte Bekleidungsformen, Gestiken und Redeweisen als zeichenhafte Oberfläche verwendet, sodass die jeweiligen Gegenüber nie ‚hinter die Maske' blicken konnten, um dort an Daten zu gelangen, aus denen sich Informationen über die „wirkliche Position" der Träger:in generieren lassen würden [58, S. 183]. Wie im mittelalterlichen Feudalismus ging es noch darum, dass das Gegenüber „die Maske korrekt trägt", nicht von der Ordnung abweicht (ebd.:

S. 126). Ob die Masken und ihre Träger:innen dabei *übereinstimmten,* war aber schon von sekundärer Bedeutung: „Die Kleidung brauchte nicht sicher anzuzeigen, mit wem man es zu tun hatte, sie sollte aber erlauben, so zu tun, als ob man sich dessen sicher wäre." (ebd.: S. 132) So lassen sich nur solche Informationen senden, die mit der hergebrachten Ordnung übereinstimmen. Gelingt dies, so bleibt die „Ehre" der Akteure, Sozialkapital der repräsentativen Ordnung, intakt [14].

Gegen die soweit skizzierten Subjektivierungsanforderungen formieren sich indes bereits „inoffiziell", aber doch wirksam, entgegengesetzte Notwendigkeiten. Angeschoben durch Arbeitsteilung und daraus resultierende Komplexitätssteigerung wächst die wechselseitige soziale Abhängigkeit der Akteure. Handeln in Übereinstimmung mit der auf Standes- und Familienzugehörigkeit basierenden, hergebrachten Ordnung ist normativ weiterhin gefordert, garantiert aber immer weniger sozialen Erfolg. Folge ist eine Intensivierung der sozialen Positionierungskämpfe, in deren Rahmen es immer wichtiger wird, das eigene Verhalten und das der anderen permanent zu überwachen – „eine ‚psychologische' Betrachtung des Menschen" tritt auf den Plan [16, S. 385]. Das Tragen der hergebrachten Masken zur Wahrung des Rufs – das *Reputation Management* – stellt einen Kompromiss dar: Die Akteure greifen auf alte Techniken zurück (die der repräsentativen Ordnung), um auf neue Probleme zu antworten (die der Moderne). Es ist daher bis zu einem gewissen Grade korrekt, wenn behauptet wird, dass die „political and social values of ‚dignity' and ‚honor' are indeed what is at stake in the continental concept of privacy" [70, S. 1165] – dies gilt zumindest für die aus dem 18. Jahrhundert vererbte Bedeutungsschicht informationeller Privatheit, die wir heute als *Reputation Management* bezeichnen.

Repräsentative Privatheit ermöglicht den Akteuren einen Umgang mit den Subjektvierungswidersprüchen des 18. Jahrhunderts, indem sie erlaubt, so zu tun, als ob man noch in ehrenhafter Übereinstimmung mit alten Ordnung agierte, während man schon längst in normativ gegenläufige soziale Positionierungskämpfe verstrickt ist. Visualisieren lässt sie sich diese Situation wie in Abbildung 1.

4 19. Jahrhundert: Bürgerliche Privatheit als Rückzug vom Sozialen

Im 19. Jahrhundert wird das Bürgertum zur gesellschaftlich dominanten Gruppe [52, S. 242 ff.], das absolutistische Gewalt- und Steuermonopol vom Staat als „öffentliche Gewalt" übernommen [16, S. 157–160], [27, S. 69]. Das Gegenspiel von öffentlicher politischer Macht einerseits, und privatem ökonomischen

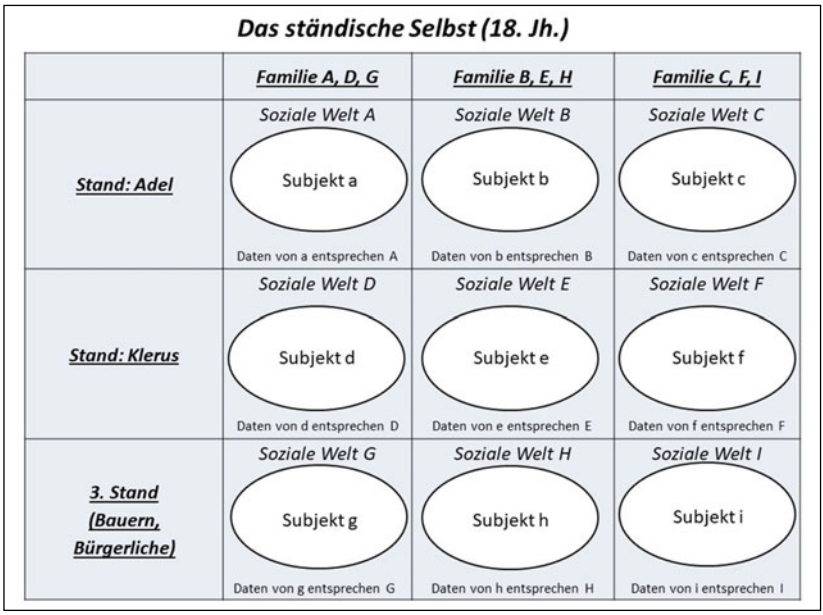


Abb. 1 Soziale Maskerade: Repräsentative Privatheit als Ehrschutz *(Reputation Management)*

Handeln andererseits, wird zu einem Strukturprinzip moderner Vergesellschaftung [24, S. 252]. Kapitalistische Produktionsweise und Nationalstaat dominieren nun die politisch-ökonomische Szene [22, S. 135], [49, S. 105 ff.]. Während die Industrialisierung an Fahrt aufnimmt, vervielfältigen sich die Überwachungstechniken in dem Maße, in dem staatliche Verwaltungsapparate und das Fabriksystem immer ausgefeiltere Überwachungsformen entwickeln [25, S. 138; 169–176].

Die Industrialisierung treibt die Arbeitsteilung voran [13], woraus weitere dynamische soziale Differenzierungsprozesse hervorgehen. Die neuartige Wissenschaft von der Gesellschaft – Soziologie – tendiert dazu, Gesellschaft als einen Organismus zu porträtieren, der aus zahlreichen „Körperteilen" besteht (Spencer). Die so perspektivierte und rasch voranschreitende Differenzierung des Sozialen zeitigt weitreichende Konsequenzen auch für die Prozesse der Selbst-Konstitution. Sofern letztere nicht mehr im vorbestimmten Gerüst des Ständesystems verlaufen, sind die sozialen Akteure nunmehr dazu aufgerufen, sich *selbst* als individuelle Akteure zu konstituieren. Simmel (1989) [61, S. 241] erklärt das Individuum

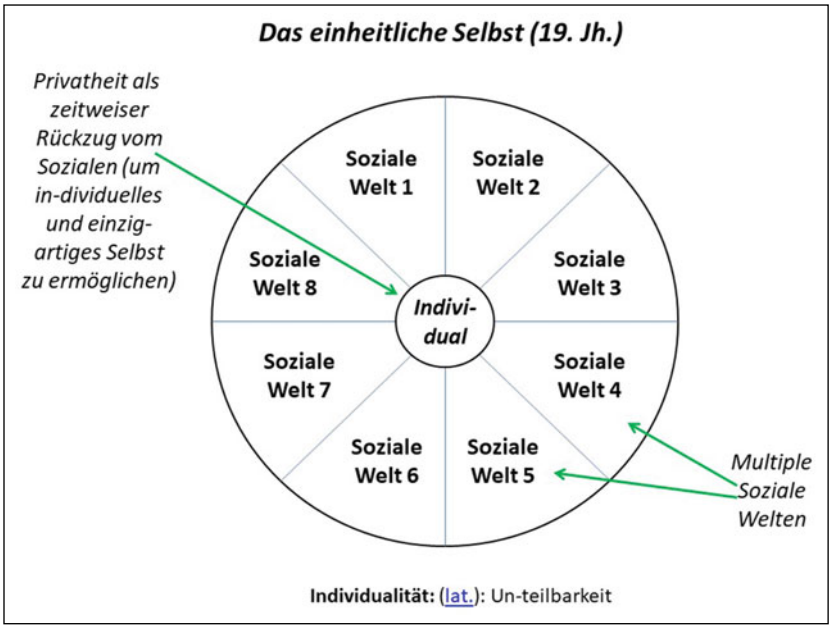


Abb. 2 Sozialer Rückzug: Bürgerliche Privatheit als zeitweiser Ausstieg

dementsprechend zum „Schnittpunkt der sozialen Kreise", denen es angehört – Subjektivität wird zum je individuellen Mischungsverhältnis. Während in der vormodernen Ära noch die ganze Persönlichkeit in einer kohärenten, umfassenden sozialen Welt involviert war und in dieser eine einheitliche soziale Existenz pflegte (Kongruenz persönlicher, beruflicher, politischer, religiöser, amouröser Kreise), kommt es nun zu einer Aufspaltung. Die Anforderung an das Individuum, sich selbst mithilfe prä-fixierter Sozialpositionen zu konstituieren, entfällt nach und nach, stattdessen soll es sich und sein soziales Leben in einer Vielzahl inkohärenter und heterogener Kontexte ausformen, und so auch von jedem anderen Akteur unterscheiden [35, S. 215].

Die Idee der unteilbaren In-dividualität[1] hat genau ab jenem Moment Konjunktur, ab dem die soziale Existenz der Akteure von sozialen Fragmentierungstendenzen geprägt ist. Subjektivierungsanforderung ist die Ausbildung eines ungeteilten,

[1] Mit der Schreibweise „In-dividualität" bzw. „In-dividuum" soll betont werden, dass die zugrundeliegende lateinische Begrifflichkeit „Un-geteiltheit" bedeutet.

kohärenten, ganzheitlichen und einzigartigen Selbst. Wie aber soll eine solche ungeteilte Ganzheit herzustellen sein, wenn der alltägliche Handlungsstrom dazu führt, ständig den widersprüchlichen normativen Spielregeln differenzierter sozialer Welten entsprechen zu müssen? Wie soll Einzigartigkeit gewährleistet werden, wenn die Akteure permanent beobachtet, befragt, überwacht, analysiert und verglichen werden im Rahmen von vielfältigen Disziplinartechniken, die die Vergesellschaftungsprozesse in Schulen, Internaten, Fabriken, Krankenhäusern und Militäreinrichtungen durchziehen? Die Verhaltensweisen der Akteure werden mithilfe dieser Überwachungstechniken in Richtung des statistischen Durchschnittsmittels hin orientiert [17, S. 234–237], was dem individuellen Einzigartigkeitsgebot diametral entgegenläuft: die Normalisierungseffekte der Disziplinen arbeiten individueller Differenz entgegen.

Eben daran zeichnet sich der Subjektivierungswiderspruch des 19. Jahrhunderts ab: wie soll man ein ungeteiltes, einzigartiges Individuum werden, wenn man gleichzeitig gezwungen ist, eine differenzierte soziale Existenz zu führen, die obendrein ständig auf Konformität getrimmt wird? Die dominante informationelle Privatheitstechnik des 19. Jahrhunderts hält eine Antwort parat: durch *regelmäßigen Rückzug vom Sozialen.* Denn „[d]ie Privatleute, die sich hier zum Publikum formieren, gehen nicht ‚in der Gesellschaft' auf; sie treten jeweils erst aus einem privaten Leben sozusagen hervor, das im Binnenraum der patriarchalischen Kleinfamilie institutionelle Gestalt gewonnen hat." [27, S. 109] Nur im Rückzug können die Akteure sicher sein, keine Informationen über sich selbst an normativ widersprüchliche Kontexte auszusenden, und nur dort können sie immer wieder die verstreuten Einzelteile einer differenzierten sozialen Existenz zu einem kohärenten Ganzen zusammenzufügen. Nur in der zeitweisen Unbeobachtetheit ist es darüber hinaus möglich, der disziplinären Überwachung zu entgehen, um dort dann Einzigartigkeit zu entwickeln. Visuell vorgestellt werden kann die dominante informationelle Privatheitstechnik des 19. Jahrhunderts daher wie in Abbildung 2.

5 20. Jahrhundert: Hochmoderne Privatheit als Informationskontrolle

Die ersten beiden Weltkriege, in deren Zuge Deutschland zu Beginn des 20. Jahrhunderts große Teile der Welt in die Barbarei der industrialisierten Kriegsführung und des bürokratisierten Massenmords hineinzieht, markieren in soziologischer Hinsicht sowohl das Ende der Dominanz der bürgerlichen Subjektkultur [52, S. 275] als auch den Auftritt der *Organisierten Moderne* [69]. Letztere organisiert das soziale Leben zunehmend in Großgruppenverbänden, wie z. B.

Gewerkschaften, Arbeitgeberverbände, Parteien, Großkonzerne etc. Transport-, Kommunikations-, Medien- und Produktionstechnologien ermögliche die Ausweitung von Sozialbeziehungen. Der beständig erhöhte Grad der Selbst-Überwachung aller möglichen Institutionen mündet zum Jahrhundertende schließlich in eine *Reflexive Moderne,* die permanent rekursiv auf sich selbst einwirkt [2].

Für den Aufschwung der individuellen Informationskontrolle zur dominanten Privatheitstechnik ist zunächst die immer weiter um sich greifende Vervielfältigung sozialer Teilwelten sowie deren zunehmendes Reflexivwerden verantwortlich zu machen: Im 20. Jahrhundert gilt nicht nur, dass „m]ost people live more or less compartmentalized lives, shifting from one social world to another as they participate in a succession of transactions“ [60, S. 567], sondern dass alle auch darum *wissen, dass alle wissen,* dass alle „compartmentalized lives“ führen. Der Grund für diese Reflexivität liegt darin, dass Urbanisierung, Radio und Fernsehen die Differenziertheit des Sozialen gesamtgesellschaftlich wahrnehmbar machen [3, S. 64 ff.].

Die so charakterisierte Vergesellschaftungssituation stellt spezifische Anforderungen an die Subjektivierungsbemühungen der Akteure. Das Leben in differenzierten Kontexten, deren soziale Verhaltensregeln nicht per Tradition festgelegt sind, nötigt den Akteuren permanent die interaktive Definition sozialer Situationen ab, inklusive der Rollen, die sie darin spielen sollen. Daraus ergibt sich wiederum die Notwendigkeit, ständig Informationen über die Anderen und sich selbst ins Spiel bringen und umgekehrt auch aus dem Spiel nehmen zu müssen [26, S. 1]. Bereits auf Ebene des alltäglichen Umgangs entwickeln sich so Praktiken der Informationskontrolle, die sich in besonderer Weise auch auf die Selbst-Konstitution erstrecken. Wie oben angemerkt, hat die Vorstellung von Individualität im Sinne einer unteilbaren Sozialexistenz durch das massenmedial hervorgebrachte Reflexivwerden der „compartmentalization“ des sozialen Lebens an Plausibilität verloren: wenn alle wissen, dass alle wissen, dass alle ein differenzierte Sozialleben führen, verliert die gesellschaftliche Aufforderung, ein sozial homogenes Leben zu führen, nachhaltig an Plausibilität. An diese Stelle tritt nun die Erwartung, dass die vielfältigen sozialen Welten, die die Einzelnen im Zuge ihrer sozialen Existenz durchlaufen, eine relative Passung aufweisen. Die Homogenitätsforderung wechselt vom Individuum zu den sozialen Welten [52, S. 50 ff.]; klassisch: [4] – Fließband passt zu Stehtribüne, Vorstandsetage zu Golfplatz.

Indem die Akteure im Zuge der Selbst-Konstitution eine Vielzahl sozialer Welten durchlaufen, entfalten sie Subjektivierungslaufbahnen, die sich soziologisch auf den Begriff eines „Projekt-Selbst“ bringen lassen [23, S. 75–80], das gesellschaftlich durch „Karrieren“ integriert wird [35]. Persönliche Vergangenheit wird

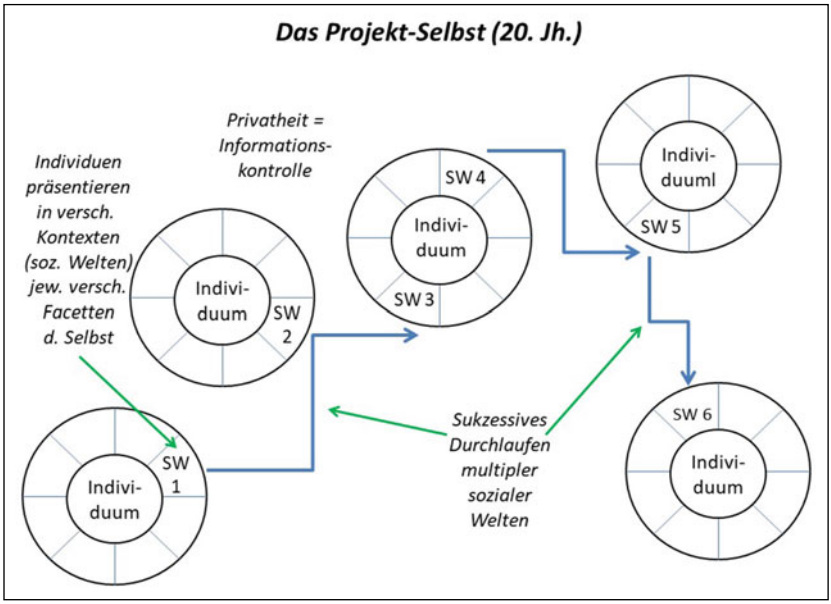


Abb. 3 Soziale Kontextgrenzen: Hochmoderne Privatheit als individuelle Informationskontrolle

damit zu Last oder Potenzial zukünftiger Weiterentwicklung [36, S. 742]: Projekt-Selbste werden regelmäßig durch institutionelle Prüfungssituationen geschickt, in denen sie gegenwärtig die Berechtigung nachweisen müssen, zur Wahrnehmung zukünftiger Handlungsoptionen befähigt zu sein (z. B.: *Nach*weise berechtigen *heute,* an einem Eignungstest für ein *zukünftiges* Studium teilzunehmen). Dabei determinieren Vergangenheit und Gegenwart jedoch nicht die Zukunft, sondern strukturieren bloß grob mögliche Laufbahnen vor.

Während es in der Gegenwart agiert, um Zukunftschancen zu wahren, wird das Projekt-Selbst stetig von machtvollen Institutionen beobachtet, die auf eine „Feststellung der Identität" abzielen [41]. Genau an dieser Stelle entsteht wiederum ein auf die Subjektivierungspraktiken durchschlagender Vergesellschaftungswiderspruch: während das Selbst auf *Weiterentwicklung* angelegt ist, und dabei notwendigerweise normativ widersprüchliche sozialen Welten durchläuft, versuchen staatliche und ökonomische Organisationen permanent, die Identität der Akteure zu *fixieren.* Um mit der normativen Widersprüchlichkeit zwischen den

durchlaufenen Welten und deren Fixierungsversuchen umzugehen, werden informationelle Grenzen zwischen den sozialen Kontexten eingezogen, entweder von den Akteuren selbst [26], [56] oder durch kollektive Absicherung „kontextueller Integrität“ [42]. Beide Vorgehensweisen fußen letztlich auf der Annahme, dass erfolgreiche Subjektivierung nur dann möglich ist, wenn die Teilhabe der sozialen Welten an Informationen über ihre Existenzweisen in den jeweiligen Kontexten beschränkt wird – es geht die Ärztin der Konto-, den Bankangestellten der Gesundheitszustand nichts an. Die zugrunde liegende gesellschaftliche Konstellation kann wie in Abb. 3 dargestellt werden.

6 21. Jahrhundert: Vernetzte Privatheit als Unschärfegarantie

Zeitgenössische Sozialformationen befinden sich aktuell mitten im soziodigitalen Strukturwandel. Obgleich dessen Komplexität kaum seriöse Voraussagen erlaubt, lassen sich doch zumindest zwei prägende und zentrale Dynamiken identifizieren: Erstens die Entstehung einer digitaltechnologisch gestützten „Network Society“ [8], sowie zweitens der jüngere Trend hin zur „Datafizierung“ [29].

Die erste Dynamik verweist auf die Transformation der gesellschaftlichen Organisationslogik durch die soziotechnische Restrukturierung der nun transnationalen Kommunikationsinfrastruktur. Sie setzte in einer Situation tiefgreifender Verunsicherung ein der sozialen Akteure im Zuge der in den 1990er Jahren auf den Plan tretenden „Zweiten Moderne“ ein [71]: (Berufs-)Biographien wurden fragil, ihre kulturelle Einbettung brüchig, soziale Sicherheitssysteme abgebaut [2]. Vor diesem Hintergrund übernahm das frühe, zunächst nur mäßig ökonomisierte Internet die Rolle einer (potenziellen) Re-Sozialisierungsagentur [8, S. 388]. Bis heute verspricht seine Nutzung die Erweiterung selbstgewählter Handlungsmöglichkeiten [50, S. 19], die ich hier als *Optionalität* bezeichne. Wer sich in digitalen Vergesellschaftungszusammenhängen als vollwertiges Subjekt konstituieren will, kommt kaum umhin, die Optionalität des Digitalen praktisch zu nutzen. Sofern aktuell „Unsichtbarkeit den digitalen Tod bedeutet“ [53, S. 247], erfolgt Personenkonstitution immer stärker datenbasiert [33, S. 30]: Die Akteure sind darauf angewiesen, mithilfe eines eher „sendefreudigen“ Datenumgangs versch. Selbst-Facetten digital kuratierend zu einem Ganzen zusammenzusetzen [48, S. 108].

Die zweite Dynamik setzt Anfang der 2000er Jahre ein und vollzieht sich im Kontext einer tiefgreifenden Ökonomisierung digitaler Vernetzungstechnologien. Dabei lässt sich zum einen konstatieren, dass die digitale Ermöglichung technisch

vermittelter Sozialität („connectedness“) zunehmend der technischen Zurichtung sozialer Beziehungen („connectivity“; [66]) weicht. Digitale Sozialität konstituiert sich zunehmend in datenökonomischen Infrastrukturen [11], deren Anbieterinnen astronomische Gewinne durch Bildung und Verkauf von Verhaltenssteuerungspotentialen realisieren. Die Ausbeutung des datenmäßigen „Verhaltensüberschusses“ [71] mündet in das Versprechen, Nutzer:innenverhalten vorhersagen zu können, um diese Vorhersagen dann an Organisationen zu veräußern, die so Kontingenz auszuschalten hoffen. Die einmal losgetretenen Dynamiken legen es den Internetkonzernen schließlich nahe, ihrerseits Nutzungskontingenz herabzusetzen, indem sie mithilfe von Nutzungsdaten Verhalten vorformen – *predictive analytics* resultieren in „Verhaltensmodifikationsmitteln.“ In Anlehnung an Zuboff lässt sich diese Entwicklung als die Erfindung der *Prediktivität* des Digitalen bezeichnen. Mit ihr ändert sich die temporale Logik von Herrschaftstechniken: Der Datenbestand, auf den solche Techniken zugreifen, erstreckt sich immer weiter in die Vergangenheit [34], während der Analysehorizont der Politische Ökonomie Herrschaftsapparate asymptotisch an die Gegenwart heranrückt, um Zukunft festzulegen (mithilfe von Echtzeitdaten, bspw. über affektive Zustände, Verhalten unterhalb der Wahrnehmungsschwelle beeinflussen; [46]). Prediktivität zielt somit auf das genaue Gegenteil der Optionalität des Digitalen, auf „Verhaltensausrichtung durch die Entscheidungsarchitektur“ [32, S. 53] der digitalen Subjektivierungsangebote – auf die Herabsetzung von Handlungsmöglichkeiten.

Subjektivierungspraktiken sind in der Folge mit dem Widerspruch konfrontiert, einerseits datenbasierte Sichtbarkeit generieren zu müssen, um auch im Rahmen der ubiquitären digitalen Bewertungspraktiken [39] Handlungsmöglichkeiten zu wahren; andererseits ermöglicht genau dies den im Internet allgegenwärtigen Datenanalysten [9], [10] die gezielte Kanalisierung dieser Möglichkeiten für eigene Zwecke [20, S. 23]: Die selbst-bestimmte Bestimmung des Selbst droht in eine Objektivierung der Nutzenden als *targets* umzukippen [45]. Was könnte nun „informationelle Privatheit“ unter diesen datenminimierungs*un*freundlichen Bedingungen genau heißen, und wie wäre sie zu gewährleisten?

Interessanterweise haben die empirisch beobachtbaren Nutzungspraktiken längst begonnen, sich auf den identifizierten Subjektivierungswiderspruch einzustellen. Konstatiert werden kann zunächst, dass hergebrachte Privatheitspraktiken, wie *Reputation Management,* Rückzug (Nichtnutzung) und individuelle Informationskontrolle nach wie vor vollzogen werden, dabei allerdings keinen Umgang mit dem spezifischen Subjektivierungswiderspruch digitaler Vergesellschaftung erlauben – auf diesen antwortet die Erfindung neuartiger Privatheitsformen [44]. „Hiding in plain sight“ nennt danah boyd Nutzungspraktiken, die gerade nicht auf Sichtbarkeit verzichten, dabei aber ihre weithin sichtbaren Botschaften sozial so

verschlüsseln, dass nur Eingeweihten noch ein „korrektes“ Verständnis möglich wird, während alle anderen gar nicht erst bemerken, dass die Daten durch „soziale Steganographie“ „undekodierbar“ gemacht worden sind [1], [5, S. 65]. Potenziale und Möglichkeiten der „obfuscation“, d. h. der Verschleierung der Daten werden ausgelotet, um *gleichzeitig Unschärfe und Sichtbarkeit zu gewährleisten* [7].

Hierin finden sich dann auch die gesellschaftsstrukturelle Konstellation und der maßgebliche Subjektivierungswiderspruch, auf den die in Entwicklung begriffene Form informationeller Privatheit als *networked privacy* [5] reagieren muss: Privatheitsschutz trotz datenintensiver Subjektivierungspraktiken [63]. Eben diese Analyse verdichte ich hier im Bild des *blurry self,* womit ein Subjektivierungsmodus gemeint ist, der den Akteuren Möglichkeiten weitreichender Sichtbarkeit einräumt, gleichzeitig aber ein hohes Maß an Unschärfe garantiert. Visualisiert wird die Grundsituation in Abbildung 4.

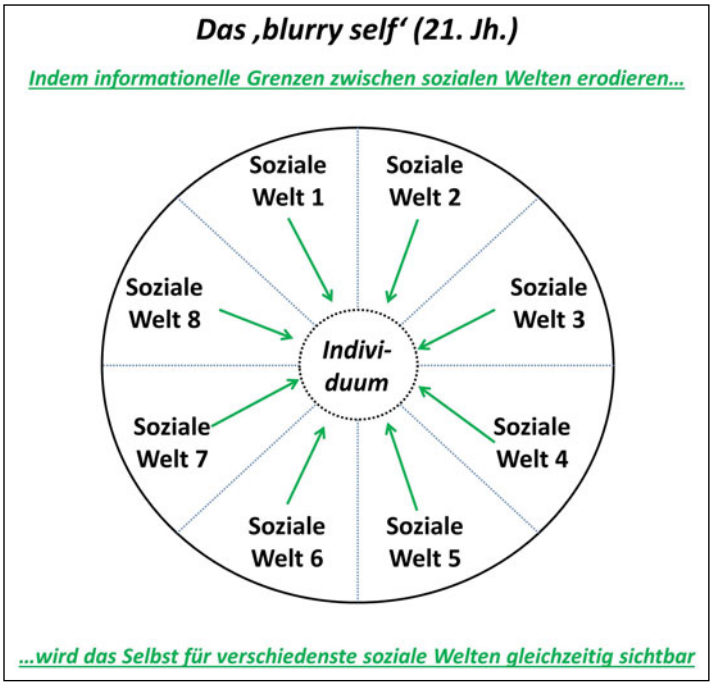


Abb. 4 Privatheit trotz datenbasierter Sichtbarkeit: *Networked Privacy* als Unschärfegarantie

7 Schluss: Strukturelle Bedingungen der Technikgestaltung

Ziel dieses Beitrags ist es, Technikgestaltungsdiskursen Expertise hinsichtlich der gesellschaftsstrukturellen Grundbedingungen zur Verfügung zu stellen, unter denen digitale Privatheitspraktiken heute vollzogen werden, um so die Reflexion über „Parameter" der Gestaltung von Privatheitsschutz anzuregen. Wie zu sehen, kann Gestaltung dabei auf ganz unterschiedliche informationellen Privatheitspraktiken abzielen, die allesamt im Rahmen der oben skizzierten kulturhistorischen Prozesse in den gesellschaftlichen „Werkzeugkasten" der Privatheit sedimentiert sind: Wir verfügen auch heute noch über Techniken des *Reputation Management,* des Rückzugs und der individuellen Informationskontrolle, nur haben sich mittlerweile neue Problemlagen und Lösungsanforderungen ergeben [55]. Technikgestaltung ist daher immer aufgerufen, bei der Problembeabeitung im Blick zu behalten, ob gerade die Erzeugung digitaler Avatare (*Reputation Management;* [40, S. 104–106]), die Verfügbarmachung nicht-digitaler Alternativangebote (Rückzug; [30]) oder Möglichkeiten der individuellen Informationskontrolle (ohne, dass dies in Überforderung umkippt; [38]) technischer Stützung bedürfen. Wenn sich aber nun einige aktuelle und zentrale Problemlagen nicht mehr mithilfe hergebrachter Techniken bearbeiten lassen – was wäre dann unter der Alternativstrategie einer „Unschärfegarantie" zu verstehen? Zwei Dinge sind diesbezüglich zu berücksichtigen:

Erstens meint Unschärfe gerade keinen Freifahrtschein dafür, auf statistischer Korrelation basierende Verhaltensmodifikationen vorzunehmen, die die traditionellen Privatheitsgarantien der „persönlichen Daten" unangetastet lassen. „Indirect group-level targeting" kann individuelle Anonymität wahren, und dennoch in statistisch signifikantem Ausmaß Kollektivverhalten – und damit individuelles Verhalten – modifizieren [37]. „Unschärfe" meint hier die Unmöglichkeit für Herrschaftsapparate, aus Daten Informationen zu generieren, die die Optionalität des Digitalen, und damit die Zukunftsoffenheit individueller Existenzweisen untergraben.

Daraus folgt *zweitens,* dass Schutzmechanismen immer schon auf der kollektiven Ebene ansetzen müssen. Der aktuelle Privatheitsdiskurs weiß genau um die Kollektivität der Problemlagen [28], [64], weil individuelle Verschleierungstaktiken punktuell Abhilfe schaffen, sich aber gegenüber den Analysekapazitäten der Konzerne und Geheimdienste als stumpf erweisen [54, S. 1204]. Zudem droht auf verallgemeinertem Misstrauen basierendes individuelle *Obfuscation* letztlich den digitalen Sozialraum auszuhöhlen – dieser kann nur zur digitalen Vergesellschaftung beitragen, wenn *gerechtfertigte Vertrauen* institutionell verankert

wird [65]. Unschärfegarantien können daher nur kollektiv, politisch, rechtlich, infrastrukturell vergeben werden.[2]

Die Diskussion, die der vorliegende Beitrag anregen möchte, dreht sich also darum, wie Sichtbarkeit mit hinreichenden Unschärfegarantien auf dieser Ebene des gesellschaftsstrukturellen *set-ups* verbunden werden könnte, um so zu gewährleisten, dass auf Sichtbarkeit abstellende datenintensive Subjektivierungspraktiken nicht automatisch im Zuge allgegenwärtigen Berechnet-Werdens Lebenschancen verspielen. Wie im Vollzug digitaler Praktiken Optionalität gewahrt werden kann, ohne von Prediktivität „aufgefressen" zu werden – das ist die Frage, an deren Beantwortung sich nicht nur eine zeitgenössische Form der informationellen Privatheit bewähren muss, sondern an der sich gleichermaßen auch die Demokratiefähigkeit digitaler Vergesellschaftung schlechthin entscheidet.

Literatur

1. Barth, N.: Kalte Vertrautheiten. Private Kommunikation auf der Social Network Site Facebook. Berl. J. Soziol. **25**(4), 459–489 (2016)
2. Beck, U.: Risikogesellschaft. Suhrkamp, Frankfurt/M (1986)
3. Berger, P., Berger, B., Kellner, H.: Das Unbehagen in der Modernität. Campus, Frankfurt/M (1975)
4. Bourdieu, P.: Die feinen Unterschiede. Kritik der gesellschaftlichen Urteilskraft. Suhrkamp, Frankfurt/M (1987)
5. boyd, d.: It's Complicated: The Social Lives of Networked Teens. Yale University Press, New Haven (2014)
6. Brandt, R.: … his stupris incumbere non pertimescit publice. Heimlichkeit zum Schutz sozialer Konformität im Mittelalter. In: Assmann, A., Assmann, J., Hahn, A. Lüsebrink, H.-J. (Hrsg.) Geheimnis und Öffentlichkeit, S. 71–88. Fink, München (1997)
7. Brunton, F., Nisssenbaum, H.: Obfuscation: A User's Guide to Privacy and Protest. MIT Press, Cambridge (2015)
8. Castells, M.: The Rise of the Network Society. Blackwell, Cambridge (1996)
9. Christl, W.: Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions. A Report by Cracked Labs, Vienna, June 2017. https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf. Zugegriffen: 07. Jan. 2021
10. Christl, W.: How Companies Use Personal Data Against People: Automated Disadvantage, Personalized Persuasion, and the Societal Ramifications of the Commercial Use of Personal Information. https://digitalcourage.de/sites/default/files/users/161/crackedlabs_christl_dataagainstpeople.pdf. Zugegriffen: 07. Jan. 2021

[2] Die Ausführungen dieses Abschnitts sind von kritischen Einwänden Matthias Hollicks, Beate Rösslers und Jörn Lamlas inspiriert – ich schulde meinen Fragesteller:innen Dank dafür.

11. Dolata, U.: Plattform-Regulierung. Berl. J. Soziol. **29**(3), 179–206 (2020)
12. DSGVO: Europäische Datenschutzgrundverordnung. https://dsgvo-gesetz.de/art-25-dsgvo/. Zugegriffen: 23. Okt. 2020
13. Durkheim, E.: Über soziale Arbeitsteilung. Studie über die Organisation höherer Gesellschaften. Suhrkamp, Frankfurt/M (1992)
14. Elias, N.: Die höfische Gesellschaft. Untersuchungen zur Soziologie des Königtums und der höfischen Aristokratie. Suhrkamp, Frankfurt/M (2002)
15. Elias, N.: Über den Prozeß der Zivilisation. Soziogenetische und psychogenetische Untersuchungen, Bd. 1. Suhrkamp, Frankfurt/M (1997a)
16. Elias, N.: Über den Prozeß der Zivilisation. Soziogenetische und psychogenetische Untersuchungen, Bd. 2. Suhrkamp, Frankfurt/M (1997b)
17. Foucault, M.: Überwachen und Strafen. Die Geburt des Gefängnisses. Suhrkamp, Frankfurt/M (1994)
18. Foucault, M.: Geschichte der Gouvernementalität. Bd. 1: Sicherheit, Territorium, Bevölkerung: Vorlesung am Collège de France, 1977–1978. Suhrkamp, Frankfurt/M (2006a)
19. Foucault, M.: Geschichte der Gouvernementalität. Bd. 2: Die Geburt der Biopolitik: Vorlesung am Collège de France, 1978–1979. Suhrkamp, Frankfurt/M (2006b)
20. Fourcade, M., Healy, K.: Seeing like a market. Socio-Econ. Rev. **15**(1), 9–29 (2017)
21. Füssel, M., Weller, T.: Einleitung. In: Füssel, M., Weller, T. (Hrsg.) Ordnung und Distinktion. Praktiken sozialer Repräsentation in der ständischen Gesellschaft, S. 9–22. Rhema, Münster (2005)
22. Giddens, A.: The Nation-State and Violence. University of California Press, Berkeley (1987)
23. Giddens, A.: Modernity and Self-Identity: Self and Society in the Late Modern Age. Polity, Cambridge (1991)
24. Giddens, A.: Die Konstitution der Gesellschaft. Grundzüge einer Theorie der Strukturierung. Campus, Frankfurt/M (1995a)
25. Giddens, A.: A Contemporary Critique of Historical Materialism. University of California Press, Berkeley (1995b)
26. Goffman, E.: The Presentation of Self in Everyday Life. Overlook, Woodstock (1973)
27. Habermas, J.: Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft. Suhrkamp, Frankfurt/M (1990)
28. Helm, P., Eichenhofer, J.: Reflexionen zu einem social turn in den privacy studies. In: Aldenhoff, C.; Raabe, L. Hennig, M. (Hrsg.) Digitalität und Privatheit: Kulturelle, politisch-rechtliche und soziale Perspektiven, S. 139–165. transcript, Bielefeld (2019)
29. Houben, D., Prietl, B. (Hrsg.): Datengesellschaft: Einsichten in die Datafizierung des Sozialen. transcript, Bielefeld (2018)
30. Karaboga, M., Matzner, T., Obersteller, H., Ochs, C.: Is there a right to offline alternatives in a digital world? In: Leenes, R., van Brakel, R., Gutwirth, S., De Hert, P. (Hrsg.) Data Protection and Privacy: (In)visibilities and Infrastructres, S. 31–57. Springer, Cham (2017)
31. Koselleck, R.: Über die Theoriebedürftigkeit der Geschichtswissenschaft. In: Conze, W. (Hrsg.) Theorie der Geschichtswissenschaft und Praxis des Geschichtsunterrichts, S. 10–28. Klett, Stuttgart (1972)

32. Lamla, J.: Selbstbestimmung und Verbraucherschutz in der Datenökonomie. APuZ **69**(24–26), 49–54 (2019)
33. Lamla, J., Ochs, C.: Selbstbestimmungspraktiken in der Datenökonomie: Gesellschaftlicher Widerspruch oder „privates" Paradox? In: Blättel-Mink, B., Kenning, P. (Hrsg.) Paradoxien des Verbraucherverhaltens, S. 25–39. Springer, Wiesbaden (2019)
34. Lindemann, G.: Die Verschränkung von Leib und Nexistenz. In: Süssenguth, F. (Hrsg.) Die Gesellschaft der Daten. Über die digitale Transformation der sozialen Ordnung, S. 41–66. transcript, Bielefeld (2015)
35. Luhmann, N.: Individuum, Individualität, Individualismus. In: Luhmann, N. (Hrsg.) Gesellschaftsstruktur und Semantik. Studien zur Wissenssoziologie der modernen Gesellschaft, S. 149–258. Suhrkamp, Frankfurt/M (1989)
36. Luhmann, N.: Die Gesellschaft der Gesellschaft, Bd. 2. Suhrkamp, Frankfurt/M (1997)
37. Matz, S.C., Kosinski, M., Nave, G., Stillwell, D.J.: Psychological targeting as an effective approach to digital mass persuasion. PNAS **114**(48), 12714–12719 (2017)
38. Matzner, T., Masur, P., Ochs, C., von Pape, T.: Do-it-youself-data protection – empowerment or burden? In: Gutwirt, S., Leenes, R., De Hert, P. (Hrsg.) Data Protection on the Move, S. 277–305. Springer, Cham (2016)
39. Mau, S.: Das metrische Wir: Über die Quantifizierung des Sozialen. Suhrkamp, Berlin (2017)
40. Miller, D.: Das wilde Netzwerk. Ein ethnologischer Blick auf Facebook. Suhrkamp, Berlin (2012)
41. Mönkeberg, S.: Feststellungen der Identität? Über Nutzen und Laster digitaler Sichtbarkeit. Der Bürger im Staat **4**(2014), 268–275 (2014)
42. Nissenbaum, H.: Privacy in Context. Technology, Policy, and the Integrity of Social Life. Stanford University Press, Stanford (2010)
43. Ochs, C.: Teilhabebeschränkungen und Erfahrungsspielräume: Eine negative Akteur-Netzwerk-Theorie der Privatheit. In: Behrendt, H., Loh, W., Matzner, T., Misselhorn, C. (Hrsg.) Privatsphäre 4.0. Eine Neuverortung des Privaten im Zeitalter der Digitalisierung, S. 13–31. Springer, Stuttgart (2019)
44. Ochs, C., Büttner, B.: Das Internet als »Sauerstoff« und »Bedrohung«: Privatheitspraktiken zwischen analoger und digital-vernetzter Subjektivierung. In: Friedewald, M. (Hrsg.) Privatheit und Selbstbestimmtes Leben in Der Digitalen Welt. Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes, S. 33–80. Springer, Wiesbaden (2018)
45. Ochs, C., Büttner, B.: Selbstbestimmte Selbst-Bestimmung? Wie digitale Subjektivierungspraktiken objektivierte Datensubjekte hervorbringen. In: Ochs, C., Friedewald, M., Hess, T., Lamla, J. (Hrsg.) Die Zukunft der Datenökonomie: Zwischen Geschäftsmodell, Kollektivgut und Verbraucherschutz, S. 181–214. Springer, Wiesbaden (2019)
46. Ochs, C., Büttner, B., Lamla, J.: Trading social visibility for economic amenability: data-based value translation on a 'health- and fitness-platform'. Sci. Technol. Hum. Values (2020). https://doi.org/10.1177/0162243920928138
47. Oexle, O.G.: Die funktionale Dreiteilung als Deutungsschema der sozialen Wirklichkeit in der Gesellschaft des Mittelalters. In: Schulze, W., Gabel, H. (Hrsg.) Ständische Gesellschaft und soziale Mobilität, S. 19–52. Oldenbourg, München (1988)

48. Pittroff, F.: Profile als Labore des Privaten. In: Degeling, M., Othmer, J., Weich, A., Westermann, B. (Hrsg.) Profile. Interdisziplinäre Beiträge, S. 101–113. Meson Press, Lüneburg (2017)
49. Polanyi, K.: The Great Transformation. Politische und ökonomische Ursprünge von Gesellschaften und Wirtschaftssystemen. Suhrkamp, Frankfurt/M (1978)
50. Rainie, L., Wellman, B.: Networked: The New Social Operating System. MIT Press, Cambridge (2012)
51. Rammert, W., Windeler, A., Knoblauch, H., Hutter, M.: Die Ausweitung der Innovationszone. In: Rammert, W., Windeler, A., Knoblauch, H., Hutter, M. (Hrsg.) Innovationsgesellschaft heute. Perspektiven, Felder & Fälle, S. 3–13. Springer, Wiesbaden (2016)
52. Reckwitz, A.: Das hybride Subjekt. Eine Theorie der Subjektkulturen von der bürgerlichen Moderne zur Postmoderne. Velbruck, Weilerswist (2006)
53. Reckwitz, A.: Die Gesellschaft der Singularitäten. Zum Strukturwandel der Moderne. Suhrkamp, Berlin (2017)
54. Richards, N., Hartzog, W.: Privacy's trust gap: a review. Yale Law J. **126**(4), 1180–1224 (2017)
55. Roßnagel, A.: Quantifizierung der Persönlichkeit – aus grundrechtlicher und datenschutzrechtlicher Sicht. In: Baule, B., Hohnsträter, D., Krankenhagen, S., (Hrsg.) Transformationen des Konsums. Vom industriellen Massenkonsum zum individualisierten Digitalkonsum, S. 33–53. Nomos, Baden-Baden (2019)
56. Rössler, B.: Der Wert des Privaten. Suhrkamp, Frankfurt/M (2001)
57. Schulze, W.: Die ständische Gesellschaft des 16./17. Jahrhunderts als Problem von Statik und Dynamik. In: Schulze, W., Gabel, H. (Hrsg.) Ständische Gesellschaft und soziale Mobilität, S. 1–17. Oldenbourg, München (1988)
58. Sennett, R.: Verfall und Ende des öffentlichen Lebens: Die Tyrannei der Intimität. Berlin-Verlag, Berlin (2008)
59. Shaw, D.: The construction of the private in medieval London. J. Mediev. Early Mod. Stud. **26**(3), 447–466 (1996)
60. Shibutani, T.: Reference groups as perspectives. Am. J. Sociol. **60**(6), 562–569 (1955)
61. Simmel, G.: Aufsätze 1887–1890: Über sociale Differenzierung. Die Probleme der Geschichtsphilosophie (1892). Gesamtausgabe, Bd. 2. Suhrkamp, Frankfurt/M (1989)
62. Solove, D.J.: Understanding Privacy. Harvard University Press, Cambridge (2008)
63. Stalder, F.: Autonomie und Kontrolle nach dem Ende der Privatsphäre. In Stempfhuber, M., Wagner, E. (Hrsg.) Praktiken der Überwachten. Öffentlichkeit und Privatheit im Web 2.0, S. 97–110. Springer, Wiesbaden (2019)
64. Taylor, L., Floridi, L., van der Sloot, B. (Hrsg.): Group Privacy: New Challenges of Data Technologies. Springer, Cham (2017)
65. Uhlmann, M.: Netzgerechte Datenschutzgestaltung: Herausforderungen, Kriterien, Alternativen. Nomos, Baden-Baden (2020)
66. van Dijck, J.: The Culture of Connectivity. A Critical History of Social Media. Oxford University Press, Oxford (2013)
67. Vincent, D.: Privacy. A Short History. Polity, Cambridge (2016)
68. Vismann, C.: Akten: Medientechnik und Recht. Fischer, Frankfurt/M (2000)
69. Wagner, P.: A Sociology of Modernity. Liberty and Discipline. Routledge, London (1994)

70. Whitman, J.Q.: The two western cultures of privacy: dignity versus liberty. https://digitalcommons.law.yale.edu/fss_papers/649. Zugegriffen: 23. Okt. 2020
71. Zuboff, S.: Das Zeitalter des Überwachungskapitalismus. Campus, Frankfurt/M (2018)

Maschinelles Lernen und das Recht auf Nichtwissen

Michael Kreutzer und Johanna Mittermeier

Zusammenfassung

Das Recht auf Nichtwissen ist ein Teil der informationellen Selbstbestimmung. Als Persönlichkeitsschutz wurde es bislang überwiegend aus medizinischer Sicht betrachtet, dort ist es anerkannt und wird angewendet. Durch den Output Maschineller Lernsysteme, die u. a. mit persönlichen Daten trainiert werden, kann das aufgeklärte Recht auf Nichtwissen ebenfalls bedroht werden. Selbstanalysen, Selbstoptimierungsvorschläge und ggf. Hinweise zur Anpassung, die auf diesem Wege erstellt werden, bergen Gefahren für die freie Entfaltung der Persönlichkeit und sozialisatorischer Beziehungen – die vermittelte Information ist irreversibel. Dieser Beitrag ordnet die technischen Möglichkeiten zu Selbstanalysen, Selbstoptimierungsvorschlägen und Prognosen durch Maschinelles Lernen ein und verknüpft diese mit einer philosophischen Betrachtung entlang folgender Fragestellung: Wie steht es um die Freiheit der Entscheidung, ob das Individuum durch Maschinelles Lernen berechnete, auf sich bezogene Analysen wissen sollen muss oder ob es sich dazu entschließen darf, diese nicht wissen zu wollen.

Schlüsselwörter

Nichtwissen • Maschinelles Lernen • Wissen

M. Kreutzer
Fraunhofer SIT, Darmstadt, Deutschland
E-mail: michael.kreutzer@sit.fraunhofer.de

J. Mittermeier (✉)
Fraunhofer SIT, Darmstadt, Deutschland
E-mail: johanna.mittermeier@sit.fraunhofer.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_4

„[...] Sie sind so jung, so vor allem Anfang, und ich möchte Sie, so gut ich es kann, bitten, lieber Herr, Geduld zu haben gegen alles Ungelöste in Ihrem Herzen und zu versuchen, die Fragen selbst liebzuhaben wie verschlossene Stuben und wie Bücher, die in einer sehr fremden Sprache geschrieben sind. Forschen Sie jetzt nicht nach den Antworten, die Ihnen nicht gegeben werden können, weil Sie sie nicht leben könnten. Und es handelt sich darum, alles zu leben. Leben Sie jetzt die Fragen. Vielleicht leben Sie dann allmählich, ohne es zu merken, eines fernen Tages in die Antwort hinein. [...]“
Rainer Maria Rilke: Brief an Franz Xaver Kappus z. Zt. Worpswede bei Bremen, am 16. Juli 1903

1 Einleitung und Beispiele

Dieser Beitrag hat nicht die Intention und soll nicht so verstanden werden, dass wissenschaftliches Wissen oder die Errungenschaften der Aufklärung relativiert werden sollen oder dass ein Ignorantentum propagiert werden soll – im Gegenteil: Er argumentiert pro Aufklärung, pro Mündigkeit, pro Freiheit und pro Pluralität.

Bei dem aufgeklärten Recht auf Nichtwissen ist die Willenserklärung, den Output Maschineller Lernsysteme (ML-Systeme) über sich *nicht* kennen zu wollen, keine Weltflucht, sondern ein informierter Akt und Ausdruck der Mündigkeit. Dabei spielt es keine Rolle, wie akkurat und präzise die Ergebnisse der Maschine sind bzw. wären. Selbst die (ggf. paternalistische) Ausrichtung auf das Wohlergehen des Individuums zählt hier nicht – allein entscheidend ist das legitime Interesse des Individuums auf eine selbst gewählte Freiheit von Wissen über sich selbst.

Um dieses Argument zu entfalten, wird es erforderlich sein, zunächst das Vorhersagepotenzial des Maschinellen Lernens darzustellen (Abschn. 2). Daraufhin erfolgt eine zusammenfassende Darstellung der rechtlichen Lage und ihrer philosophischen Bewertung (Abschn. 3). Darin wird aufgezeigt, dass das Recht auf Nichtwissen von Prognosen über sich selbst weder Verschlossenheit noch Weltflucht noch Dummheit ist, sondern in der Tradition der Aufklärung steht. Da es um Informationen des Menschen über sich selbst geht, werden die gesammelten Erkenntnisse zusammengeführt und der Nutzen für das Individuum dargestellt (Abschn. 4). Auf dieser Basis diskutiert der Beitrag erste Ideen für Schutzmechanismen (Abschn. 5) und endet mit einer zusammenfassenden Schlussbetrachtung (Abschn. 6).

Zwei Beispiele von Apps und ein ins Extrem fortgeschriebenes fiktives Beispiel sollen in den Problemraum einführen. Ein durch Maschinelles Lernen generiertes „Wissen“ über sich selbst, das auf einem digitalen Zwilling beruht, der beispielsweise mittels Fortschreibungen von bisherigem Verhalten – unter Einbezug von Statistiken und Analysen von Verhalten, Kontaktpersonen und Umgebungen – gespeist wird, ist ein realistisches Szenario. Bereits heute gibt es Selbstanalyse- und Selbstoptimierungsapps für das Arbeitsleben wie MyAnalytics von Microsoft Teams. Microsoft nennt folgende Vorteile von MyAnalytics: *„Verbessern Sie Ihre Beziehungen […] Mehr konzentrierte Arbeitszeit […] Verbessern Sie die Balance zwischen Arbeit und Privatleben […].“* [14] Die Gesundheitsapp „MindDoc“ wird u. a. beworben mit: *„[…] Wenn du mit deiner emotionalen Gesundheit zu kämpfen hast, begleitet dich MindDoc auf deinem Weg zu mehr Kontrolle und effektiveren Strategien für dein emotionales Wohlbefinden. […]“* sowie *„[…] Du erhältst regelmäßig Rückmeldung zu deiner emotionalen Gesundheit, die deine Symptome und emotionalen Ressourcen detailliert beschreiben. Aufgeteilt auf die für dich relevanten Lebensbereiche, gibt dir das Ergebnis einen Einblick, wo es gut läuft und was vielleicht Verbesserungen erfordert. […]“* An anderer Stelle heißt es auf derselben Webseite: *„[…] Du beantwortest drei Mal täglich einige Fragen. Basierend auf deinen Antworten lernt MindDoc, was häufiger oder seltener gefragt werden sollte und zeigt dir zu deinen Herausforderungen passende Inhalte. […]“* [21]

Das fiktive Beispiel handelt von der Firma „OPTYLMAL – Optimize your life with machine learning“:

OPTYLMAL bringt eine neue App auf den Markt, die „EYLMAB – Enhance your life based on Machine Learning of your app behaviour“. EYLMAB wird damit angepriesen, dass alle Daten ausschließlich auf dem Gerät erhoben, verarbeitet und dargestellt werden und es dadurch die Privatheit besonders gut schützt. Das Programm erfasst, welche Online-Kontakte und -medien die Nutzenden abrufen und speist diese als Trainingsdaten in ein System des Maschinellen Lernens ein, das nach den ersten zwei Wochen bereits Analysedaten ausgibt. Die Auswertungen im Vergleich zu Kontrollgruppen erfolgen vollständig anonym und die Datenschutzbeauftragten haben die Konformität mit der DSGVO bestätigt. Die Nutzenden können in einer Selbstanalyse erfahren, was das Programm bezüglich ihrer Neigungen herausgefunden hat und können sich mit einer Zusatzfunktion Empfehlungen ausgeben lassen. Eine Auswertung lautet beispielsweise: *In den Gesprächen, die Du online führst, werden von Dir und Deinen Gesprächspartnern 310 % mehr pessimistische*

Äußerungen getätigt, im Vergleich zu den Äußerungen, die der Durchschnitt der Bevölkerung macht. Eine andere ist: *Die Hörbücher, die Du anhörst, erreichen 63 % des Sprachniveaus der Hörbücher, die die durchschnittliche Bevölkerung anhört.* Eine weitere lautet: *Die Wohnorte der Personen, mit denen Du interagierst, gehören zu 79 % dem prekären Milieu an.* Das Programm empfiehlt nach einer Gesamtauswertung: *Auf Basis Deines Verhaltens und Deiner Beziehungen hat dein digitaler Zwilling eine gegenüber der Normalbevölkerung ca. doppelt so hohe Perspektive, in das Prekariat zu kommen und eine gegenüber der Normalbevölkerung ca. dreifach erhöhte Perspektive, unstete Partnerschaften zu führen.*

Kurz nach der Einführung der App stellt sich heraus, dass sie bei der Bevölkerung in mehreren Staaten ein ungeahnter Erfolg wird. Ein Konkurrenzunternehmen möchte die App mit dem Geschäftsmodell nachbauen. Das Geschäftsmodell sieht vor, dass Prämien bei Versicherungsgesellschaften bei guten Prognosewerten von Kunden verringert werden, wenn diese ihre aggregierten Daten nach eigener Prüfung an die Versicherung weiterleiten. Ein Staat auf einem anderen Kontinent mit einem anderen Regierungs- und Rechtssystem hat großes Interesse daran, diese App – in *kulturell angepasster Form* - bei allen seinen Bürgern auf den Smartphones zu installieren. Dieser Staat führt ein Punktesystem ein, welches denjenigen bevorzugt Zugang zu Bildung, Reisen und beruflichem und sozialem Aufstieg gewährt, die die Handlungsempfehlungen der App umsetzen.

Das fiktive Beispiel OPTYLMAL stellt EYLMAB mit einem sehr guten Vorhersagepotenzial dar – wie steht es um das tatsächliche Potenzial des Maschinellen Lernens als Vorhersagetool?

2 Maschinelles Lernen – ein gutes Vorhersagewerkzeug?

2.1 Kausalität und Korrelation

Der Unterschied zwischen Kausalität und Korrelation ist grundlegend für die Bewertung der Leistungsfähigkeit von Maschinellem Lernen als Vorhersagewerkzeug.

Kausalität ist dadurch bestimmt, dass der Begriff der Ursache ausdrückt, dass die Wirkung nicht bloß zu der Ursache hinzukommt, sondern *„[...] durch dieselbe gesetzt sei und aus ihr erfolg[t].“* [7]

Korrelation „[...] ist ein Maß für den statistischen Zusammenhang zwischen zwei Datensätzen. Unabhängige Variablen sind daher stets unkorreliert. Korrelation impliziert daher auch stochastische Abhängigkeit. Durch Korrelation wird die lineare Abhängigkeit zwischen zwei Variablen quantifiziert. [...] Korrelationen sind wichtig, weil ein existierender korrelativer Zusammenhang auch Hinweise geben

kann, wie sich Variablen in der Zukunft verhalten werden. Damit können Korrelationen Indizien für eine Vorhersage liefern.“ [10]

Eine Maschine erkennt Korrelationen von Variablen großer Datensätze in einer Geschwindigkeit, die ein Mensch nicht erreichen kann. Eine Korrelation zwischen zwei Variablen bedeutet jedoch nicht, dass der Wert einer Variablen ursächlich für den Wert der anderen ist. Sie liefert Hinweise auf das eventuelle Vorhandensein einer Kausalität, die Beziehung der beiden Variablen kann aber auch eine Koinzidenz sein, der keinerlei ursächlicher Zusammenhang zu Grunde liegt.

Hierzu ein Beispiel [20]: Prof. Steinebach und sein Team vom Fraunhofer SIT trainierten ein System des Maschinellen Lernens - unter anderem mit Bildern von Personen in Badesituationen. Zusammen mit den Bildern wurde dem System als ein Merkmal das Geschlecht der Menschen auf den Bildern eingegeben (supervised learning). Dem System wurde dann ein neues Bild mit einer Frau in Badekleidung präsentiert und auf Basis des Trainings erfolgte die Ausgabe, dass es sich um einen Mann handelte. Prof. Steinebach suchte den Grund des Fehllernens und fand heraus, dass die Bierdose, die die Frau in der Hand hielt, der Grund für die fehlerhafte Zuordnung des Geschlechts der Frau war. Die Variable „Geschlecht“ korrelierte offenbar in ihrem Wert „Mann“ mit der Variable „Bierdose in der Hand“. Erst als die Dose unkenntlich gemacht wurde, gab das System das korrekte Geschlecht „Frau“ aus. Im Referenzdatenset waren Bierdosen offenbar ausschließlich in der Hand von Männern aufgetaucht. Es gab also eine Korrelation zwischen Bierdose in der Hand am Wasser und Mann, aber das ist natürlich keine Kausalität. Wir Menschen wissen, dass aus „Bierdose in der Hand am Wasser“ eben nicht „Geschlecht Mann“ folgt. Die Korrelation sagt allerdings vermutlich etwas über gesellschaftliche Konventionen aus: Es scheint für einen Mann weniger ein Problem darzustellen, mit einer Bierdose am Pool, Schwimmbad oder Strand zu sein (oder fotografiert zu werden?) als für eine Frau.

2.2 Vorhersagen mit Maschinellem Lernen

Maschinelles Lernen ist ein neues Werkzeug für Vorhersagen, das sich von statistischen Auswertungen und Fortschreibungen unterscheidet. Grob gesagt besteht der Unterschied zwischen Statistik und Maschinellem Lernen in der Prognostik darin, dass Statistik dazu geeignet ist, Inferenzen bei vorgegebenen Modellen zu finden, während das Maschinelle Lernen auf „empirische Weise“ selbst Vorhersagemodelle konstruiert. In anderen Worten: Wenn statistisch ausgewertet wird, dann werden Zusammenhänge (Korrelationen) gefunden, die zwischen den Daten bestehen. Wenn Maschinelles Lernen angewendet wird, dann vermag das trainierte

System für unbekannte Eingabedaten – solange diese eine gewisse Ähnlichkeit mit den Trainingsdaten haben – Zielwerte auszugeben.

Im Folgenden wird das überwachte Maschinelle Lernen betrachtet. Hier gibt es Trainingsdaten, bei denen der Mensch die Eingangs-Parameter und das Ergebnis kennt und diese der Maschine im Lernprozess vorgibt. Der Maschine wird während der Lernphase diese „Grundwahrheit" (ground truth) präsentiert und sie passt das Modell (das ist der Algorithmus, der durch mathematische Operationen entsteht bzw. „das Wissen, das gelernt wird") des Systems mit jedem präsentierten Paar Eingangsdatum und Ergebnis an. Nachdem das Modell erstellt wurde, können in dieses (bisher) unbekannte Daten eingegeben werden und das System berechnet das Ergebnis, also die „Vorhersage".

Grob teilt man die verschiedenen Verfahren des überwachten Lernens in die Kategorien Klassifikation und Regression ein. Bei der Klassifikation soll ein Modell den Eingabedaten einen Zielwert aus einer endlichen diskreten Menge zuordnen. Ein Beispiel wäre die Ziffernerkennung der Postleitzahlen auf Briefen. Bei der Regression werden stetige Wertverläufe vorhergesagt, z. B. die Temperatur bei der Wettervorhersage.

Für statistische Methoden muss ein Modell ausgewählt werden, das Domänenwissen über die Daten einbezieht. Beim Maschinellen Lernen kann die Domänenagnostische Konstruktion eines Modells von der „Essenz" des modellierten Systems abweichen. Dies ist insbesondere dann der Fall, wenn wenige Trainingsdaten vorhanden sind oder wenn diese einen Bias enthalten. Die Maschine findet dann nicht valide Prädikatoren - vergleiche obiges Beispiel: Bierdose in der Hand am Wasser bedeutet Mann. Es gibt Schnittmengen zwischen den beiden Ansätzen, die sich nutzen lassen. Mittels statistischer Analyse können beispielsweise Hinweise gefunden werden, was ein guter Prädiktor sein könnte.

In der Statistik dienen Variablen (Merkmale) dem Finden von (erklärbaren) Wahrscheinlichkeitswerten, während sie beim Maschinellen Lernen vielfach in Richtung Passfähigkeit für Vorhersagen ausgewählt werden. Zudem beinhalten Systeme des Maschinellen Lernens Dutzende, manchmal sogar Hunderte Variablen (Merkmale) - viel mehr als herkömmliche statistische Modelle. In der Anwendung von Maschinellem Lernen als Vorhersagewerkzeug ist das Ziel in der Regel nicht, die Bedeutung einzelner Merkmale möglichst präzise zu halten, sondern vielmehr die Vorhersagekraft eines Modells hochzutreiben.

2.3 Chancen und Grenzen von Prognosen durch Maschinelles Lernen

Die Erkennungsleistungen und Prognosen durch Maschinelles Lernen, insbesondere durch Deep Learning, können den Menschen in vielen Aufgaben unterstützen. Sie können sogar in vielen kognitiven Bereichen über die menschliche Leistungsfähigkeit hinausgehen. Ein Beispiel für eine herausragende Unterstützungsleistung in der medizinischen Diagnostik ist die Früherkennung von Herz- und Lungenkrankheiten. [8] Substanzielle Entlastungen des Menschen finden sich beispielsweise durch Anwendungen des Maschinellen Lernens in der Bild- und Spracherkennung, bei Web-Suchen, in der Betrugserkennung, bei E-Mail- bzw. Spam-Filterung und bei Kreditwürdigkeitsprüfungen. [18] Beispiele für Leistungen durch Maschinelles Lernen, die diejenigen des Menschen übertreffen, sind belegt bezüglich des Go-Spiels, selbstfahrenden Autos und Bildklassifikation. [18]

Beim Einsatz von Maschinellem Lernen gibt es auch Grenzen und Probleme, gerade auch im Themenfeld der Vorhersagbarkeit. Vier davon stehen in besonders engem Zusammenhang mit der hier behandelten Fragestellung:

- **Underfitting und Overfitting von Trainingsdatensätzen:**
  Die Intuition zu Underfitting und Overfitting trifft bereits recht gut das mit diesen Wörtern verknüpfte Problem *„Im statistischen Kontext beschreibt Underfitting, dass die Einflussvariablen die Zielvariable nicht hinreichend gut beschreiben. Das statistische Modell für die Beschreibung der Daten ist zu einfach (z. B. lineares Modell, nur eine Einflussvariable). Das Modell sagt die Zielvariable dann nicht gut genug vorher. Die Maßzahlen für die Modellgüte sind zu niedrig. Die Modellgüte erreicht keine hinreichend hohen Werte. Sinnvolle Vorhersagen sind somit nicht durchführbar. Hierfür gibt es meist zwei wesentliche Gründe:*
  1. *Das Modell, d. h. der funktionale Zusammenhang bzw. im Data Mining der gewählte Algorithmus passt nicht*
  2. *Wesentliche Einflussfaktoren wurden nicht berücksichtigt.*“ [9]

  Demnach ist das Modell beim Underfitting nicht passend bzw. „zu grob“. Beim Overfitting ist das Modell wiederum zu stark an die Trainingsdaten angepasst: *„In der Statistik spricht man von Overfitting (oder Überanpassung), wenn das Modell auf die Trainingsdaten spezialisiert ist. Im Trainingsdatensatz erzielt man dann eine sehr hohe Modellgüte. Bei Anwendung auf Testdaten ergeben sich deutlich niedrigere Werte für die Modellgüte. Das Modell ist an die Trainingsdaten übermäßig angepasst, eine Übertragung des Modells auf die Grundgesamtheit (Generalisierung) ist dadurch nicht möglich.*

Folgende Faktoren begünstigen ein Overfitting:

1. *Geringe Anzahl von Beobachtungen in der Trainingsmenge im Vergleich zu den Einflussvariablen. Insbesondere im Data Mining ist Overfitting Neural Network meist auf diesen Punkt zurückzuführen. Bei vielschichtigen neuronalen Netzen werden tausende von Parametern geschätzt!*
2. *Verzerrung (Bias) bei der Auswahl der Stichprobe aus der Grundgesamtheit.*
3. *Spezielles Overfitting Machine Learning entsteht dadurch, dass die Modelle zu sehr trainiert werden. Durch wiederholtes Aufsplitten des gleichen Datensatzes in Trainings- und Testdaten werden die Modelle immer besser hinsichtlich der Modellgüte. Wird zu viel trainiert, beschreiben die Modelle allerdings nur mehr die Trainingsdaten, eine Übertragung auf die Grundgesamtheit misslingt.“* [9]

- **Vorurteile, die in Modellen von Maschinellem Lernen entstehen:** Eine vereinfachte Version der wichtigsten Fehlerquellen wird in [15] gegeben. Sie enthält die vier Punkte: subjektive Definition von Zielvariablen, falscher Umgang mit Trainingsdaten, ungenaue Feature-Selection und Maskierung bzw. verborgene Diskriminierung.
- **Über längere Zeit nicht bemerkte Fehler wegen mangelnder Erklärbarkeit Maschineller Lernverfahren:**
  Warum bestimmte ML-Systeme entsprechende Ergebnisse generieren, wie z. B. Prognosen von Deep Neural Networks ist häufig kaum nachvollziehbar. Entsprechend stark widmet sich derzeit die Forschung diesem Aspekt. Dieser Forschungszweig heißt „Erklärbarkeit Maschineller Lernverfahren“ (Explainable Machine Learning). Solange die Wirkweise von ML-Systemen noch nicht ausreichend nachvollziehbar ist, können wesentliche Probleme in dem gelernten Vorhersagemodell über lange Zeit unbemerkt bleiben und zu Prognosefehlern führen.
- **Ergebnisse sind immer Wahrscheinlichkeiten (vgl.** [13]**)**
  Eine fundamentale Eigenschaft von Maschinellem Lernen ist, dass die Ergebnisse immer eine Wahrscheinlichkeit darstellen. Diese Wahrscheinlichkeit beschreibt die Übereinstimmung, die das trainierte System zwischen den vorliegenden Daten und den Trainingsdaten feststellen kann. Dabei besteht immer die Chance, dass das System fehlerbehaftet ist. Je nach Methode und Datengrundlage sind hier Fehlerwahrscheinlichkeiten im Bereich von einem Promille bis hin zu 20 % und mehr zu beobachten. Das Maß, in dem solche Fehler akzeptabel sind, ist stark abhängig von der Anwendung. Während im Marketing eine Fehlerrate von 20 % immer noch ein erfolgreiches Instrument beschreiben kann, ist dies in einer Sicherheitsanwendung eventuell ein Ausschlusskriterium: Ist jeder fünfte Empfänger eines Werbeschreibens nicht an einem Produkt interessiert, kann die Kampagne durchaus erfolgreich sein. Wird jede fünfte Transaktion eines Kre-

ditinstituts als Betrugsversuch angesehen und gestoppt oder jede fünfte Internetverbindung unterbunden, da das Maschinelle Lernen einen Angriff vorhersieht, ist dies für die Betroffenen unzumutbar.

Nach dieser informatischen Betrachtung von ML als Vorhersagetool folgt nun eine Darstellung der rechtlichen Lage bezüglich des Rechts auf Nichtwissen und ihrer philosophischen Bewertung, um den Problemraum aufspannen zu können.

3 Recht auf Nichtwissen

Im folgenden wird das Recht auf Nichtwissen aus dem Blickwinkel einschlägiger Urteile und Gesetze betrachtet, um aufzuzeigen, dass es in der freien Entfaltung der Persönlichkeit begründbar ist. Anschließend wird diese rechtliche Betrachtung aus einer philosophischen Sicht reflektiert. Um mögliche Auswirkungen auf den Willen und die Freiheit zu verdeutlichen, wird nachfolgend ein fiktives Szenario aufgezeigt. Abschließend wird mit philosophischen Mitteln versucht, das Argument zu verteidigen, dass die Ausübung eines Rechts auf Nichtwissen eine Ausführung der eigenen Autonomie ist und rationales Handeln ausdrücken kann.

3.1 Juristische Rahmenbedingungen

Das Recht auf Nichtwissen basiert in der Bundesrepublik Deutschland wesentlich auf Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG. Dieser Artikel (Art. 2 Abs. 1 GG) enthält ein Recht auf die freie Entfaltung der Persönlichkeit, aus welchem zum einen die allgemeine Handlungsfreiheit abgeleitet wird und zum anderen (i. V. m. Art. 1 Abs. 1 GG) das allgemeine Persönlichkeitsrecht. Dieses wurde wiederum zum Recht auf informationelle Selbstbestimmung konkretisiert.

Das Volkszählungsurteil vom 15.12.1983 des Bundesverfassungsgerichtes, durch das die informationelle Selbstbestimmung als Grundrecht anerkannt wurde, besagt, dass *„[d]iese Befugnis [der Selbstbestimmung] [...] unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes [bedarf]. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muß, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten [vgl. §2 Abs. 1 BDSG]) technisch gesehen 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.“ [5]

Im allgemeinen Persönlichkeitsrecht ist das Recht auf Nichtwissen als *„negative Variante des Rechts auf informationelle Selbstbestimmung“* [16] umfasst und bezieht sich insbesondere auf Informationen zur genetischen Veranlagung einer Person. [2]

Der Zweck des am 1. Februar 2010 in Kraft getretenen Gendiagnostikgesetzes ist die Achtung und der Schutz der Würde des Menschen, ebenso wie die Wahrung des Rechts auf informationelle Selbstbestimmung. Der BGH führt hierzu aus, dass die genetische Konstitution die Persönlichkeit des Einzelnen prägt, wesentliche Rahmenbedingungen seiner Existenz bestimmt und Informationen hierzu Aussagekraft für die persönliche Zukunft einer Person haben: *„Die Kenntnis von Erbanlagen, insbesondere genetisch bedingten Krankheitsanlagen, kann maßgeblichen Einfluss auf die Lebensplanung und Lebensführung einer Person haben und berührt deshalb unmittelbar ihr in Art. 2 Abs. 1 GG gewährleistetes Selbstbestimmungsrecht.“* [3]

Ein Recht auf Nichtwissen ist in Deutschland bisher überwiegend in Privatrechtsverhältnissen bedeutsam und fokussiert sich auf die Genomanalyse, dem Verfahren der Analyse des Erbguts eines Menschen. Im nächsten Abschnitt wird beispielhaft gezeigt, dass auch im philosophischen Kontext dieses Recht bereits gefordert wurde.

3.2 Philosophische Betrachtung

Ein Recht auf Nichtwissen hat zweierlei Funktion: Es dient als Schutz des vorhandenen Wissens sowie einer gewollten Aufrechterhaltung eines Zustands des Nichtwissens. Dieses Recht ist ein Anrecht auf ein willentliches Nicht-Wissen-Wollen.

Hans Jonas zielte 1985 im Rahmen einer verantwortungsethischen Betrachtung erstmals auf eine Forderung auf ein Recht auf Nichtwissen, um die Abwehr von identitätsstörenden Informationen zu ermöglichen.

„Niemals darf einem ganzen Dasein das Recht zu jener Ignoranz versagt werden, die eine Bedingung der Möglichkeit authentischer Tat, d. h. der Freiheit überhaupt ist; oder: Achte das Recht jedes Menschen, seinen eigenen Weg zu finden und eine Überraschung für sich selbst zu sein.“ [11, S. 190]

Jonas zeigt auf, dass dieses „Selbst-Werden“ verhindert werden kann, wenn verfügbares Wissen ungewollt gewusst werden muss. Durch diese identitäre Bewegung desjenigen Lebenskonzepts, kann die freie Entfaltung der jeweiligen Persönlichkeit eingeschränkt und manipuliert werden. Nach Hans Jonas ist diese

„Unwissenheit allerseits [...] eine Vorbedingung der Freiheit.“ [11, S. 188]

Entscheidet man sich explizit für ein Wissen-Wollen, liegt dies in der Verantwortung jedes Einzelnen und gehört zu seinem Weg des Selbst-Werdens. Diese Selbstverantwortung ist die eines mündigen, freien Menschen. Die Unwissenheit ist selbst gewollt. Man will etwas nicht wissen, man erkennt und willigt in die eigene Unwissenheit ein – nicht aus Mangel an Wissen, sondern aus dem Bewusstsein heraus, dass Selbsterkenntnis ein nachhaltigeres Konzept sein kann, als von außen auferlegte Konventionen zu übernehmen. Mit der Forderung eines Rechts auf Nichtwissen geht es um die Aufrechterhaltung des Möglichkeitsraums einer offenen, unbekannten und selbstbestimmten Zukunft.

Um mögliche Auswirkungen des Wissen-Müssen für das Individuum und die Gesellschaft aufzuzeigen, wird im kommenden Abschnitt ein fiktives Szenario dargestellt.

3.3 Fiktiver Raum und Wirklichkeit

Im Folgenden werden im Gegensatz zu unserer Wirklichkeit - in der Algorithmen noch nicht komplex genug sind, um wahre Aussagen zu treffen - beispielhaft zwei mögliche Szenarien vorgestellt, um auf den Willen und die Freiheit einzugehen. In beiden Szenarien können Algorithmen wahre, fehlerfreie Aussagen treffen.

Im ersten Szenario würde der Algorithmus voraussagen, dass ein Mensch in fünf Jahren ein Haus baut. Was würde dies nun für den Menschen bedeuten? Kann er überhaupt noch eine freie und willentliche Entscheidung treffen? Kann er sich entscheiden sein Haus nicht in fünf Jahren zu bauen? In unserem fiktiven Szenario wäre die Antwort ganz klar „Nein“. Dieser Mensch kann sich nicht mehr willentlich entscheiden, denn Maschinen treffen immer fehlerfreie Aussagen. Diese Wahlmöglichkeit wäre ihm verwehrt und der Wille würde keine Rolle spielen, denn die Vorhersage ist gesetzt.

Stellen wir uns nun Szenario 2 vor, in welchem Algorithmen fehlerfreie Vorhersagen treffen können und zugleich ein Staat utilitaristische Ziele zum Nutzen aller durchsetzen würde. In diesem Fall wäre es für das Allgemeinwohl am besten, wenn ein Mensch sein Haus in fünf Jahren baut. Was würde dies nun für diesen Men-

schen bedeuten? Es müsste bedeuten, dass dieser Staat diesen Menschen zwingt, sein Haus in fünf Jahren zu bauen, weil es für das Allgemeinwohl das prognostiziert Sinnvollste wäre. Wenn es diesen fiktiven Raum gäbe, in dem Maschinen Aussagen in die Zukunft treffen könnten und ein Staat das Allgemeinwohl über alles stellt, dann könnte eine totalitäre Herrschaftsform sich auf die technischen Möglichkeiten berufen und den menschlichen Willen entwerten.

Das Leben, wie wir es bisher kennen, mit seinen freien Entscheidungen, wäre in solchen Szenarien nicht gegeben. Würden Bürgerinnen und Bürger „Wissen-Müssen", wäre eine wesentliche Bedingung für Freiheit nicht gegeben, denn Freiheit schließt Zwang aus. Und ohne die Wahlmöglichkeit eines Rechts auf Nichtwissen wäre eine freie Willensentscheidung nicht mehr gegeben. Dies steht aber dem aufklärerischen Ideal entgegen, dass wir wissentlich unsere Entscheidungen treffen (können).

Um diesen Konflikt zu lösen, wird im folgenden Abschnitt aufgezeigt, dass bestimmte Formen des Nichtwissens durchaus wünschenswert und wollbar sind. Dafür wird sich im folgenden beispielhaft einer systematischen Behandlung der Begriffsstruktur von Thomas von Aquin beholfen, um die Voraussetzungen einer freiwilligen Handlung näher zu betrachten.

3.4 Nichtwissen und Freiwilligkeit

Friedo Ricken hat in seinem Buch „Allgemeine Ethik" [23] eine theologische Abhandlung von Thomas von Aquin aufgegriffen. Obwohl es sich hier bei Thomas von Aquin um keine normativ verfasste Abhandlung handelt, ist diese systematische Behandlung der Begriffsstruktur des Verhältnisses von Nichtwissen und Wollen bis heute eine der differenziertesten. Es geht in dieser Darstellung darum, wie sich Nichtwissen zum Wollen bzw. zur Freiwilligkeit verhält. Die Frage ist, ob Nichtwissen in irgendeiner Weise abhängig vom Wollen ist. Diese Fragestellung dient dazu, die Freiwilligkeit bzw. Unfreiwilligkeit einer Handlung festzustellen. Thomas von Aquin hat zu dem Verhältnis von Nichtwissen und Wollen drei Möglichkeiten herausgearbeitet. Die Freiwilligkeit einer Handlung ist noch nicht entschieden, sobald jemand etwas will – er muss dies auch wissentlich tun.

Am Beispiel eines Jägers werden drei Möglichkeiten von Nichtwissen und Wollen aufgezeigt. Die Geschichte, die aufgezeigt wird, handelt von einem Jäger, der bei der nächstmöglichen Gelegenheit seinen Feind erschießen will.

Die nachfolgenden drei Möglichkeiten zeigen eine systematische Differenzierung von Nichtwissen und Wollen:

1. **Das Wollen begleitet das Nichtwissen**
   Ein Jäger geht in den Wald auf Jagd und schießt auf eine irrtümlich für ein Reh gehaltene Gestalt. Im Nachhinein stellt sich heraus, dass diese Gestalt sein Feind war, den er ohnehin töten wollte. Die Frage ist nun, ob er seinen Feind freiwillig erschossen hat.
   Die Antwort hierzu lautet „Nein". Er wollte seinen Feind nicht erschießen. Warum? Man kann nichts wollen, was man nicht weiß. Wenn ich etwas will, muss ich wissen was ich will. Also ist die Handlung nicht freiwillig. Dennoch ist die Handlung nicht unfreiwillig, sie ist weder freiwillig noch unfreiwillig. Unfreiwillig ist nur, was gegen unseren Willen geschieht. Was in der Handlung geschieht, geschieht nicht gegen den Willen des Jägers, denn er wollte bei der nächsten Gelegenheit seinen Feind erschießen. Die Freude über den Tod des Feindes drückt aus, dass die Tat auch ohne seinem Wissen, seinem Wollen entspricht. Die Handlung wurde jedoch ohne Wissen ausgeführt. Und dennoch von einem Wollen begleitet, welches die Handlung bejahte.
2. **Die Unwissenheit ist Folge des Wollens**
   Hierbei wird zwischen zwei Handlungen unterschieden:
   1. Die Unwissenheit ist selbst gewollt – man will etwas nicht wissen. Zum einen, eine bewusst gewollte bzw. gesuchte Unwissenheit. Man unterlässt es absichtlich sich zu informieren, man möchte absichtlich in Unwissenheit bleiben. Thomas von Aquin begründet diese absichtliche Unwissenheit (Ignorantia affectata) damit, sich mit dieser Unwissenheit zu entschuldigen und bezeichnet diese als „sündhafte Unwissenheit".
      Eine Handlung ist durch ein absichtliches Tun gekennzeichnet und eine Unterlassung durch ein absichtliches Nicht-Tun. Die Frage ist nun ob Unterlassung eine Form von Handlung ist? Wenn ein scheinbares Nichts-Tun willensabhängig erfolgt, hat es formal den Status des Tuns. Wenn eine Person aufgrund des eigenen Willens etwas unterlässt oder absichtlich etwas nicht tut, dann heißt es nicht, dass das Wollen unabhängig von einer Handlung ist. Das bestärkt erneut die Annahme, dass unser Wille immer auf eine Handlung zielt. Somit hebt die Unterlassung in Bezug zum Wollen die Beziehung zwischen dem Tun und dem Wollen nicht auf, sondern verstärkt diese Verbindung.
   2. Zum anderen, dass man etwas nicht weiß, was man wissen könnte und wissen müsste. Man überlegt nicht, was in der betreffenden Situation zu bedenken wäre. Wie beispielsweise, dass zwischen parkenden Autos ein kleines Kind hervorrennen könnte.

3. **Die Unwissenheit und die aus der Unwissenheit resultierende Handlung ist in keiner Weise gewollt**
   Es besteht keine ursächliche Abhängigkeit zwischen Wollen und Nichtwissen. Diese Unwissenheit hebt die Freiwilligkeit auf, da das Wollen das Nichtwissen nicht begleitet – sie stehen in keinerlei Beziehung zueinander.

Warum ist Freiwilligkeit relevant für ein Recht auf Nichtwissen? Eine Handlung ist dann freiwillig, wenn sie absichtlich, mit Wissen und Willen durchgeführt wird. Das geforderte Recht auf Nichtwissen steht nicht in Zusammenhang mit verdrängtem Wissen. Unbewusstes Nichtwissen könnte z. B. dafür genutzt werden, sich im Nachhinein mit der Unwissenheit zu entschuldigen, um sich der Verantwortung der Folgen zu entziehen. In diesem Beitrag wird ein reflektiertes, aufgeklärtes Recht auf Nichtwissen betrachtet. Es handelt sich hier um ein ausdrückliches Nicht-Wissen-Wollen zum Zwecke der Unterbindung von unüberschaubaren und überschaubaren Auswirkungen. Die Möglichkeit über Kenntnis der gezogenen Schlüsse und Vorhersagen über einen selbst, muss demnach immer ein bloßes Angebot bleiben.

3.5 Aufgeklärtes Nichtwissen

Willensfreiheit ist eine Vorbedingung für Handlungsfreiheit, welche in unserem Grundgesetz von Artikel 2 Abs. 1, der freien Entfaltung der Persönlichkeit, abgeleitet wird. In diesem Beitrag wird eine Unterscheidung zwischen verdrängtem Wissen und Unwissenheit als Folge des Willens getroffen. Es handelt sich hier um ein ausdrückliches Nicht-Wissen-Wollen. Denn ein Überschuss an Wissen kann die individuellen Entfaltungsmöglichkeiten einschränken und somit ein Individuum an einer authentischen Lebensgestaltung hindern. Die hier verstandene Unwissenheit ist gewollt – man will etwas nicht wissen und man erkennt und willigt in die eigene, in diese Unwissenheit ein. Die Entscheidung, ein aufgeklärtes Recht auf Nichtwissen in Anspruch zu nehmen, kann zu einer bewussten Gestaltung der Zukunft anleiten und befreit von extern Übernommenem. Ein aufgeklärtes Nichtwissen ist stets begleitet vom Bewusstsein des eigenen Nichtwissens und somit eine beabsichtigte Entscheidung.

Im Zusammenhang mit der Entscheidungsfreiheit führt der BGH aus, dass die *„[i]ndividuelle Selbstbestimmung [voraussetzt] – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – [...], daß [sic.] 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 betreffende [sic.] Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind [...], kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“ [4]

Ein Recht auf Nichtwissen zielt auf den Schutz eines jeden Einzelnen, Wissen über seine Person, anderen oder der Person selbst zugänglich zu machen, ohne dass dies von der Person gewollt wurde. Mit dem Recht auf Nichtwissen im digitalen Kontext wird eine situationsrelevante Wahl-, Entscheidungs- und Handlungsfreiheit gefordert. Eine informierte Einwilligung ist immer dann gegeben, wenn die Entscheidung eines Menschen absichtlich, mit Verständnis und frei von kontrollierendem Einfluss anderer erfolgt.

3.6 Nichtwissen – Konform zur Aufklärung?

In seinem Buch „Vom Nutzen des Nichtwissens“ schreibt Peter Wehling, dass *„Autonomie [...] (mindestens) ebenso gut darin bestehen [kann], bewusst mit Ungewissheit und Offenheit zu leben, wie darin, das eigene Leben auf der Grundlage und nach Maßgabe tatsächlicher oder vermeintlicher Gewissheiten [...] zu planen.“* [24]

Der Wunsch auf eine offene, unbekannte Zukunft kann zu einer bewussten Gestaltung der Zukunft anleiten. Das hier geforderte Recht ist nicht mit der Aufklärung in Uneinigkeit, denn der bekannte und Gesellschaft prägende Leitspruchs Kants zur Aufklärung lautet: *„Aufklärung ist der Ausgang des Menschen aus seiner selbst verschuldeten Unmündigkeit.“* [12]

Selbstverschuldet bedeutet, dass die Fähigkeit (zu denken) vorhanden ist, aber man tut es aus Bequemlichkeit, Anpassung, Feigheit etc., nicht. *Unmündigkeit* ist die Unfähigkeit sich seines eigenen Verstandes, ohne Anleitung von außen, zu bedienen. Was braucht man laut Kant nun zur Aufklärung? *Verstand* um zwischen wahr und falsch zu unterscheiden. *Mut* sich seines Verstandes zu bedienen. *Freiheit* als Voraussetzung dies zu dürfen. Und *Vernunft* um Urteile zu fällen und die Wahrheit zu erkennen. [22]

Der Ausgang aus dieser selbstverschuldeten Unmündigkeit, sei nun im stetigen Bestreben zu finden *„[...] seine [...] Erkenntnisse zu erweitern, von Irrtümern zu reinigen [...].“* [12] In der menschlichen Wahrnehmung oft unbeachtet bleibt dabei die Einsicht, dass der Verzicht auf lebenskonzept- oder identitätsstörende Informationen, Resultat dessen sein kann, *„[...] sich seines Verstandes ohne Leitung eines anderen zu bedienen.“* [12] Ein Überschuss an *Wissen* kann das Selbst-Werden eines Menschen einschränken und die Abwehr von identitätsstörenden Informationen ist der Grund, der diese Wissensabwehr durchaus rational erscheinen lässt.

Um ein Recht auf Nichtwissen anzuerkennen, muss (natürlich) ein gewisses Wissen vorausgesetzt werden. Im Unterschied zu wirklich propositionalem Wissen unterscheidet sich das aufgeklärte Recht auf Nichtwissen dahingehend, dass dieses Recht ein Wissen über mögliche Auswirkungen dessen verlangt, welche einen gewollt zu einer Entscheidung bzw. Handlung bewegen. Dieses Nicht-Wissen-Wollen ist mehr als lediglich die Abwesenheit von Wissen, diese Entscheidung setzt Wissen über das zu Entscheidbare voraus. Diese Schwierigkeit bleibt bei der Ausübung eines Rechts auf Nichtwissen (im digitalen Kontext) bestehen.

Dass das Recht auf Nichtwissen Funktionalitäten haben kann, wird im folgenden vertieft.

4 Funktionalität von Nichtwissen

Das Kapitel „Das Geheimnis und die geheime Gesellschaft" in Georg Simmels 1908 veröffentlichtem Buch „Soziologie" beschäftigt sich mit der Funktionalität von Nichtwissen in der zwischenmenschlichen Begegnung. Demnach beruhen gelingende soziale Beziehungen nicht allein darauf, wie viel die Beteiligten voneinander wissen, sondern sie setzen *„ebenso ein gewisses Nichtwissen, ein, freilich unermeßlich wechselndes Maß gegenseitiger Verborgenheit voraus."* [19] Vertrauen bildet eine der synthetischen Kräfte in einer Gesellschaft. Wenn alle alles voneinander wüssten, müssten wir einander nicht mehr vertrauen.

In den USA gibt es ein sog. „therapeutic privilege". Dies ist das Recht des behandelnden Arztes, einem Patienten Informationen vorzuenthalten, wenn befürchtet wird, dass die Offenlegung dem Patienten unmittelbaren und ernsthaften Schaden zufügen könnte (z. B. bei Vorliegen einer schweren Depression). Dieses „therapeutic privilege" wäre nicht mehr effektiv anwendbar, wenn ein rein Maschinelles Diagnostiksystem (genauer: Quasi-Diagnostiksystem) frei verfügbar ins Internet gestellt wird. Dieser Schutz vor belastenden Informationen – seien sie falsch und selbst wenn sie richtig sind – lässt sich aus dem medizinischen Bereich auf die hiesige Problemstellung übertragen.

Wissen muss nicht unbedingt wünschenswerte Konsequenzen haben, insbesondere, wenn Wissen unvollkommen oder fälschlich generiert wurde - im Zweifelsfall sogar gegen eine Person verwendet wird. Fehlanalysen, welche das Lebenskonzept eines Menschen beeinflussen (können), sind denkbar und möglich, und gerade deswegen ist es nötig, mögliche Auswirkungen unter den Aspekt der Entscheidungsfreiheit zu stellen. Dem nichtwissenden Individuum könnten, wenn es Kenntnis über alle vorhandenen Informationen hat, belastende Konsequenzen bekannt werden und vielleicht möchte es gerade deswegen vor diesem „Wissen" geschützt werden. Es

muss eine gewollte, wissentliche und absichtliche Entscheidung bleiben, diese Information zu erhalten, denn die vermittelte Information ist irreversibel.

Systeme müssen von vornherein im Bewusstsein dieser Verantwortung entworfen und geeignete Sicherungsmechanismen implementiert werden. Inwiefern das Individuum Kenntnis von Vorhersagen über sich erhalten soll oder muss, ist eine Frage der informationellen Selbstbestimmung. Zur Wahrung der informationellen Selbstbestimmung dienen unter anderem technische Schutzmechanismen. Ein auf das Problem bezogenes Angreifermodell und technische Schutzmechanismen werden im Folgenden vorgeschlagen.

5 Angreifermodell und Schutzmechanismen

Die Beachtung des Rechts auf Nichtwissen lässt sich technisch beispielsweise mit Privatheitsmechanismen unterstützen. Hierfür gibt es verschiedene technische Mechanismen wie Selbstschutz (Filtertechnologien), Verhinderung des Entstehens (Anonymisierung bei Auswertung zur Verhinderung von Personenbezug) und kryptographische Mechanismen, die perspektivisch praktikabel werden könnten, wie Fully Homomorphic Encryption. Welche technischen Schutzmechanismen zu wählen sind, hängt essenziell von der identifizierten Bedrohung, den Schutzzielen und dem konkreten Angreifermodell ab. Eine grobe Darstellung von aus unserer Sicht plausiblen Annahmen für diese Kategorien ist in Tab. 1 dargestellt.

6 Schlussbetrachtung

Im US-amerikanischen Science-Fiction-Film Minority Report wird wegen der Existenz von false positives von vorhergesagten Morden (eine kleine Anzahl von Morden, die vorhergesagt wurden, wären retroperspektivisch auch ohne Verhaftung nicht verübt worden) das sogenannte „Precog-Programm“ eingestellt. In der Bewertung bezüglich der deutschen und EU-Gesetze hätte dieses Programm des predictive policing gar nicht gestartet werden dürfen [1]: *„Das Minority-Report-Szenario, nämlich allein auf der Basis statistischer Analysen künftige Kriminelle vorherzusagen, wäre hierzulande rechtlich gar nicht möglich. Der Bayerische Landesbeauftragte für den Datenschutz Thomas Petri, [...] sagt: ‚Das kollidiert mit dem Grundsatz der Unschuldsvermutung.‘ Außerdem seien einem derartigen Profiling ‚auch EU-rechtlich enge Grenzen gesetzt. Artikel 11 der EU-Richtlinie über den Datenschutz in der Strafjustiz untersagt jedenfalls grundsätzlich die automatisierte Einzelfallentscheidung und lässt Ausnahmen nur in engen Grenzen zu.‘“* Hier ist

Tab. 1 Wert, Bedrohung, Schutzziele, und eventuelle Angreifermodelle und technische Mechanismen des Rechts auf Nichtwissen

Kategorie	Recht auf Nichtwissen
Wert	Informationelle Selbstbestimmung, konkret: „Negative Variante des Rechts auf informationelle Selbstbestimmung“ [16]
Bedrohung	Einschränkung der Mündigkeit und Selbstbestimmung von Menschen, z. B. durch gezielt eingesetzte, plausible, ggf. psychisch belastende Information über sie selbst. Diese können beispielsweise durch einseitig gewählte Trainingsdaten erzeugt werden, was zur beabsichtigten Verzerrung von Ergebnissen führt Individuell gesehen ggf. eine gezielte Herbeiführung • mentaler Belastung • Gefährdung der persönlichen Offenheit für die Zukunft • Gefährdung der Leichtigkeit/der Unbeschwertheit der eigenen Lebensführung
Schutzziele	Kann als Ausprägung des Schutzziels „Beherrschbarkeit“ angesehen werden („Freiheit von Nebenwirkungen“) – s. Dierstein [6]: „Beherrschbarkeit (controllability) – Sicherheit vor dem System – die Sicht der Sachlage, bei der Rechte oder schutzwürdige Belange der Betroffenen durch das Vorhandensein oder die Nutzung von IT-Systemen nicht unzulässig beeinträchtigt werden“ • Variante von „Plausible Deniability“, glaubhafte Abstreitbarkeit • Variante von „Verfügbarkeit“ (vgl. Spam)
Angreifermodell	• Unternehmen im (mentalen) Gesundheitsbereich, Werbeindustrie, Versicherungsbranche • Organisationen und Staaten, die „mit der Wahrheit“ einschüchtern, verunsichern, manipulieren und Macht demonstrieren möchten
Techn. Mechanismen	Selbstschutz: Filtertechnologien (vgl. Spam) Verhinderung des Entstehens: Anonymisierung bei Auswertung zur Verhinderung von Personenbezug, Fully Homomorphic Encryption; Nichttechnische Empfehlung („Beipackzettel“), z. B.: „Wenn Sie diese Informationen konsumieren, dann könnten Sie sich nach und nach in eine Filterblase begeben – die gegebenen Vorhersagen können sich zu selbsterfüllenden Prophezeiungen ausweiten.“

ein Analogieschluss mit dem Recht auf Nichtwissen hinsichtlich durch Maschinelles Lernen erlangtem Wissen über sich selbst denkbar: Bezüglich der eigenen Entwicklung gilt der Grundsatz der „Selbstermächtigungsvermutung“. Nicht nur wegen der Existenz von falschen Vorhersagen (und seien sie noch so selten) ist das

Recht auf Nichtwissen geboten, sondern auch wegen des Rechts auf informationelle Selbstbestimmung. Das Recht auf Nichtwissen des Individuums über den Output Maschineller Lernsysteme, die mit Verhaltens-, Umgebungs- und Beziehungsdaten des Individuums trainiert wurden, muss in einer Gesellschaft durchsetzbar sein, für die die informationelle Selbstbestimmung konstituierend ist. Beim aufgeklärten Recht auf Nichtwissen ist die Willenserklärung, den Output der ML-Systeme über sich nicht kennen zu wollen keine Weltflucht, sondern ein informierter Akt und Ausdruck der Mündigkeit.

Selbst beim Gedankenexperiment einer absolut korrekten Vorhersage durch eine Maschine, bleibt das Recht auf Nichtwissen unangetastet. Menschen, die sich dazu entschließen, diese negative Variante des Rechts auf informationelle Selbstbestimmung für sich in Anspruch zu nehmen, dürfen weder negativ sanktioniert, noch diskriminiert werden.

Durch Maschinelles Lernen generierte „Aussagen" über sich selbst, können nützlich für ein Individuum sein, aber auch schädlich. Es geht um die Freiheit der Entscheidung, ob das Individuum dies wissen sollen muss oder sich dazu entschließen darf, dies nicht wissen zu wollen.

Die hier vorgelegte Betrachtung fokussierte das individuelle Recht, etwas nicht zu wissen, damit z. B. die eigene Handlungsfreiheit bestehen bleibt. Maschinelles Lernen für Vorhersagen, oder genereller predictive analytics, bedeutet allerdings auch: Andere wissen etwas über das Individuum und können damit potenziell dessen Verhalten verändern. Dies gilt für beide Fälle, nämlich, ohne dass das Individuum jemals davon erfährt und auch, dass es davon erfährt. Diese Problemstellung floss teilweise in die hiesige Betrachtung mit ein, beispielsweise bezüglich der fiktiven App EYLMAB, die für ein Punktesystem für erwünschtes soziales Verhalten verwendet wird. Diese modifizierte Fragestellung – mit dem Fokus weg vom Nichtwissen und hin zu neuartigen Machtinstrumenten durch ML – werden andere weitere Forschungsfragen aufgeworfen. In einem Interview [17] skizzierte Hauke Ritz ein entsprechendes dystopisches Szenario:

„ [...] Und aufgrund dieser Daten kann dann auch politische Macht ausgeübt werden. Wir könnten in eine Gesellschaft kommen – ich hoffe wir sind im Moment noch nicht in einer solchen Gesellschaft – aber man könnte in eine Gesellschaft kommen, wo bestimmte Leute eben nicht in bestimmte Positionen kommen und andere durchaus. Also, dass man sagt, ja im politischen Bereich möchten wir vor allem konforme Menschen haben, Menschen mit einem schwachen Rückgrat, die sich anpassen. Und anhand dieser ganzen Daten, die wir gesammelt haben, erkennen wir diese Menschen und sie lassen wir in den politischen Prozess eintreten, sie dürfen dort Karriere machen. Aber jemand, der ein bisschen eigensinnig ist, der irgendwie zu

selbstständig denkt, der sozusagen gegen den Strom schwimmt, der wird sozusagen automatisch vom Computer aussortiert. Wir schaffen es, dass seine Bewerbungen am Ende irgendwie scheitern oder ihm werden Steine in den Weg gelegt. Ich hoffe nicht, dass wir bereits in einer solchen Gesellschaft sind, aber technologisch wäre es sicher bald möglich, solche Machtmittel einzusetzen."

Wir danken den Hinweisen der Gutachterinnen und Gutachter. Stellvertretend sei Herr Dr. Carsten Ochs hervorgehoben – er hat uns hilfreiche Impulse gegeben, die unsere Argumentation stark vorangebracht haben.

Für Unstimmigkeiten und Fehler in dieser Betrachtung sind selbstverständlich wir allein verantwortlich – wir freuen uns über Hinweise hierauf!

Literatur

1. Beuth, P.: Die Polizei, dein Freund und Hellseher. https://www.zeit.de/digital/datenschutz/2017-10/pre-crime-film-predictive-policing. online: 21-October-2020
2. BGH, NJW 2014, 2190 (2191, Rn. 14)
3. BGH, NJW 2014, 2190 (2191)
4. BVerfG, NJW 1983, 209 (83, Rn. 146)
5. BVerfG, NJW 1984, 419 (422)
6. Dierstein, R.: Sicherheit in der Informationstechnik-der Begriff IT-Sicherheit. Info.-Spekt. 27(4), 343–353 Springer (2004)
7. Eisler, R.: Kant-Lexikon: Nachschlagewerk zu Kants sämtlichen Schriften, Briefen und handschriftlichem Nachlaß, 10. unveränd. Nachdr. der Ausg. Berlin G. Olm Verlagsbuchhandlung (1930)
8. Ghosh, P.: AI early diagnosis could save heart and cancer patients. https://www.bbc.com/news/health-42357257. online: 21-October-2020
9. Grünwald, D.R.: Gefährdet Overfitting die Gültigkeit Ihrer Analyseergebnisse? Mit diesen Tipps vermeidet man Overfitting und Underfitting! https://novustat.com/statistik-blog/overfitting-und-underfitting.html. online: 19-October-2020
10. Hemmerich, W.: Korrelation, Korrelationskoeffizient. https://matheguru.com/stochastik/korrelation-korrelationskoeffizient.html. online: 16-October-2020
11. Jonas, H.: Laßt uns einen Menschen klonieren: Von der Eugenik zur Gentechnologie. Technik, Medizin und Ethik: zur Praxis des Prinzips Verantwortung. Suhrkamp (1987)
12. Kant, I.: Beanwortung der Frage: Was ist Aufklärung? Stuhr (1845)
13. Kreutzer, M., Küch, O., Steinebach, M.: Eberbacher Gespräch on AI, Security & Privacy. https://www.sit.fraunhofer.de/de/reports/. online: 28-October-2020
14. Microsoft: Verbessern Sie Ihre Arbeitsmuster durch persönliche Produktivitätseinblicke. https://docs.microsoft.com/de-de/workplace-analytics/myanalytics/overview/better-work-habits. online: 16-October-2020
15. Nord, T.: Was ist algorithmische Voreingenommenheit (Algorithmic Bias)? https://www.lernen-wie-maschinen.ai/ki-pedia/was-ist-algorithmische-voreingenommenheit-algorithmic-bias/. online: 17-October-2020

16. OLG Celle, NJW 2004, 449 (450)
17. Ritz, H., Kaiser, G.: Technologie der unfreien Welt - Hauke Ritz im Gespräch. https://www.youtube.com/watch?v=Z6WWB-f7FAI, transkribiert von Michael Kreutzer. online: 06-January-2021
18. Schmidt, J., Marques, M.R., Botti, S., Marques, M.A.: Recent advances and applications of machine learning in solid-state materials science. npj Comput. Mat. 5(1), 1–36 (2019)
19. Simmel, G.: Soziologie. Untersuchungen über die Formen der Vergesellschaftung, S. 391 (1908). Otthein Rammstedt (Hrsg.). Suhrkamp, Frankfurt a. M. (1992)
20. Steiner, H.: Selbstlernende Maschinen – wie Künstliche Intelligenz entsteht. https://www.hr-inforadio.de/podcast/wissen/selbstlernende-maschinen---wie-kuenstliche-intelligenz-entsteht,podcast-episode-53312.html. online: 13-October-2020
21. Stoetter, N.: Dein Begleiter im Umgang mit deiner emotionalen Gesundheit. https://www.minddoc.de/app. online: 12-Dec-2020
22. Vgl. Kant, I.: Beanwortung der Frage: Was ist Aufklärung? Stuhr (1845)
23. Vgl. Ricken, F.: Allgemeine Ethik. W. Kohlhammer (1998)
24. Wehling, P.: Vom Nutzen des Nichtwissens: sozial-und kulturwissenschaftliche Perspektiven. Transcript (2015)

Verteilte Erreichbarkeit: Postdigitale Personalisierung durch Selfies als Gestaltungsaufgabe

Fabian Pittroff

Zusammenfassung

Personalisierung ist eine verbreitete Strategie in der digitalen Welt. In sozialen Netzen sammeln und verteilen Nutzer:innen persönliche Fragmente aus ihrem Leben, während Plattform-Unternehmen auf dieser Basis Angebote und Infrastrukturen personalisieren. Ziel des Aufsatzes ist es, in dieser Situation die These zu plausibilisieren, dass die Personalisierung aufseiten der Nutzer:innen eigenen Methoden und Zielen folgt. Dies soll beitragen zur Beantwortung der Frage, welche Weisen der Personalisierung vor einer möglichen Manipulation durch Plattformen geschützt werden sollten und welche Privatheit dabei helfen kann. Zu diesem Zweck skizziere ich erstens ein sozialtheoretisches Konzept, um Personalisierung als sozio-materiellen Aufbau von Erreichbarkeit verständlich zu machen. Personalisierung in diesem Sinne ist kein digitales Phänomen, sondern eine allgemeine Form der Identifikation menschlicher Wesen und Grundlage für persönliche Beziehungen aller Art. Zweitens präsentiere ich Ergebnisse einer autoethnografischen Studie zur Herstellung von Selfie-Fotografien, die eine mögliche Form der Personalisierung aufseiten der Nutzer:innen unter postdigitalen Bedingungen illustrieren. Die Selfie-Produktion erweist sich dabei als eine verteilte und artifizielle Weise der Gestaltung persönlicher Erreichbarkeit. Im Anschluss an diese Analysen bespreche ich drittens, welche spezifischen Schutzbedürfnisse sich daraus ergeben und welche Form des Privaten zu diesen passt.

F. Pittroff (✉)
Universität Kassel, Kassel, Deutschland
E-Mail: pittroff@uni-kassel.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_5

Schlüsselwörter

Personalisierung • Digitalisierung • Privatheit • Selfie • Nutzer:innen • Autoethnografie

1 Einleitung: Die Nutzer:innen der Digitalisierung

Personalisierung ist zu einer verbreiteten Strategie in der digitalen Welt geworden. Auf der einen Seite sammeln und verteilen Nutzer:innen mithilfe digitaler Netzwerke persönliche Fragmente aus ihrem Leben, auf der anderen verwenden Plattform-Unternehmen diese Fragmente als Ressource, um ihre Angebote personenbezogen anzupassen. Diese doppelte Personalisierung erweist sich als höchst ambivalent: Für Datenökonomien ist Personalisierung ein Mittel der Manipulation [60, S. 293–334], für Nutzer:innen ist sie die Grundlage für persönliche Beziehungen der Freundschaft oder Liebe [31, S. 13–19]. In dieser Situation gilt es nicht nur die datenökonomischen Mechanismen manipulativer Personalisierung kritisch im Blick zu behalten [23; 59; 60], sondern auch die Personalisierungsanstrengungen der Nutzer:innen als eigenständige Größe in Rechnung zu stellen. Mit dem vorliegenden Text will ich insbesondere letzteres verfolgen und die These plausibilisieren, dass es eine Personalisierung aufseiten der Nutzer:innen gibt, die eigenen Methoden und Zielen folgt. Vor dem Hintergrund dieser Arbeitshypothese stellen sich dann Fragen nach den Schutz- und Privatheitsbedürfnissen der Nutzer:innen anders: Im Zentrum eines solchen Vorgehens steht nicht die – weiterhin relevante – Frage, wie Plattformen Nutzer:innen manipulieren, sondern die komplementäre Frage, welche Weisen der Personalisierung vor einer möglichen Manipulation durch Plattformen geschützt werden sollten und welche Privatheit dabei helfen kann.

Um also die Personalisierung aufseiten der Nutzer:innen als eigenständige Größe zu untersuchen, gehe ich im Folgenden in vier Schritten vor. Zunächst möchte ich hier im ersten Teil des Textes zwei Grundbegriffe klären: Ich werde einen soziologischen Begriff der Digitalisierung vorstellen, um deren Wirkungsweise und Reichweite abzustecken, sowie einen programmatischen Nutzer:innen-Begriff einführen. Anschließend werde ich im zweiten Teil die Bedeutung der Personalisierung über die Digitalisierung hinaus verständlich machen, indem ich sie mithilfe soziologischer Theorien als eine allgemeine Form der Identifikation menschlicher Wesen beschreibe. Im dritten Teil werde ich dann Ergebnisse einer autoethnografischen Studie zur Herstellung von Selfie-Fotografien vorstellen, um

Einblicke in eine Form der Personalisierung unter postdigitalen Bedingungen zu geben. Im vierten Teil werde ich schließlich ausloten, welche spezifischen Schutzbedürfnisse sich aus diesen Analysen ergeben und was diese wiederum für die Zukunft des Privaten bedeuten.

Auf der Suche nach einer soziologischen Fassung der Digitalisierung stellt Noortje Marres die instruktive Frage, wie digitale Technologien sozial werden [35, S. 45]. Digitale Technologien sind sozial – so ihre Antwort –, insofern sie Interventionen in Sozialität ermöglichen [35, S. 61]. Digitalisierung meint dann nicht bloß die Intensivierung ansonsten stabiler Formen des Sozialen, sondern die Transformation sozialer Kategorien und Praktiken. Wer als „Freund:in" gilt und was als „privat" interpretiert wird, wird im Zuge der Digitalisierung verändert – in Auseinandersetzung mit digitalen Technologien und letztendlich auch über technische Situationen hinaus. Digitalisierung lässt sich so als allgemeiner Sammelbegriff für heterogene Interventionen digitaler Technologien in die soziale Welt verstehen. Diese Annäherung macht deutlich, dass konkrete Formen der Digitalisierung immer ein Stück weit empirisch bestimmt werden müssen. Digitalisierung als eine Menge von Interventionen zu verstehen, impliziert die Aufforderung, konkrete Einmischungen zu untersuchen und jeweils am Fall zu bestimmen, wie Digitalisierung wirkt.

Gleichzeitig lässt sich aber auch eine zusammenhängende Kultur der Digitalisierung identifizieren [1, S. 69; 54, S. 18].[1] Diese Kulturform folgt aus dem Umstand, dass der soziale Austausch heute dauerhaft und in erheblichem Ausmaß mit digitalen Technologien durchsetzt ist; viele Aspekte zeitgenössischer Sozialität bedienen sich digitaler Mittel oder haben digitale Komponenten. Digitale Technologien sind dabei in einem Ausmaß sozial geworden, das übergreifende Muster nach sich zieht, die sich zu einer postdigitalen Kultur verdichten. Das Präfix „post-" meint in diesem Zusammenhang nicht das Ende oder die Abgeschlossenheit der digitalen Transformation, sondern soll deutlich machen, dass die entsprechende Kulturform auch über digitale Technologien hinaus ihre Wirkung entfaltet [9, S. 21; 54, S. 20].[2] Digitalisierung ist also sowohl ein Haufen heterogener Interventionen digitaler Technologien als auch eine Kulturform mit

[1] Kultur bezeichnet allgemein die symbolische und sinnhafte Dimension des Sozialen [46, S. 84–89] sowie Prozesse der Verwirklichung sozialer Bedeutung durch Zeichen, Praktiken, Artefakte und Institutionen [54, S. 16]. Diese Bedeutungsproduktion geschieht nicht irgendwie, sondern selektiv; Kultur wirkt als soziales Gedächtnis, als „Filter von Vergessen/Erinnern" [32, S. 588].

[2] Im Gegensatz zu mir spricht sich Stalder trotz gewisser Sympathien gegen die Vorsilbe „post-" aus, um dem Missverständnis vorzubeugen, der (soziale) Prozess der Digitalisierung sei abgeschlossen [54, S. 20].

wiederkehrenden Mustern. Dieser Digitalisierungsbegriff schließt dann kulturelle Reflexionen und Einhegungen der Intervention digitaler Technologien in und durch das Soziale ein, denn auch scheinbar anti-digitale Techniken wie „Digital Detox“ sind erst in Auseinandersetzung mit Digitalisierung sinnvoll und als solche Teil postdigitaler Kultur [29, S. 42].

Digitalisierung in diesem Sinn betrifft schließlich nicht zuletzt die Arten und Weisen der Personalisierung. Generell ist Personalisierung kein digitales Phänomen, sondern eine allgemeine Form der Identifizierung menschlicher (und nicht-menschlicher) Wesen mit historisch und kulturell unterschiedlicher Gestalt [11, S. 181–189]. Eine Person zu sein bedeutet, als etwas erreichbar zu sein, das ein Selbstverhältnis unterhält und über eine Innenwelt verfügt [18; 33]. Personalisierung bezeichnet entsprechend den Aufbau dieser Erreichbarkeit. Ich werde die sozialtheoretische Fassung von Personalisierung im zweiten Kapitel genauer ausführen. An dieser Stelle sei festgehalten, dass der Modus der Personalisierung historisch variiert und deshalb vermutet werden darf, dass die Digitalisierung und ihre Kultur die Weisen der Personalisierung nicht unberührt lassen. Freundschaft beispielsweise – eine typische Beziehung der Personalisierung – ist heute im oben genannten Sinne postdigital, insofern sie auch mit digitalen Mitteln gepflegt wird [5, S. 16–25] und durch digitale Interventionen Wandel erfährt [4, S. 63–65]. Neben solchen Transformationen etablierter Personalisierungsweisen finden sich dann aber auch neue Formate, wie etwa jene Selfie-Fotografien, die ich im vorliegenden Text noch eingehender bespreche. Solche Mittel der Personalisierung sind – je nach sozialer und kultureller Position mehr oder weniger – essenziell, um für sich selbst und andere als Person und für persönliche Beziehungen erreichbar zu sein.

Im Folgenden werde ich insbesondere der Nutzer:innen-Seite der Personalisierung Beachtung schenken, weshalb ich an dieser Stelle kurz die Position der Nutzer:innen in der Digitalisierung besprechen will. Nutzer:innen verstehe ich nach einem Vorschlag der Medienwissenschaftlerin Olia Lialina (2012) [28] als Turing Complete Users.[3] Dieser Begriff markiert vor allem die kreativen Kompetenzen der Nutzer:innen, die grundsätzlich fähig seien, Probleme zu lösen und Ziele zu erreichen – wenn nötig auch gegen die Architektur und Gestaltung der genutzten Systeme und Infrastrukturen. Aus diesem positiven Nutzer:innen-Konzept folgen dann nicht zuletzt Annahmen über jene Situation, die ich in Kontrast zu den Personalisierungsanstrengungen der Plattformen als die

[3] „Users could more accurately be called […] Turing Complete Users, as a reference to the […] Universal Turing Machine — Alan Turing’s conception of a computer that can solve any logical task given enough time and memory. […] There is nothing one user can do, that another can’t given enough time and respect. Computer Users are Turing Complete“ [28].

Nutzer:innen-Seite der Personalisierung untersuche. Diese lässt sich mit Lialina als *Liaison* zwischen Mensch und Maschine verstehen; nicht notwendigerweise eine Beziehung wechselseitiger Kontrolle, sondern eine dynamische Situation der Aushandlung, in der Leerstellen als Spielräume genutzt werden können. Lialina spricht von Situationen, in denen „the work flow of an application has gaps that can be filled by users, where smoothness and seamlessness are broken" [28].[4] Ich stelle den folgenden Überlegungen dieses programmatische Nutzungskonzept voran, um die grundsätzliche Eigenständigkeit der Nutzer:innen-Position gegenüber infrastrukturellen Regulierungsanstrengungen zu markieren.[5]

2 Elemente einer Soziologie der Personalisierung

Personalisierung ist kein neues Phänomen, nimmt aber im Zuge der Digitalisierung neue Formen an. Mit Blick auf soziologische Theorien zeigt sich Personalisierung nicht nur als Mittel der Manipulation, sondern als grundlegende soziale Form der Identifikation und Grundlage unterschiedlicher persönlicher Beziehungsformen.[6] So kann ich im Folgenden skizzieren, inwiefern *Personalisierung als sozio-materieller Modus der Erreichbarkeit* zu verstehen ist. Ein solcher Personalisierungsbegriff erfasst dann sowohl plattformökonomische Weisen der Identifikation und Prädiktion von Personen als auch Formen der persönlichen und intimen Selbstgestaltung. Denn Personalisierung kommt nicht nur zum Einsatz, wenn Plattformen ihre Angebote anpassen und Nutzer:innen

[4] Lialina verweist damit nicht nur auf die Eigenständigkeit der Nutzer:innen, sondern skizziert außerdem ein Gestaltungsprogramm, das den kreativen Kompetenzen der Nutzer:innen Raum gibt. Damit tritt Lialina ausdrücklich in Opposition zu einer Technologie-Gestaltung, die Computer und Infrastrukturen unsichtbar machen möchte, um mögliche Reibungspunkte bei der Nutzung zu beseitigen. Angesichts lernender Algorithmen und dynamisch modulierter Entscheidungsinfrastrukturen, in denen Nutzungsverhalten reibungslos kanalisiert zu werden droht, könnte es sich lohnen, auch über weniger nahtlose Gestaltungsprinzipien nachzudenken [23, S. 54].

[5] In gewisser Weise handelt es sich um eine postdigitale Version Michel de Certeaus Theorie des aktiven Konsums. Certeaus fasst diesen als „eine andere Produktion, die als ‚Konsum' bezeichnet wird: diese ist listenreich und verstreut, […] äußert sich nicht durch eigene Produkte, sondern in der *Umgangsweise* mit den Produkten" [8, S. 13], kursiv im Original.

[6] Die grundlegende Bedeutung der Form der Person für die Erfahrung und Organisation der Welt auch über die europäische Modere hinaus steht im Zentrum jüngerer Debatten der Anthropologie [11; 58; 25]. Philippe Descola vertritt hier die These, es sei ein anthropologischer Universalismus, dass menschliche (und teils nicht menschliche) Wesen als Personen – d.h. als Dualität aus Interiorialität und Physikalität – erfahren werden und sich selbst als solche erfahren [11, S. 181–189].

zu kategorisieren suchen, sondern eben auch in den persönlichen Beziehungen der Liebe oder Freundschaft. Unter Bedingungen der Digitalisierung werden Nutzer:innen deshalb durch Plattformen personalisiert, nutzen diese aber zugleich, um sich selbst und andere zu personalisieren. Diese unterschiedlichen Situationen sollen im Rahmen einer Soziologie der Personalisierung nicht gleich, sondern vergleichbar gemacht werden. Mein Vorschlag eines sozialtheoretischen Konzepts von Personalisierung speist sich aus zwei Theorietraditionen; zum einen aus der soziologischen Systemtheorie im Anschluss an Niklas Luhmann, zum anderen aus Subjektivierungsforschungen ausgehend von Michel Foucault.

Der ersten Theorietradition – der soziologischen Systemtheorie – entnehme ich die Einsicht, dass Personalisierung soziale *Erreichbarkeit* zum Ziel hat. Person zu sein bedeutet, wiederholt als dieselbe adressiert werden zu können und über unterschiedliche Situationen hinweg erreichbar zu bleiben – nicht unverändert, aber wiedererkennbar als diese oder jene Person. Personen können in diesem Sinne auch als soziale *Adressen* verstanden werden – als Identifikationspunkte für „persönlich adressierte Erwartungen" [18; 30, S. 431]. Eine paradigmatische Form dieser Erreichbarkeit sind persönliche Beziehungen wie Freundschaft oder Liebe. Hier sind Menschen füreinander in besonders intensiver Weise zugänglich, hier ist das Netz persönlich adressierter Erwartungen besonders dicht [31, S. 14; 56, S. 447; 55, S. 73]. Personen werden aber beispielsweise auch – weniger persönlich zwar, aber ebenso wenig austauschbar – in bürokratischen Kontexten durch Steuernummern und Ausweisdokumente als bestimmte Einzelne adressiert. Mit Blick auf die postdigitale Welt sind schließlich auch die Nutzer:innen von Plattformen persönlich erreichbar; für andere Nutzer:innen – für fans, friends und followers – und ebenso für das jeweilige Plattform-Unternehmen und deren personalisierte Ansprachen in Form von Empfehlungen, Werbung und anderen Beeinflussungsanstrengungen. In all diesen Fällen geht es darum, menschliche Wesen mit persönlich zugeschriebenen Erwartungen zu belegen und so wiederholt adressierbar zu machen. Den Aufbau dieser Form von Erreichbarkeit nenne ich Personalisierung.

Was durch Personalisierung erreichbar gemacht wird, darf nicht mit einem festen Kern des adressierten Menschen verwechselt werden, sondern ist ein soziales Artefakt [30, S. 430]. Systemtheoretisch gesprochen bedeutet das, Personen sind rein kommunikative Phänomene; genauer ein „Wiedereintritt der Unterscheidung von Kommunikation und Bewußtsein auf der Seite der Kommunikation" [18, S. 62]. Das heißt, Personalisierung erzeugt soziale Adressen, denen Selbstbezug und Bewusstsein unterstellt werden kann. Personalisierung geht in diesem Sinn immer mit der Zuschreibung einer Innenwelt einher [18, S. 62 f.]. Die Systemtheorie

verortet diese Innerlichkeit und ihre Organisation in der Umwelt des Sozialen – die Person ist sozial, die Psyche individuell, und beide sind strikt voneinander getrennt, insofern sie sich durch unterschiedliche Systemoperationen organisieren. Bei der Beschreibung des Sozialen belässt es die Systemtheorie deshalb bei der Diagnose, dass Personen Selbstbezug unterstellt wird, ohne weiter zu fragen, inwiefern diese Innenwelt sozial mit konstituiert wird.

Ich möchte deshalb die systemtheoretische Theorie der Person an diesem Punkt durch Ansätze der Subjektivierungsforschung ergänzen. Letztere klammern die Selbstreferenz von Personen nicht aus, sondern untersuchen diese als Prozesse der Subjektivierung, in denen das Subjekt als „sozial-kulturelle Form“ [47, S. 47] gestaltet wird. Selbstreferenz wird so als soziale Genese von Innerlichkeit zum Thema der Analyse. Subjektivierungsforschung bedeutet dann zu untersuchen, „welches die Formen und die Modalitäten des Verhältnisses zu sich sind, durch die sich das Individuum als Subjekt konstituiert und erkennt“ [15, S. 12]. Personalisierung ist nicht gleichbedeutend mit Subjektivierung und der Konstitution von Innerlichkeit, aber jede Personalisierung hat subjektivierende Effekte, insofern die Adressierung von Innerlichkeit zu ihrer Genese beiträgt – nicht jede Subjektivierung ist persönlich, aber jede Personalisierung ist subjektivierend. Die Subjektivierungsforschung liefert der Soziologie der Personalisierung so einen wertvollen Beitrag, weil sie die im Prozess der Personalisierung referenzierte Innerlichkeit und ihre soziale Konstitution in die Analyse einbezieht.

Geht man in dieser Weise vor, stoppt die Analyse also nicht an den Grenzen von Kommunikation und Semantik, sondern geht über diese hinaus, indem man die soziale Konstitution von Innerlichkeit mithilfe der Subjektivierungsforschung zum Thema macht, bringt dies einen weiteren wichtigen Aspekt der Personalisierung aufs Tableau; ihre Materialität. Generell befasst sich die Subjektivierungsforschung mit der Konstitution von Subjekten und versteht diese ausgehend von Michel Foucault als synchron und diachron kontingente Formen menschlicher Existenz [16, S. 265]. Menschen werden zu Subjekten im Rahmen von Prozessen der Subjektivierung, in denen Selbst- und Fremdformung in kulturellen und materiellen Praktiken zusammenwirken. Subjektivität ist hier keine natürliche Form des Menschen oder Grundlage der Erkenntnis, sondern – wie es Ulrich Bröckling kompakt zusammenfasst – ein „Produktionsverhältnis“ [7, S. 22].

Analysen dieses Produktionsverhältnisses – von Michel Foucault über Gilles Deleuze bis hin zu Bruno Latour – haben durchweg die Beteiligung der materiellen Welt stark gemacht [10, S. 134 f.; 14, S. 119 f.; 27, S. 269–296]. Materialität in dieser Weise einzubeziehen, bedeutet nicht, die Sozialität der Personalisierung aufzugeben, sondern diese im Gegenteil durch eine Ausweitung des Sozialen

zu radikalisieren. Eine solche Ausweitung haben wenige so vehement vertreten wie Bruno Latour mit seiner „Soziologie der Assoziationen“ [26, S. 19–32]. Das Soziale ist hier nicht – wie aus Sicht der Systemtheorie – auf Kommunikationen beschränkt, sondern ein Modus der Assoziation und Verbindung, der ganz unterschiedliche Register der Realität verknüpft.[7] Entsprechend sind dann auch am Aufbau von Personen verschiedene, sowohl semantische als auch materielle Komponenten beteiligt, um Erreichbarkeit herzustellen und aufrechtzuerhalten.

In welcher Weise heterogene Komponenten für eine Personalisierung zusammenkommen, hat Bruno Latour mit dem Begriff der *Plug-ins* plastisch gemacht [26, S. 352–368]. Diese aus der Digitaltechnologie entlehnte Metapher referenziert die Möglichkeit, Software durch das Hinzufügen von Modulen in ihrem Funktionsumfang zu erweitern. Analog dazu markiert der Begriff im Kontext von Personalisierung, dass auch menschliche Wesen nicht schon von vornherein mit einer vollständigen Innenwelt ausgestattet sind. Stattdessen gebe es, so Latour, zahlreiche vermittelnde Komponenten, „die Individualität, Subjektivität, Persönlichkeit und Innerlichkeit befördern“ [26, S. 357]. Eben diese Mittler lassen sich mit Latour als Plug-ins bezeichnen und meinen damit all jene Elemente, die es Menschen ermöglichen, sich selbst und anderen Innerlichkeit und Intentionalität zuzurechnen. Analytisch bedeutet das, Innerlichkeit nicht vorauszusetzen, sondern nachzuvollziehen, „wie ein anonymer und generischer Körper dazu gebracht wird, eine Person zu werden: Je intensiver der Schauer angebotener Subjektivitäten, desto mehr Innerlichkeit erhält man“ [26, S. 359 f.].

Dieser knappe Durchgang einiger Elemente meines Vorschlags einer Soziologie der Personalisierung sollte verständlich gemacht haben, was es bedeutet, Personalisierung als sozio-materiellen Modus von Erreichbarkeit zu fassen. Personen sind dann aus Sinn und Materie zusammengesetzte soziale Adressen, die so stabil sind, dass sie wiederholt als solche referenziert werden können. Wie Personalisierung schließlich unter postdigitalen Bedingungen vonstattengehen kann, will ich im nächsten Teil am Fall von Selfie-Fotografien erörtern.

[7] Neben der Traditionslinie von Foucault über Deleuze zu Latour wird die Materialität sozialer Wirklichkeit und Subjektivität auch in den (feministischen) Technowissenschaften stark gemacht: Donna Haraway nennt solche Verflechtungen „material–semiotic“ (2008) [19, S. 4], Karen Barad „materiell-diskursiv“ (2012) [2, S. 20] und Annemarie Mol „socio-material“ (2010) [39, S. 266].

3 Selfies als Mittel postdigitaler Personalisierung

Selfies sind zunächst Fotografien, die Personen von sich selbst machen, um sie anschließend über Plattform-Dienste zu verbreiten [13]. Als Abbildungen von Personen – häufig persönlich erstellt und mithilfe unterschiedlicher Technologien – sind sie ein prägnanter Fall postdigitaler Personalisierung. Weil Selfies in mehrerlei Hinsicht von digitalen Infrastrukturen abhängen, sind sie in der Regel sogar in einem doppelten Sinn Mittel der Personalisierung; einerseits für Plattform-Unternehmen, die ihre Nutzer:innen zum Zwecke der Verhaltensprädiktion personalisieren, andererseits für Nutzer:innen, die mit ihrer Hilfe versuchen, für sich selbst und andere persönlich erreichbar zu sein. Im Folgenden will ich Ergebnisse einer von mir durchgeführten Studie vorstellen, die insbesondere die Nutzer:innen-Seite der Herstellung von Selfies im Blick hatte. Ziel dieser Besprechung ist es, den spezifischen Gestaltungsweisen dieser Personalisierung aufseiten der Nutzer:innen sowie ihren besonderen Schutzbedürfnissen näher zu kommen.

Ich habe oben mit Referenz auf die Subjektivierungsforschung und Latours Konzept der Plug-ins schon vorgeschlagen, Personalisierung generell als eine Versammlung heterogener Elemente zu untersuchen. Aus dieser sozialtheoretischen Perspektive sind dann auch Selfies nicht als isolierte Objekte relevant, sondern als Effekte einer sozio-materiellen Komposition, die persönliche Erreichbarkeit etabliert. Meine Annahme ist, dass sich an der Genese von Selfies nachvollziehen lässt, wie Nutzer:innen in diesem Fall versuchen, ihre Erreichbarkeit unter postdigitalen Bedingungen zu gestalten. Dieses Vorgehen erlaubt zwar keine generellen Aussagen über postdigitale Personalisierung, verspricht aber Thesen über mögliche Gestaltungsweisen, die weiter beforscht werden können.

Entscheidend für diese Herangehensweise ist nicht so sehr das fertige Foto als vielmehr die Situationen seiner Erstellung und Verbreitung, in denen die vielen beteiligten Elemente verschiedentlich in Beziehung gesetzt werden. Es gilt also auch in diesem Fall zu rekonstruieren, wie ein menschliches Wesen „durch einen Schwarm anderer Existenzformen“ [26, S. 367] dazu gebracht wird, als Person erreichbar zu sein. Dieser Ansatz erweist sich auch mit Blick auf die Forschung zum Thema als anschlussfähig; in der Literatur werden Selfies häufig nicht (ausschließlich) als fotografische Einzelobjekte untersucht, sondern als Phänomene, die mal als Objekte, mal als Praktiken wirken [13, S. 8; 34, S. 6; 48, S. 142; 52, S. 1589].

Methodisch habe ich eine autoethnografische Beobachtung der Produktion von Selfies aufseiten der Nutzer:innen durchgeführt und deren Ergebnisse mit theoretischen und empirischen Positionen aus der Literatur abgeglichen. Das heißt, ich habe selbst Selfies aufgenommen, veröffentlicht und den Prozess detailliert

in einem Feldtagebuch dokumentiert. Generell ist das Ziel ethnografischer Forschung eine narrative Datenproduktion auf Basis persönlicher Erfahrungen, die anschließend systematisch reflektiert wird [20, S. 31]. Eine autoethnografische Forschungsstrategie bietet sich in diesem Fall aus zwei Gründen an [20, S. 81–85]; zum einen verspricht der ethnografische Zugriff in Form teilnehmender Beobachtung ein hochaufgelöstes und situiertes Bild der beteiligten Elemente sowie der Praktiken, die diese Elemente verknüpfen. Zum anderen ermöglicht ein *auto*ethnografischer Ansatz die Teilnahme an den häufig stark individualisierten Situationen postdigitaler Personalisierung, die sich etwa zwischen Nutzer:innen und Smartphone abspielen und entsprechend schwer durch Dritte beobachtbar sind.[8]

Die Analyse der so entstandenen Dokumentation zeigt schließlich, dass die Herstellung von Selfies nicht nur als momenthafte Versammlung heterogener Komponenten, sondern auch als verkettete Sequenz unterschiedlicher Situationen verstanden werden muss. Besonders prägnant tritt diese Verkettung in einem Eintrag des Feldtagebuchs aus dem Januar 2019 zutage: Den Anstoß, ein Selfie aufzunehmen, gibt in dieser Episode die Rezeption anderer Selfies, die einen spezifischen Filtereffekt nutzen. Um diesen an der eigenen Person zu testen, also ein Foto mit einer spezifischen App aufzunehmen, müssen Körper, Smartphone und Raum auf besondere Weise arrangiert werden. Unter diesen Bedingungen entsteht eine Reihe von Aufnahmen, die vom Interface der verwendeten Software zur sofortigen Veröffentlichung gedrängt werden. Entgegen diesem Sog speichert sie der Nutzer[9] ab, um sie in einer nächsten Situation – an einem anderen Ort, in einer anderen Körperhaltung, mit anderer Software – zu sortieren, zu bearbeiten und mit Metadaten anzureichern, um die Aufnahme anschließend – in diesem Fall sogar erst am nächsten Tag – zu veröffentlichen. So eingespeist in die Plattform und somit anderen Nutzer:innen zugänglich gemacht, zieht das Selfie schließlich Feedback an, das dem Produzenten und Objekt des Selfies zurückgespielt wird.

[8] Ich folge hier dem von Christine Hine (2015) [20] erprobten und ausgearbeiteten Ansatz einer *ethnography for the internet*. Die Feldphase lief von Januar 2019 bis Januar 2020. Im Sinne einer Arbeitsdefinition verstehe ich solche Fotografien als Selfies, die meinen Körper zeigen und von mir selbst aufgenommen wurden [13, S. 4]. In der Feldphase habe ich 19 Posts auf der Foto-Sharing-Plattform Instagram veröffentlicht, von denen ich sieben als Selfies im Sinne der Arbeitsdefinition werte. In derselben Zeit habe ich 111 Selfies über die Story-Funktion von Instagram gepostet, die klassischen Posts im Profil haben jedoch hinsichtlich Dokumentation und Auswertung die meiste Aufmerksamkeit erfahren. Die Fotos wurden mit einem Apple iPhone 8 und ab Oktober 2019 mit einem iPhone 11 aufgenommen.

[9] Obwohl es sich beim beobachteten Nutzer auch um den Autor dieses Textes handelt, verwende ich hier und im Folgenden die dritte Person, um die methodische Distanz zwischen Praxis und Analyse zu markieren.

Über jede dieser Stationen ließe sich vieles sagen, aber an dieser Stelle geht es mir vor allem um Folgendes: Das hier verfolgte Selfie durchschreitet heterogene Situationen und jede dieser Situationen trägt dazu bei, dass es zu dem wird, was es ist. Dabei ist unklar, ob die ausgewählte Episode in ihrer spezifischen Sequenz typisch für Selfie-Produktionen ist. Darüber hinaus handelt es sich um einen spezifischen Ausschnitt der Existenz des verfolgten Selfies, da die Perspektive des beobachtenden Nutzers zeitlich und räumlich limitiert ist. Notwendigerweise unbehandelt bleibt etwa, wie das Selfie durch Rechenzentren zieht oder in den Timelines anderer Nutzer:innen landet. Nichtsdestotrotz zeigt die geschilderte Episode – ebenso wie meine autoethnografische Dokumentation insgesamt –, dass die Herstellung eines Selfies viele verkettete Situationen kennt, um zu seiner Existenz zu kommen und persönliche Erreichbarkeit aufzubauen.

Ähnliche Überlegungen zur prozesshaften Existenz von Selfies finden sich in der Literatur. So argumentiert etwa Daniel Rubinstein, Selfies zeichneten sich durch ihre Verteilbarkeit (*shareability*) aus und seien deshalb zugleich Produkt ihrer Aufnahme sowie ihrer Veröffentlichung [51, S. 173]. Das Selfie existiert nicht nur an einem Punkt, sondern durchläuft notwendigerweise mehrere Situationen. „The right question to ask is not ‚what the selfie represents' but ‚where it is'" [51, S. 175]. Ein Konzept dieser prozesshaft verteilten Existenzweise liefert Annemarie Mol mit ihrer praxeografischen Arbeit zur Untersuchung der Krankheit Atherosklerose. Auch diese durchlaufe unterschiedliche Situationen, so Mol, in denen sie auf verschiedene Weise praktisch ausgeführt (*enacted*) und erst so zur Existenz gebracht werde [38, S. 32 f.]. Die Krankheit und die von ihr befallenen Körper existierten damit ausschließlich im Prozess sozio-materieller Praktiken [38, S. 6]. Analog dazu lassen sich auch Selfies als Sequenzen unterschiedlicher Situationen und Praktiken fassen; Selfies werden im Zusammenspiel von Nutzer:in und Smartphone aufgenommen, durch Filter modifiziert, von App zu App geschoben und bearbeitet, an Plattformen übergeben, in Timelines eingeordnet und von anderen Nutzer:innen gesehen, gemocht oder kommentiert – und alle diese Situationen tragen zur Existenz eines Selfies bei.

Nachdem so hoffentlich ein Eindruck der verteilten Existenz von Selfies als Mittel der Personalisierung entstanden ist, möchte ich nun genauer bestimmen, auf welche Weise das Selfie im hier untersuchten Fall zur Personalisierung beiträgt. Noch einmal kurz zur Erinnerung: Personalisierung habe ich im zweiten Kapitel generell als den Aufbau der Erreichbarkeit einer persönlichen Innenwelt beschrieben. Eine Person zu sein bedeutet, als etwas erreichbar zu sein, das ein Selbstverhältnis unterhält. Die Analyse meiner ethnografischen Dokumentation liefert schließlich Hinweise auf eine Charakteristik der Selfie-Produktion, die in dieser Hinsicht aufschlussreich ist. Identifizierbar sind nämlich eine Reihe von

Techniken in der Herstellung der beobachteten Selfies, die ich mit dem Begriff der *Artifizialisierung* zusammenfassen möchte. Das heißt, in der Genese der Selfies finden sich zahlreiche Momente der Vermittlung und Modifizierung, die die Direktheit der Fotografie überschreiben und Künstlichkeit an deren Stelle setzten. Diese Artifizialisierung in der Selfie-Produktion wirkt schließlich – so meine These – als ein Mittel der Personalisierung, weil sie den Gestaltungsprozess unter aktiver Beteiligung der abgebildeten Person transportiert.

Welche Rolle Artifizialisierung bei der Personalisierung durch Selfies spielt, zeigt sich in meiner ethnografischen Dokumentation an einer Episode aus dem Mai 2019. Motiviert durch ein im Auge des Nutzers gelungenes Outfit, kommt die Intention zu einem Selfie auf. Um das Outfit einzufangen, werden unterschiedliche Aufnahme-Situationen erprobt und mehrere Versionen des zukünftigen Selfies angefertigt. Hierfür werden eine Reihe kleinerer Teilpraktiken ausgeführt, um etwa die Position des Smartphones und des Körpers zu variieren oder wiederholt den Selbstauslöser der aufnehmenden Software zu aktivieren. Nach der Erstellung einer zweistelligen Anzahl an Fotos, werden diese in verschiedenen Apps weiterverarbeitet; das Selfie ist hier kein einziges Bild, sondern ein Bilderhaufen, aus dem durch Sortierung, Bearbeitung und Filterung wenige weitere Bilder raffiniert werden. Veröffentlicht werden schließlich zwei Fotos; zum einen das vom Nutzer als besonders gelungen bewertete Bild, zum anderen eine missglückte Aufnahme, auf der nur unscharf die Schulter des Nutzers zu sehen ist. Im Feedback durch andere Nutzer:innen nach der Veröffentlichung wird die Kombination positiv zur Kenntnis genommen. Das feinteilig komponierte erste Bild wird also von einem (ebenfalls manipulierten) Fehlschuss begleitet, der die Künstlichkeit der Produktion transparent macht. In dieser Episode – ebenso wie an anderen Stellen in meinen Daten – zeigt sich Artifizialisierung nicht nur als Technik der Gestaltung, sondern auch als sichtbare Komponente des Selfies. Artifizialisierung macht das Selfie als Ergebnis kontingenter Selektionen sichtbar und markiert so die Beteiligung des Nutzers an der Gestaltung.

Die Künstlichkeit der Selfies ist auch in der Forschungsliteratur präsent. Ramón Reichert etwa bezeichnet Selfies als zeitgenössische Form der *prosopopeia,* d. h. als eine Technik der Personalisierung von Dingen, durch die dem Selfie die „individuelle Ausdrucksweise des Persönlichen verliehen wird“ [48, S. 141]. Diese These markiert ein weiteres Mal, dass das Selfie aktiv ausgerüstet werden muss, um seine personalisierende Wirkung zu entfalten. Dass diese Ausrüstung scheinbar widerstreitenden Anforderungen folgt, erscheint in der Selfie-Forschung teils als Irritation. So diagnostiziert Laura Maleyka, Selfies würden einerseits die Künstlichkeit der Modell- und Star-Society imitieren und andererseits versuchen, ein authentisches Bild der Person zu erzeugen [34, S. 9]. Stellt man jedoch die

Artifizialisierung von vornherein als konstitutive Technik in Rechnung, erscheint es wenig widersprüchlich oder problematisch, dass sich die Personalisierung über Selfies heterogener Ressourcen bedient. Schließlich identifizieren sowohl Brooke Wendt als auch Jill Rettberg die Filterfunktion einschlägiger Software als eine zentrale Komponente der Selfie-Produktion. Die bis zum heutigen Tag populären Filter zeigten, dass sich die Attraktivität von Selfies mithin aus der Möglichkeit speist, Versionen der eigenen Person zu erzeugen, um diese in neuer Weise zu erleben [6, S. 8]. Dabei sei es gerade die offensichtliche Künstlichkeit des Filters, die diese Distanzierung ermöglicht [49, S. 26].

Zusammenfassend möchte ich noch einmal die beiden Thesen nennen, die ich im Zuge der hier skizzierten Analyse der Personalisierung mittels Selfies aufseiten der Nutzer:innen zu entfalten versucht habe. *Erstens* handelt es sich bei dieser Form der Personalisierung um eine mehrfach verteilte Angelegenheit; für die Selfie-Produktion ist nicht nur ein Zusammenspiel heterogener Komponenten erforderlich, sondern auch eine Verkettung unterschiedlicher Situationen. *Zweitens* erweist sich Artifizialisierung als eine mögliche Technik, um Selfies zur Personalisierung zu nutzen. Künstlichkeit ergibt sich einerseits aus der verteilten Existenz der Selfies, weil die Verkettung unterschiedlicher Situationen Vermittlungen, Übersetzungen und Modifikationen notwendig macht. Anderseits befördert die Künstlichkeit des Selfies seine personalisierende Wirkung, insofern sie die Gestaltung unter aktiver Beteiligung der abgebildeten Person zugänglich macht. Die Person der Nutzer:in muss dafür nicht als kontrollierendes Zentrum aufscheinen, sondern als eine intentionale Instanz in einem Gemisch aus Effekten.

4 Schluss: Die Gestaltung persönlicher Erreichbarkeit und ihre Privatheit

Bis hierhin sollte deutlich geworden sein, inwiefern die Personalisierung aufseiten der Nutzer:innen grundsätzlich eigenen Methoden und Zielen folgt. Basis dieser These ist die sozialtheoretische Einsicht, dass Personalisierung als notwendige Bedingung persönlicher Beziehungen aller Art zu verstehen ist. Als solche ist sie kein Effekt postdigitaler Kultur oder affektives Artefakt datenökonomischer Plattformen, sondern ein darüber hinausgehender Modus der Identifikation menschlicher Wesen, der schon vor der Digitalisierung wirksam war, aber auch für das Leben in einer postdigitalen Welt bedeutsam ist. Von daher darf ich annehmen, dass Nutzer:innen digitaler Technologien im Stande sind – sowohl mit als auch ohne Plattformen –, sich selbst und andere zu personalisieren. Oder mit Olia Lialina gesprochen: „General Purpose Users can […] find a way to publish photos

online without flickr, tweet without twitter, like without facebook, make a black frame around pictures without instagram, remove a black frame from an instagram picture and even wake up at 7:00 without a ‚wake up at 7:00' app" [28].

Zusätzlich zur grundsätzlichen Rolle persönlicher Erreichbarkeit konnte ich im untersuchten Fall einer postdigitalen Personalisierung mittels Selfies zwei Charakteristiken dieses Geschehens identifizieren: Verteiltheit und Artifizialität. Diese vermitteln einen Eindruck davon, in welcher Weise Nutzer:innen-Personalisierung vonstattengehen kann und sich von den Personalisierungsanstrengungen der Plattformen unterscheidet. Dies liefert keine vollständige Beschreibung postdigitaler Personalisierung, zeigt aber, dass aufseiten der Nutzer:innen eigene Methoden und Ziele verfolgt werden. Darüber hinaus dienen mir die zwei Charakteristiken im Folgenden als Anhaltspunkte, um den spezifischen Schutzbedürfnissen der Nutzer:innen-Personalisierung sowie einer dazu passenden Formen des Privaten nachzugehen.

Dabei ist keineswegs irrelevant, dass den Personalisierungsanstrengungen der Nutzer:innen häufig datenökonomische Strategien der Plattformen gegenüberstehen, die ihrerseits Personalisierung als Mittel einzusetzen versuchen. Mit Blick auf die lebhafte Debatte um solche Strategien der Manipulation steht eine Vereinnahmung der personalisierenden Praktiken der Nutzer:innen im Sinne der ökonomischen Interessen der Plattformen zu befürchten [60, S. 278–292]. Problematisch ist dies vor allem vor dem Hintergrund des weitreichenden Einflusses der größeren Plattformen, die nicht bloß spezifische Dienste anbieten, sondern ganze Märkte oder bestimmte Aspekte zeitgenössischer Sozialität regulieren [12; 53]. Diesen Einfluss nutzten die Plattformen schließlich dazu, die Personalisierung der Nutzer:innen ökonomischen Funktionen unterzuordnen; etwa mittels einer personalisierten Modulationen von Entscheidungssituationen [59] oder einer intimen Ansprache [45]. Auf diesem Weg werden Nutzer:innen für Werbende erreichbar gemacht [40], zu mehr Aktivitäten und Veröffentlichungen verleitet [23, S. 52] oder umgekehrt in ihrer Reichweite limitiert [22]. Hier zeigt sich eindrücklich, wie Plattform-Unternehmen versuchen, Personalisierungsanstrengungen der Nutzer:innen anzuziehen, zu kanalisieren und auszubeuten.

In dieser Situation stellt sich dann um so mehr die Frage, welche Weisen postdigitaler Personalisierung jenseits der Verwertung durch Plattformen möglich und gegebenenfalls schutzbedürftig sind. Es wäre ein Fehler, an dieser Stelle wahrhaftige Formen der Personalisierung zu unterstellen, die im Umgang mit den Plattformen verfälscht würden. Die oben aufgerufene Soziologie der Personalisierung macht unmissverständlich deutlich, dass es sich bei der Erreichbarkeit einer persönlichen Innenwelt nie um einen direkten Draht zum Kern der Person handelt, sondern stets um einen kontingenten Kompositionsprozess [17, S. 210;

30, S. 430; 26, S. 360]. Es kann deshalb nicht um eine Gegenüberstellung von authentischen und verfälschten Personalisierungsweisen gehen, sehr wohl aber um unterschiedliche, möglicherweise gegenläufige Weisen der Gestaltung persönlicher Erreichbarkeit. Es ist eben dieser Hintergrund, vor dem ich vorschlage, der Debatte um datenökonomische Personalisierung als Mittel der Manipulation eine komplementäre Position hinzuzufügen, die von der Nutzer:innen-Seite ausgeht und die Frage stellt, welche Formen der Personalisierung vor einer Manipulation durch Plattformen geschützt werden können und sollen.

Wenn die Personalisierung aufseiten der Nutzer:innen als eigenständige Weise der Gestaltung in Rechnung gestellt wird, darf dabei nicht unter den Tisch fallen, dass die entsprechenden Prozesse hochgradig verteilt ablaufen können. So sind mindestens in meinem Fall der Selfie-Produktion zahlreiche Elemente jenseits der Nutzer:innen wie etwa unterschiedliche Hard- und Software-Komponenten konstitutiv am Aufbau persönlicher Erreichbarkeit beteiligt. Solche Settings als eigenständige Größe zu behandeln, kann deshalb nicht bedeuten, sie auf isolierte Intentionen individueller Nutzer:innen zuzurechnen. Stattdessen dient mir die verteilte Genese als Anhaltspunkt für die Schutzbedarfe dieser postdigitalen Personalisierung. Schutzstrategien wie klassische Formen des Datenschutzes, die eine auf das Individuum zentrierte Kontrolle anpeilen, erweisen sich in derart dezentrierten Situationen jedenfalls schnell als unrealistisch oder gar kontraproduktiv [21; 57].[10]

Geschützt werden sollte in solchen Fällen deshalb weniger der teils hohle Anspruch auf individuelle Kontrolle, sondern viel mehr die Möglichkeit, die beteiligten Komponenten im Sinne einer bestimmten Gestaltungsweise zu mobilisieren. Letztere geht nicht in individueller Kontrolle auf, sondern umfasst wechselhaftere Beziehungen zwischen Menschen und Maschine. Diese werden in der Literatur mit Metaphern wie *Liaison* [28] oder *Tanz* [24, S. 3] umschrieben, um zu markieren, dass sich Kontroll- und Handlungspotenziale im Prozess der Nutzung dynamisch verändern können. In meinem Fall liefert die beobachtete Technik der Artifizialisierung Hinweise darauf, in welcher Weise persönliche Erreichbarkeit gestaltet wird. Ziel ist hier nicht der möglichst unverstellte Zugang zur Person, sondern eine Verkettung von Vermittlungen und Modifikationen, die am Ende den Gestaltungsprozess selbst sowie die aktive Beteiligung der Nutzer:in transportiert. Der Schutzbedarf äußert sich deshalb weniger als Beschränkung

[10] Kontrollprobleme scheinen im Übrigen typisch zu sein für postdigitale Settings, die sich mithin dadurch auszeichnen, ehemals Unverbundenes über etablierte Grenzen und Kontexte hinweg zu verbinden [1, S. 20, 70; 54, S. 18].

des Zugangs zur Person und mehr als Regulierung möglicher Einflüsse auf die Gestaltung der persönlichen Erreichbarkeit.

Vor diesem Hintergrund will ich abschließend fragen, welche Rolle das Private in dieser Situation spielen kann. Verstanden als Sammelbegriff heterogener Praktiken der Beschränkung von Teilhabe, erweist sich Privatheit als historisch plastische Institution [43, S. 22–24]. Welche Praktiken der Teilhabebeschränkung jeweils als Privatheit formatiert werden, fällt abhängig von Zeit und Kultur verschieden aus. Von dieser Warte aus stellt sich dann nicht zwingend die Frage, wie Privatheit geschützt werden kann, sondern welche Privatheit einen passenden Schutz verspricht. Ohne diese Frage hier erschöpfend klären zu können, will ich auf weiterführende Ansätze verwiesen. Etablierte Prinzipien des Privaten wie individuelle Informationskontrolle [50, S. 201–215] oder Konzepte der kontextuellen Integrität [41, S. 127–148] scheinen jedenfalls mit verteilten und artifiziellen Weisen persönlicher Erreichbarkeit nur begrenzt kompatibel zu sein.

Demgegenüber lohnen sich empirische Bestandsaufnahmen der pluralen Privatheitspraktiken aufseiten der Nutzer:innen [3; 36; 42; 44]. Diese offenbaren pragmatischen Erfindungsreichtum, wenn Alternativen zu individueller Kontrolle gefragt sind. Allerdings sind viele der beobachtbaren Praktiken gegenüber mächtigen Plattformen nur beschränkt wirksam. Die institutionellen Grundlagen dafür zu schaffen, dass Nutzer:innen solche Probleme weniger individuell lösen müssen und stattdessen gerechtfertigt delegieren können, erweist sich als ebenso anspruchsvoll wie wünschenswert [57]. Insgesamt scheint hier eine Privatheit angebracht, die Möglichkeiten und Einflüsse auf die Gestaltung persönlicher Erreichbarkeit reguliert. Diese Privatheit müsste keine individuell autonome Gestaltung garantieren, sondern vielmehr unterschiedliche Personalisierungsanstrengungen so voneinander abschirmen, dass verschiedene Formen der Erreichbarkeit gelten können, ohne sich gegenseitig zu vereinnahmen [37, S. 70].

Literatur

1. Baecker, D.: 4.0 oder Die Lücke die der Rechner lässt. Merve, Berlin (2018).
2. Barad, K.: Agentieller Realismus: Über die Bedeutung materiell-diskursiver Praktiken. Suhrkamp, Berlin (2012)
3. Barth, N.: Kalte Vertrautheiten: Private Kommunikation auf der Social Network Site Facebook. Berliner Journal für Soziologie 25/4(4), 459–489 (2015).
4. Blatterer, H.: Intimacy as freedom: friendship, gender and everyday life. Thesis Eleven **132**(1), 62–76 (2016)
5. boyd, D.: It's complicated: the social lives of networked teens. Yale University Press, New Haven (2014)

6. Brooke, W.: The allure of the selfie. Instagram and the new self-portrait, Institute of Network Cultures, Amsterdam (2014)
7. Bröckling, U.: Das unternehmerische Selbst: Soziologie einer Subjektivierungsform. Frankfurt a. M, Suhrkamp (2007)
8. de Certeau, M.: Kunst des Handelns. Merve, Berlin (1988)
9. Cramer, F.: What is post-digital? In: Berry, D.M., Dieter, M. (Hrsg.) Postdigital aesthetics, S. 12–26. Palgrave Macmillan, UK, London (2015)
10. Deleuze, G.: Foucault. Suhrkamp, Frankfurt a.M. (2015).
11. Descola, P.: Jenseits von Natur und Kultur. Suhrkamp, Berlin (2013)
12. Dolata, U.: Plattform-Regulierung: Koordination von Märkten und Kuratierung von Sozialität im Internet. Berlin J. Soziol. (2020)
13. Eckel, J., Ruchatz, J., Wirth, S.: The selfie as image (and) practice: approaching digital self-photography. In: Eckel, J., Ruchatz, J., Wirth, S. (Eds.) Exploring the Selfie: Historical, Theoretical and Analytical Approaches to Digital Self-Photography. Palgrave Macmillan, Cham (2018)
14. Foucault, M.: Dispositive der Macht: über Sexualität Wissen und Wahrheit. Merve, Berlin (1978)
15. Foucault, M.: Der Gebrauch der Lüste. Frankfurt a. M, Suhrkamp (1989)
16. Foucault, M.: Die Ethik der Sorge um sich als Praxis der Freiheit. In: Foucault, M.: Ästhetik der Existenz: Schriften zur Lebenskunst, S. 253–279. Suhrkamp, Frankfurt a.M. (2013)
17. Foucault, M.: Zur Genealogie der Ethik. Ein Überblick über die laufende Arbeit. In: Ästhetik der Existenz: Schriften zur Lebenskunst, S. 191–219. Suhrkamp, Frankfurt a. M. (2013)
18. Fuchs, P.: Adressabilität als Grundbegriff der soziologischen Systemtheorie. Soziale Systeme **3**(1), 57–79 (1997)
19. Haraway, D.J.: When species meet. Univ. of Minnesota Press, Minneapolis (2008)
20. Hine, C.: Ethnography for the internet: embedded, embodied and everyday. Bloomsbury, London (2015)
21. Husemann, C, Pittroff, F.: Smarte Regulierung in Informationskollektiven - Bausteine einer Informationsregulierung im Internet der Dinge. In: Rossnagel, A., Friedewald, M., Hansen, M. (eds.) Die Fortentwicklung des Datenschutzes, S. 337–359. Springer Fachmedien, Wiesbaden (2018)
22. Köver, C., Reuter, M.: Diskriminierende Moderationsregeln. TikToks Obergrenze für Behinderungen, https://netzpolitik.org/2019/tiktoks-obergrenze-fuer-behinderungen. Zugegriffen: 10. Dez. 2020
23. Lamla, J.: Selbstbestimmung und Verbraucherschutz in der Datenökonomie. APuZ **24–26**(2019), 49–54 (2019)
24. Lange, A.-C., Lenglet, M., Seyfert, R.: On studying algorithms ethnographically: making sense of objects of ignorance. Organization. **26**(4), 598–617 (2019)
25. Latour, B.: Perspectivism: ‚Type' or ‚bomb'? Anthropol. Today **25**(2), 1–2 (2009)
26. Latour, B.: Eine neue Soziologie für eine neue Gesellschaft: Einführung in die Akteur-Netzwerk-Theorie. Frankfurt a. M, Suhrkamp (2010)
27. Latour, B.: Existenzweisen: Eine Anthropologie der Modernen. Suhrkamp, Berlin (2018)
28. Lialina, O.: Turing Complete User, https://contemporary-home-computing.org/turing-complete-user. Zugegriffen: 10. Dez. 2020

29. Lovink, G.: Sad by design: on platform nihilism (2019)
30. Luhmann, N.: Soziale Systeme: Grundriß einer allgemeinen Theorie. Frankfurt a. M, Suhrkamp (1987)
31. Luhmann, N.: Liebe als Passion: Zur Codierung von Intimität. Frankfurt a. M, Suhrkamp (1994)
32. Luhmann, N.: Die Gesellschaft der Gesellschaft. Frankfurt a. M, Suhrkamp (1998)
33. Luhmann, N.: Die Form Person. In: Luhmann, N. (Hrsg.) Soziologische Aufklärung 6, S. 142–154. Westdeutscher, Opladen (1995)
34. Maleyka, L.: Selfie-Kult: Bildvermittelte Kommunikation und Selbstbildnis als Kommunikationskode im digitalen Raum. kommunikation @ gesellschaft, 20, 1–28 (2019)
35. Marres, N.: Digital sociology: the reinvention of social research. Polity, Cambridge/UK Malden/MA (2017)
36. Marwick, A.E., boyd, D.: Networked privacy: how teenagers negotiate context in social media. New Media Soc. 16/7(7), 1051–1067 (2014)
37. Matzner, T.: Mediale und soziale Bedingtheit der Subjekte des Privaten – ein Versuch mit Hannah Arendt. In: Behrendt, H., Loh, W., Matzner, T., Misselhorn, C. (eds.) Privatsphäre 4.0, S. 55–72. Metzler, Stuttgart (2019)
38. Mol, A.: The body multiple: ontology in medical practice. Duke Univ. Pr, Durham, N.C (2002)
39. Mol, A.: Actor-Network Theory: sensitive terms and enduring tensions. Kölner Zeitschrift für Soziologie und Sozialpsychologie **50**, 253–269 (2010)
40. Muhle, F.: Stochastically Modelling the User. Systemtheoretische Überlegungen zur Personalisierung der Werbekommunikation durch Algorithmen. In: Mämecke, T., Passoth, J.H., Wehner, J. (eds.) Bedeutende Daten, S. 143–169. Springer, Wiesbaden (2018)
41. Nissenbaum, H.F.: Privacy in context: technology, policy, and the integrity of social life. Stanford Law Books, Stanford, California (2010)
42. Ochs, C., Büttner, B.: Das Internet als „Sauerstoff" und „Bedrohung". In: Friedewald, M. (Hrsg.) Privatheit und selbstbestimmtes Leben in der digitalen Welt, S. 33–80. Springer Fachmedien, Wiesbaden (2018)
43. Ochs, C.: Teilhabebeschränkungen und Erfahrungsspielräume: eine negative Akteur-Netzwerk-Theorie der Privatheit. In: Behrendt, H., Loh, W., Matzner, T., Misselhorn, C. (eds.) Privatsphäre 4.0, S. 13–31. Metzler, Stuttgart (2019)
44. Pittroff, F.: Perverse Privatheiten: Die Postprivacy-Kontroverse als Labor der Transformation von Privatheit und Subjektivität. In: Kropf, J., Laser, S. (Hrsg.) Digitale Bewertungspraktiken, S. 191–214. Springer, Wiesbaden (2019)
45. Priddat, B.P.: Das Kulturprogramm der digitalen Ökonomie: Personalisierte Märkte. ZKph **1**(1), 49–58 (2018)
46. Reckwitz, A.: Die Transformation der Kulturtheorien: zur Entwicklung eines Theorieprogramms. Velbrück Wiss, Weilerswist (2000)
47. Reckwitz, A.: Das hybride Subjekt. Eine Theorie der Subjektkulturen von der bürgerlichen Moderne zur Postmoderne (2020)
48. Reichert, R.: Selfies als Prosopopeia des Bildes. Zur Praxis der Subjektkritik in Sozialen Medien. In: Stempfhuber, M.,Wagner, E. (eds.) Praktiken der Überwachten, S. 141–155. Springer, Wiesbaden (2019).
49. Rettberg, J.W.: Seeing ourselves through technology: how we use selfies, blogs and wearable devices to see and shape ourselves. Palgrave Macmillan, New York (2014)

50. Rössler, B.: Der Wert des Privaten. Frankfurt a. M, Suhrkamp (2001)
51. Rubinstein, D.: Gift of the Selfie. In: Bieber, A. (Hrsg.) Ego update, S. 162–176. NRW-Forum, Düsseldorf (2015)
52. Senft, T.M., Baym, N.K.: What does the selfie say? Investigating a global phenomenon: introduction. Int. J. Commun. 9 (2015)
53. Staab, P.: Digitaler Kapitalismus. Markt und Herrschaft in der Ökonomie der Unknappheit. Suhrkamp, Berlin (2019)
54. Stalder, F.: Kultur der Digitalität. Suhrkamp, Berlin (2016)
55. Suttles, G.D.: Friendship as a social institution. In: McCall, G.J. (eds.) Friendship as a Social Institution, S. 95–135. Routledge, London (2017)
56. Tenbruck, F.H.: Freundschaft. Ein Beitrag zu einer Soziologie der persönlichen Beziehungen. Kölner Zeitschrift für Soziologie und Sozialpsychologie 16, 431–456 (1964)
57. Uhlmann, M.: Netzgerechte Datenschutzgestaltung. Herausforderungen, Kriterien, Alternativen. Nomos, Baden-Baden (2020)
58. Viveiros de Castro, E.B.: Kannibalische Metaphysiken: Elemente einer post-strukturalen Anthropologie. Merve, Berlin (2019).
59. Yeung, K.: Hypernudge: Big Data as a mode of regulation by design. Inf. Commun. Soc. **20**(1), 118–136 (2017)
60. Zuboff, S.: Das Zeitalter des Überwachungskapitalismus. Campus, Frankfurt New York (2018)

Anonymität

Der Wert des Anonymen

Robert Landwirth

Zusammenfassung

Das vorliegende Paper verhandelt Anonymität und Privatheit im Kontext des Internets. Wir fassen Anonymität als Differenzierung von Handlungskontexten durch Verschleierung von Identitätsmarkern. Autonomie wird mit Rössler verstanden als autonom-authentische Wahl und ihr Ausdruck in sozialem Handeln. Privatheit schützt diese Autonomie. Anonymität bezieht sich auf Privatheit technisch als kompensatorischer Schutz kontextdifferenziert gewünschten Wissens. Das Internet wird charakterisiert als Fernkommunikation, soziales Gedächtnis und Arena technischer Beobachtung. Anonymität und Privatheit werden auf die Kommunikationssituation im Internet bezogen, dabei wird herausgestellt, wie sich Darknets zu diesem Komplex verhalten. Letztlich werden einige Anmerkungen zum Wert einer „Kultur der Anonymität" gemacht.

Schlüsselwörter

Anonymität • Privatheit • Internet • Darknet • Systemtheorie

R. Landwirth (✉)
Fraunhofer SIT, Technische Universität Darmstadt, Darmstadt, Deutschland
E-mail: robert.landwirth@tu-darmstadt.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_6

1 Einleitung

Die öffentliche Debatte positioniert Darknets zwischen zwei Narrativen: Drogenverkauf und pädokriminelle Inhalte auf der einen, die Liberalisierung autoritärer Staaten auf der anderen Seite – vielleicht noch Hacker:innen und ihr Kreditkartenklau dazwischen. Mit wenigen Ausnahmen, die alternative Blickwinkel einnehmen,[1] kommt die Mehrzahl der empirischen Darknetforscher:innen zu dem Schluss, dass die dort auffindbaren Inhalte problematischen Charakters sind [4, 9, 14, 28, 34, 35, 40, 48]. Vornehmlich geht es hierbei um das Tor-Netzwerk und so wird in Konsequenz dieser Ergebnisse gefordert, *hidden services* (also das Anbieten von anonymen Diensten) zu untersagen, während das anonyme Browsen weiterhin erlaubt bleiben soll (siehe [14, 28]). Das demokratietheoretische Argument, dass Darknets positive Auswirkungen auf die Gesellschaft haben, da sie die Ausdrucksfreiheit stützen, bleibt dabei, zumindest für liberal-demokratische Staaten, Intuition.[2]

Der vorliegende Aufsatz versucht diese Intuition zu substantialisieren. Um uns dem Problem zu nähern, 1) erarbeiten wir zuerst einen Begriff von Anonymität, 2) rekonstruieren anschließend Rösslers normativen Begriff von Privatheit, wonach 3) beide Begriffe auf einander bezogen werden. 4) Folgend werden Eigenheiten des Internets als Kommunikationsraum aufgearbeitet und 5) Anonymität und Privatheit im Kontext des Internets diskutiert. 6) Schließlich wenden wir uns Darknets als Anonymisierungstechniken zu und 7) schließen mit einigen Kommentaren zu einer „Kultur der Anonymität".[3]

2 Anonymität

Ursprünglich wurde Anonymität als Phänomen der namenlosen Publikation zu Zeiten der Aufklärung relevant und im Fortlauf der Moderne zum Problem, in einer

[1] Eine ausführliche Ethnographie über Darknetkommunikation findet sich bei Gehl [11], Papsdorf liest Inhalte im Darknet als Kritik [38] und Tzanetakis untersucht, inwiefern der Drogenkauf im Internet zu *harm reduction* führen kann [53].

[2] Tzanetakis [52] weist über einen Report von Freedom House darauf hin, dass eine Reihe von Staaten bestimmte politische Diskussionen sowie Diskussionen bezüglich sexueller und religiöser Selbstbestimmung durch Zensur unterbinden. Über Darknets kann Zensur umgangen werden. Hier ist natürlich die Anbindung an liberalistische Positionen schon oberflächeneinsichtig. Allerdings bleibt die Frage offen, ob Anonymität in liberal-demokratischen Staaten ebenfalls einen Wert stellt.

[3] Dabei verstehen wir Darknets als Anonymitätsmedien, nicht nur in ihrer Technizität, sondern auch in ihrer Wahrnehmung. Deswegen diskutieren wir das Phänomen generalisiert im Hinblick auf das Internet und binden die Diskussion erst in letzter Instanz an Darknets zurück.

(wesentlich auch marktwirtschaftlichen) Entwicklung, in der ein Autorensubjekt ‚wertvoll' und „der persönliche Name des Autors die Instanz, die die Autorität eines Textes vermittelt" [36, S. 82], geworden ist (wonach sich erst Fragen von Zurechenbarkeit und Verantwortlichkeit anschließen lassen [36, S. 51 ff.]). Ein vermehrtes wissenschaftliches Interesse am Phänomen „Anonymität" erscheint wieder seit den späten 90ern mit der Verbreitung und Popularisierung des Internets. In diesen Veröffentlichungen wird Anonymität vom Verständnis als Namenlosigkeit gelöst, dabei hat sich der Aspekt der Identifikation von Personen gehalten und Anonymität wird an diesen gebunden. Anonymität steht nun in einer Dimension mit und als Gegenpol zu Identifizierbarkeit [26, 50, 54]. Eine Person, gedacht in einer sozialen Interaktionssituation, ist zuerst einmal anonym, verliert diese Anonymität allerdings durch Identifikation mit einer Identität. Im Hintergrund des Begriffs „Identität" steht dabei die Idee eines Subjekts (vermittelt Ideen von Handlungsfreiheit und Verantwortlichkeit) oder Individuums (als Zurechnung auf ein nicht teilbares Letztelement [23]).[4] Systemtheoretisch liegt es nahe (bei Anonymität) von einer Verunmöglichung der Zurechnung von Handlungen und Kommunikationen auf Personen zu sprechen.[5] „Person" ist dabei immer eine Konstruktion aus Sicht des sozialen Interaktionszusammenhangs und bestimmt als „individuell attribuierte Einschränkung von Verhaltensmöglichkeiten" [22, S. 148]. Dabei muss nicht *ein* Individuum nur *eine* Person sein. Auch unter Anonymität können (im Regelfall) handelnde Entitäten beobachtet werden und ihr Handeln zugerechnet und so quasi-persönliche Formen stellen. Im Regelfall basieren Argumente zu Anonymität allerdings auf der Vorstellung *einer* wesentlichen und mehrerer unwesentlicher Handlungsträgerschaften (also: *ein(e)* Subjekt, Individuum, Identität, Person).[6] Durch eben dieses Scheiden einer wesentlichen von unwesentlichen Handlungsträgerschaften, wird Anonymität

[4] So besonders schön bei Thiel: „Anonymität lässt sich verstehen als Zustandsbeschreibung in einer intersubjektiven Handlungssituation, in der es unmöglich ist, eine Handlung oder Kommunikation, die selbst sichtbar ist, einem Individuum oder Subjekt korrekt zuzuordnen und es hierdurch über diesen Kontext hinaus erreichbar/verantwortlich zu machen" [50, S. 153].

[5] Zum theoretischen Hintergrund siehe [24, S. 228 ff.], für einen Gebrauch in diesem Sinne [42]

[6] Siehe zu diesem Sachverhalt auch die oben zitierte Stelle aus „Soziale Systeme". Luhmann schreibt: „Beobachter können das Handeln sehr oft besser auf Grund von Situationskenntnis als auf Grund von Personenkenntnis voraussehen, und entsprechend gilt ihre Beobachtung von Handlungen oft, wenn nicht überwiegend, gar nicht dem Mentalzustand des Handelnden, sondern dem Mitvollzug der autopoietischen Reproduktion des sozialen Systems. *Und trotzdem wird alltagsweltlich Handeln auf Individuen zugerechnet.*" [24, S. 229] (Diese und alle folgenden Hervorhebungen in Zitaten sind aus dem jeweiligen Original übernommen.)

in den Dimensionen von Verantwortlichkeit,[7] „accountability“ oder Erreichbarkeit relevant [26, 33, 50, 54], denn wenn man als wesentliches Ich nicht erreichbar ist, muss man sein anonymes Handeln auch nicht verantworten.

Betrachten wir das Beispiel eines Maskenballs: Das Gesicht einer Person ist verdeckt, alles Handeln bleibt sichtbar. Man kann die Person beobachten, ihren Körper, ihre Stimme, ihre Handlungen, ihre Aussagen, man kann die Person kennenlernen und sich ein Bild von der Person am Abend des Maskenballs machen. Wenn die Maske als Anonymisierungstechnik funktioniert, wird die Zurechnung dieser situativen Erfahrung mit der Person darauf verstellt, wer diese Person ‚noch ist‘ oder ‚sonst ist‘. Die Annahme hinter der Maske als funktionierende Anonymisierungstechnik ist, dass das Gesicht einen notwendigen Indikator stellt, um eine Person zu identifizieren, um die Kenntnisse über die Person an *diesem* Abend, mit Kenntnissen über die Person *sonst* (in anderen Handlungssituationen, oder mit einer anderen Maske auch an anderen Maskenballabenden) in Verbindung zu bringen. Natürlich überbeansprucht das Beispiel die Maske als Technik, allerdings können wir anhand des Beispiels die Funktionsweise von Anonymität kenntlich machen: Anonymität beschränkt die Zurechenbarkeit von Handlungen auf ihre situativen Interaktionskontexte und entkoppelt damit Handlungsträgerschaften, die unter Voraussetzung von Allwissen auf eine ‚Superhandlungsträgerschaft‘ integrierbar wären (das Bild des Individuums und ihrer Identität).[8] Anders ausgedrückt und eine Hierarchisierung vermeidend: Anonymität verstellt die Korrelation und Aggregation von Handlungsträgerschaften (über Handlungssituationen hinweg) und damit ihre Ansprache unter einer Adresse. Die Feststellung von Anonymität ist damit auch ein Urteil über die Wiederidentifizierbarkeit von Sprecher:innen.

Beobachtungen entlang des Begriffs anonym/identifiziert geben Auskunft über die Erwartung des Beobachters[9] bezüglich der Wiederzurechenbarkeit einer Aussage in anderen Kontexten. Dabei verweisen beide Teile der Form auf ihre Gegenseite: Anonymität ist nur im Hinblick auf Identifizierbarkeit denkbar und die Zurech-

[7] „(E)in demokratischer Verfassungsstaat lässt sich nicht durch eine Ansammlung von Personen konstituieren, die sich durch ihre Anonymität jeder Adressierung von individueller und demokratischer Verantwortung entziehen“, heißt es bei Kersten [18].

[8] Wir stehen hier nahe Wallace, die Anonymität als „noncoordinability of traits“ fasst, bei ihr allerdings gekoppelt an ein ontologisches Personen- und Ordnungskonzept. „To begin, then, anonymity, is noncoordinatbility of traits in a given respect. In other words, one has anonymity or is anonymous when others are unable to relate a given feature of the person to other characteristics“ [54, S. 24].

[9] Gendergerechte Sprache wird im Rahmen des Aufsatzes im Regelfall durch Pluralisierung und Verkettung mit „:“ umgesetzt. In Ausnahmefällen findet sich die weibliche oder männliche Form. Hier, um den Bezug zu Luhmanns Theorie deutlich zu erhalten, an anderer Stelle im Sinne der Lesbarkeit. Dies gilt vor allem auch für Komposita wie „Nutzerhandlungen“.

nung als identifiziert setzt voraus, dass diese Zuschreibung verunmöglicht werden könnte. Dies gilt ebenso für die pseudonyme Kommunikation im Internet. Ohne die Verfügbarkeit weiterer Indikatoren kann die Kommunikation, die unter einem Pseudonym in einem Kommunikationsraum im Internet vollführt wird, nicht auf weitere Situationen zugerechnet werden. Es gibt technische und soziale Indikatoren, die eine solche Zurechnung erlauben.[10] Beispielsweise kann durch die Daten, die ein Browser von einem PC sendet, ein eindeutiges Profil der Nutzer:in angelegt werden, auch unter vielen Millionen Nutzer:innen.[11] Cookies und deren Aggregation sind eine weitere Option Handeln in unterschiedlichen Kontexten eindeutigen Profilen zuzurechnen sowie die IP-Adresse, solange sie konstant ist, eine situative, wenn auch relativ kurze (da sie bei jedem Verbindungsaufbau des Routers zum *Internet service provider* gewechselt wird) Zurechnung unterschiedlicher Datenströme und Nutzerhandlungen zu einem Anschluss erlauben kann. Soziale Indikatoren, die einen Hinweis darauf geben, dass Kommunikationen eventuell auf dieselbe Person verweisen, wären sozialstrukturelle und biographische Informationen, die Sprache und Eigenheiten der Ausdrucksweise oder Syntaktik.

Durch die Differenzierung von Interaktionskontexten, die von einer allwissenden Beobachterin auf einen stabilen Referenten rückgerechnet werden könnten, versichert Anonymität eine Differenzierung von Wissen, das über eine Person in diesen Interaktionskontexten besteht. Anonymität ist damit sozialpraktisch im Wesentlichen auch eine Technik zum Erwartungsmanagement. Wenn eine Gruppe von Menschen nur weiß „wer ich hier bin" und nicht weiß „wer ich noch bin", muss ich im Rahmen dieser Gruppe auch nur mein Verhalten in dieser Gruppe verantworten.[12] Durch die Herstellung von Kontextspezifizität einer Kommunikation können auch ihre Folgen besser abgesehen werden. Wenn Verhalten in unterschiedlichen Kontex-

[10] Marx [26] unterscheidet 7 Dimensionen von „identifiability": „Among 7 broad types of identity knowledge are: 1) legal name 2) locatability 3) pseudonyms that can be linked to legal name and/or locatability – literally a form of pseudo-anonymity 4) pseudonyms that can not be linked to other forms of identity knowledge – the equivalent of „real" anonymity (except that the name chosen may hint at some aspects of „real" identity, as with undercover agents encouraged to take names close to their own) 5) pattern knowledge 6) social categorization 7) symbols of eligibility/non-eligibility." Bei Nissenbaum [33, S. 141] findet sich eine ganze Liste von „information fragments", die elektronisch aufgezeichnet werden und der Idenfitikation dienen können.

[11] Die Praxis wird *browser fingerprinting* genannt. Einen einfachen Selbsttest kann jede:r unter https://amiunique.org/ (gesehen 31.10.2020) ausführen. Zum Zeitpunkt des Schreibens war mein System einzigartig unter 2.76 Mio. Nutzern identifizierbar.

[12] Dies gilt im Hinblick auf die Aufforderung, sich konstant mit vergangen Selbstdarstellungen zu verhalten [13], als auch einfach vor dem Hintergrund der Verfügbarkeit weiteren Wissens durch das kommunikativ angeschlossen werden kann.

ten von einem Beobachter auf eine stabile Person zugerechnet werden kann und wir mit der Theorie einer modernen Gesellschaft die fortschreitende Differenzierung von sozialen Kontexten, die je eigene normative Ansprüche ausbilden, unterstellen, sind die Probleme absehbar: Verhalten in Kontext B kann bei Kenntnis in Kontext A nach den Regeln von Kontext A thematisiert und hinterfragt werden. In diesem Sinne ist Anonymität eine Möglichkeit steuernd auf Kommunikation einzuwirken, indem versucht wird bestimmte Anschlussmöglichkeiten an die Kommunikation auszuschalten. Wir können in dieser Hinsicht auch sagen, dass Anonymität die Rechtfertigungskontexte für das eigene Handeln different hält.

Anonymität ist schließlich ein beobachtungsrelativer Begriff. Die Zuschreibung von Anonymität bezeichnet die Nichtbeobachtbarkeit von beobachtbar erwarteten Markern zur Integration situativen Verhaltens einer Handlungsträgerschaft in weitere Handlungskontexte derselben Handlungsträgerschaft.[13] Pseudonymität leitet die Zuschreibung auf einen von der Person selbst konstruierten Marker um. Anonymisierung kommt damit der Verschleierung von Markern gleich, die für beobachtende Personen notwendiges Wissen zur Aggregation von Handlungsträgerschaften bereithalten würden. Aus identitätstheoretischer Perspektive können wir sagen, Anonymität ermöglicht das Zuschneiden einer Selbstdarstellung auf einen Handlungskontext, ohne sich in weiteren Kontexten oder für weitere Kontexte verantworten zu müssen. Aus kommunikationstheoretischer Perspektive können wir sagen, Anonymität ermöglicht das Zuschneiden von Kommunikation auf einen Kontext ohne kommunikative Anschlüsse aus anderen Kontexten oder über andere Kontexte zu erwarten. In beiden Perspektiven ist Anonymität eine Steuerungstechnik für Erwartungen und eben damit, mit Luhmann gesprochen, eine Einschränkung der Personifikationsmöglichkeiten in Kommunikationskontexten.

Zusammenfassend können wir sagen:

- die technische Funktion von Anonymität ist die Verschleierung von Identitätsmarkern
- die soziale Funktion von Anonymität ist die Differenzierung von Handlungskontexten
- für das Individuum ist Anonymität eine Technik zum Erwartungsmanagement durch Einschränkung der Personifikationsmöglichkeiten in Interaktionszusammenhängen
- als Beobachtungsform ist die Frage nach Anonymität eine Beobachtung von Markern anhand der Unterscheidung transparent/intransparent

[13] Im Einklang damit Matthews, der Anonymität als „suite of *techniques of nonidenftifiability*" [27, S. 351] fasst.

Fundamental bleiben Aussagen über Anonymität Aussagen über Marker, spezifisch über die Nichtbeobachtbarkeit erwarteter Marker. Ich schlage deswegen vor, für die soziologische Analyse von Anonymitätsphänomenen, die typischen (sachlich relevanten) Unterscheidungen anonym/pseudonym, Anonymität/Identität, Erreichbarkeit/Nichterreichbarkeit usf., um die Form transparent markiert/intransparent markiert zu erweitern. Der Begriff der Intransparenz verweist dabei auf die Erwartung, dass etwas momentan zwar nicht beobachtbar ist, aber beobachtbar sein könnte oder sogar sein sollte und auch darauf, dass Entscheidungslagen unter Intransparenz Beobachter vor bestimmte Entscheidungsprobleme stellen [25].[14] Letztlich erlaubt die hier vorgeschlagene Fassung von Anonymität dynamisch mit Handlungsträgerschaften umzugehen, da diese nicht schon hierarchisiert in der Unterscheidung angelegt sind.[15]

3 Der Wert des Privaten

Rössler sieht persönliche Autonomie als den Kern des liberalistischen Freiheitsgedankens [43, S. 95 ff.]. Vor dem Hintergrund eines liberal-demokratischen Gesellschafts- und Menschenbilds argumentiert sie, dass Privatheit ein irreduzibler Wert ist, der für die Herausbildung und den Erhalt autonomer Subjektivität funktional notwendig ist [43, S. 135]. Autonomie ist wiederum notwendig, a) um ein selbstbestimmtes, gutes Leben zu führen und b) für eine funktionierende liberaldemokratische Gesellschaft. Zu verstehen ist:

> „Privatheit als Kontrolle über den Zugang von anderen und damit als Schutz vor dem unerwünschten Zutritt anderer – wobei dieser Zugang oder Zutritt als tatsächlicher phy-

[14] Was auch daran anschließt, dass Intransparenz aus Sicht des Individuums ein Moment von Kontrolle ermöglicht, da „Intransparenz erzeugt wird, um die Möglichkeit zu gewinnen, mit Zeit umzugehen, ohne bei Inkonsistenzen ertappt zu werden“ [25, S. 106].

[15] In sozialphilosophischer Analyse kommt Matthews zu sehr ähnlichen Ergebnissen mit zwei Differenzen. Er fasst das „sturcural aim of anonymity“ [27, S. 357] wesentlich als *untrackability* mit dem Ziel „(of) a link being made between two dissociated self-presentations“ [27, S. 355]. Er koppelt die durch Nichtverfolgbarkeit realisierte Differenzierung der Selbstpräsentationen jedoch an *eine* soziale Identität („Anonymity in these cases is realized so long as others do not aggregate pieces of personal information that are then assigned to a single indentifiable person“ [27, S. 357]). Das vorliegende Argument kann zu diesen Ausführungen zu weiten Teilen parallelisiert werden, nur führt die Fassung von Anonymität als Beobachtungsbegriff (in Essenz) dazu, von der Wahrnehmung intransparenter Markern anstatt von Nichtverfolgbarkeit als ihrem Effekt zu sprechen und die Aggregation wird durch Blickwinkelverschiebung vom Akteur auf den Interaktionskontext nicht an eine Hierarchisierung von Personenkonstrukten gekettet.

> sischer Zutritt (in Räume) und als metaphorischer Zutritt zur Persönlichkeit, und zwar im Sinne eines Zugriffs auf Informationen einerseits und im Sinne von Einspruchs- oder Verhaltensweisen andererseits bestimmt wurde; so dass sich das, was wir unter *privat* verstehen, in diese drei Hinsichten oder Dimensionen aufgliedern lässt: Privatheit des Ortes, Privatheit der Informationskontrolle und Privatheit der Entscheidung oder Handlung.“ [43, S. 84]

Privatheit ist dabei wiederum auf Schutz angewiesen und zwar durch rechtliche und soziale Normen. Das, was als privat gilt, ist nicht objektiv festzuschreiben, sondern konventionell definiert (und ändert sich damit über Zeiträume oder Handlungskontexte hinweg). Wir folgen Rösslers Arbeiten zu Privatheit durch Rekonstruktion der relevanten Begriffe (bei generellem Erhalt des Begriffsgebäudes und der Intention) und schließen mit einer zusammenfassenden (Re)deskription am Ende des Kapitels.

3.1 Autonomie

Aus der Beobachtungsperspektive einer Person besteht Freiheit allein in der Wahrnehmung verfügbarer Handlungsmöglichkeiten ohne Urteil über deren Attraktivität. Ein Wert ist Freiheit an sich noch nicht, sondern erst wenn eine Wahlmöglichkeit unter Angabe guter selbstbestimmter Gründe besteht und diese guten Gründe mit dem eigenen Selbstverständnis in Einklang stehen. Dabei ist das eigene Selbstverständnis und die damit einhergehende Genese von Wünschen und Zielen immer auch Produkt der eigenen Sozialisation. Um Autonomie emanzipatorisch zu denken, ist deswegen notwendig nicht nur von Einklang mit einem Selbstverständnis zu sprechen, sondern mögliche Selbstverhältnisse (im Sinne von Modi der identifizierenden Selbstbezugnahme) zu differenzieren. Deswegen setzt Rössler für Autonomie nicht nur Wahl im Einklang mit irgend einem Selbstbild, sondern authentische Identifikation im Einklang mit dem ‚richtigen‘ Selbstbild voraus. Die autonome Wahl verwirklicht sich schließlich im Fassen und Durchführen von Zielen und Projekten, wobei diese Ziele und Projekte wiederum Reflexionsquelle für das eigene Selbstverständnis sein können. Schließlich ist Autonomie qua authentischer Identifikation mit einer selbstbestimmten Wahl auch auf Anerkennung der Selbstdarstellungen angewiesen, in denen sie Ausdruck findet.

Wir haben damit ein Modell mit fünf Ebenen:

1. die Wahrnehmung von Möglichkeiten
2. eine selbstbestimmte Hierarchisierung dieser Möglichkeiten
3. die Übereinstimmung der eigenen Entscheidung mit einem Selbstbild

4. die Reflexion auf dieses Selbstbild als authentisch bzw. die Möglichkeit es zu ändern
5. die Möglichkeit autonom-authentische Wahl praktisch und sozial umzusetzen und aufrechtzuerhalten (qua Anerkennung)[16]

3.2 Privatheit

Wie oben erwähnt, artikuliert sich Privatheit bei Rössler in drei Dimensionen. **Dezisionale Privatheit** umfasst selbstbestimmte Lebensführung als Wahl und Ausdruck dieser Wahl. Sie artikuliert sich in der Möglichkeit, „mich im sozialen Raum *unbehelligt* so zu verhalten, so zu leben, wie ich es möchte" [43, S. 151] und zwar ohne „den unerwünschten Einspruch von anderen" und unter „Freiheit von Rechtfertigungszwängen" [43, S. 161 f.]. Im öffentlichen Raum ist dieser Schutz wesentlich realisiert durch Normen und Praxen der „Zurückhaltung, Nichtwahrnehmung, Reserve oder Indifferenz" [43, S. 153].[17] Über die Darstellungen in „Der Wert des Privaten" hinausgehend, können Momente der unbewussten Beeinflussung von Entscheidungsfindung ebenfalls dazugerechnet werden [49, S. 34 ff.]. Internetphänomene wie das Schalten manipulativer Facebookwerbung oder das Tracken und Verarbeiten von Daten, die sich in personalisierter Aufbereitung von Webseiten oder im Schalten von Werbung speisen, überschreiten die Grenzen dezisionaler Privatheit, da sie eben die autonom-authentische Entscheidungsfindung beeinträchtigen.

Informationelle Privatheit fußt auf der persönlichen Kontrolle des Wissens über die eigene Person, seine selbstbestimmte, differenzierte Weitergabe und damit einhergehend auf einer realistischen Vorstellung dessen, was von der eigenen Person in bestimmten Kontexten erwartet wird. Sie ist ebenso auf die Aufrichtigkeit von Interaktionspartner:innen angewiesen. Das selbstbestimmte und differenzierte Teilen von

[16] Trotz der Relativierung eines „wahren Kern des Selbst" [43, S. 115] in der Thematisierung von Authentizität und die Rückbindung von Autonomie an intersubjektive Handlungsprozesse [43, 108] bleibt das zugrundeliegende Handlungsmodell rationalistisch (das natürlich aus gutem Grund und in Einklang mit ihrer liberalistischen Beobachtungsposition; für eine Diskussion der Struktur und Implikationen rationalistischer Handlungsmodelle siehe [16]). Besonders deutlich zeigt sich dies in einer Betonung der expliziten Entscheidung. Beispielsweise vor dem Hintergrund einer soziologischen Identitätstheorie müsste man die Beschreibungen der selbstbezogenen Deliberation und des Fassens von Zielen und Projekten um eine (vielleicht sogar wesentlichere) implizit-unbewusst-körperliche Ebene der Identifikation und Entscheidungsfindung erweitern (siehe dazu bspw. [17, S. 157 ff.]).

[17] Sie schließt dort bspw. an Goffmans Beschreibung von „civil inattention" an, eine Form alltäglicher, respektvoller und aktiv hergestellter Nichtinteraktion; dazu Wesentliches u. a. in Goffmans „Behavior in Public Places" [12, S. 83 ff.].

Wissen einerseits und die Vertrauenswürdigkeit von Interaktionspartner:innen andererseits, sind notwendig, um sich kontextgerecht authentisch verhalten zu können, denn 1) abhängig von kontextspezifisch verfügbarem Wissen entstehen Erwartungen, die die Grundlage dafür schaffen, was es in den Augen anderer (aber auch im eigenen Selbstverständnis) heißt, sich authentisch zu verhalten. Rössler schreibt:

> „Deshalb will ich vorschlagen, generell Verletzungen informationeller Privatheit zu verstehen und zu interpretieren als falsche oder enttäuschte Erwartungen: hinsichtlich des Wissens und damit einer bestimmten Haltung oder Einstellung von Interaktions- und Kommunikationspartnern einer Person gegenüber. Spezifikum der Verletzung informationeller Privatheit ist also, dass es sich um Erwartungen und Annahmen darüber handelt, was diese anderen Personen oder Institutionen jeweilig über eine Person wissen, wie sie an Ihr Wissen gelangt sind, und damit, *in welcher Beziehung* sie *aufgrund dieses Wissens* zu ihr stehen" [43, S. 205].

Der Hintergrund dieses Problems ist, dass Erwartungserwartungen an andere mein Verhalten zuforderst moderieren und enttäuschte Erwartungen aufgrund fehlerhafter Erwartungserwartungen zu Konflikten führen können. 2) Durch die Asymmetrisierung von Wissen werden bestimmte Typen von Beziehungen mitbestimmt oder ermöglicht. Gerade die intime Beziehung, die sich in einem Kontext realisiert, „in dem man davon ausgehen kann, dass die in die Kommunikation eingebrachten Standpunkte keine nicht-involvierten Standpunkte einer Beobachterperspektive sind, dass also ein sympathetisches Interesse der Personen untereinander gegeben ist" [43, S. 238], hat eine Differenzierung der mitgeteilten Informationen nach sozialem Kontext als Voraussetzung. Die Interaktion in intimen Beziehungen ist eine der Hauptressourcen in denen sich die Identität der Person dialogisch konstituiert und ist deshalb a) auf den Schutz der Privatheit angewiesen, der diese Form von Interaktion ermöglicht und b) auf den Schutz der internen Struktur dieser Interaktionsform, gestellt durch die Interaktionspartner:innen selbst. Das heißt, es wird erwartet, dass sich Partner:innen sympathetisch, authentisch und aufrichtig zeigen und sorgsam mit den geteilten Informationen umgehen, da sie sich um den Stellenwert und die Fragilität der Situation bewusst sind.

Lokale Privatheit fordert unbeobachtete Räumen, die der eigenen Kontrolle unterliegen. Rössler konstatiert privaten Räumen einerseits die Möglichkeit einer persönlich-bedeutsamen Selbstgestaltung des Raums durch private Objekte (die durch den Raum als private Objekte konstituiert werden können) und weiterhin des versicherten ‚Für-sich-seins'. Diese Beobachtungs- und Erwartungsfreiheit ermöglicht auszuprobieren, „wer man sein will".[18] Die private Wohnung kann eine

[18] Mit Kaufmann können wir vom Erproben möglicher Selbste sprechen [17, S. 78 ff.].

absolute „Hinterbühne“ [13] stellen (also eine in Freiheit jeglichen Darstellungszwangs)[19], dies aber nur unter Ausschluss der Anwesenheit und des Blickes (sie bezieht sich hier auf Sartre) jeglicher anderer, da „in intersubjektiven Beziehungen zum anderen sich immer auch eine Festlegung, ein Ausschluss von Möglichkeiten des Sich-zu-sich-verhaltens und der Selbstinterpretation zum Ausdruck bringt“ [43, S. 273]. Die Notwendigkeit dieser Rückzugsmöglichkeiten ist nicht nur relevant in Bezug auf unbestimmte andere, sondern auch in (intimen) persönlichen Beziehungen. Letztlich ermöglicht lokale Privatheit auf Dauer gesetzte Sorgebeziehungen in einem Haushalt (ihre Definition von Familie [43, S. 283]) sowie körperliche Intimität bzw. die freie Inszenierung von Körperlichkeit [43, S. 270 f.]. Sie schreibt zusammenfassend: Lokale Privatheit schätzen wir,

> „weil sie die Möglichkeit bietet, ungestört und ungesehen mit sich allein zu sein; eine Möglichkeit, die für das gelungene Erproben, Erlernen, Suchen von (Aspekten von) Autonomie unerlässlich scheint. Mit sich allein zu sein, um so autonom und authentisch zu suchen, was man will und »wer man sein möchte«, ist offenbar ein zentraler Aspekt dessen, warum wir die einsame Privatheit suchen und schätzen“ [43, S. 304].[20]

Damit schließen wir unsere Rekonstruktion von Rösslers Begrifflichkeiten ab. Wir können sie nun zusammenfassend reformulieren. Bei **dezisionaler Privatheit** geht es um die Kontrolle ungewollter Kommunikation als ungewolltes Thematisieren der eigenen Lebensentscheidungen, jedoch bei Erhalt der Beobachtbarkeit des Handelns (also in sozialen Situationen, in denen das Leben der eigenen Entscheidung grundsätzlich hinterfragbar ist). Dieses Erfordernis entspringt Rösslers Fassung von Autonomie, da Autonomie nicht nur auf die eigenständige Wahl, sondern wesentlich auch auf Möglichkeiten ihres Ausdrucks in Handlungen angewiesen ist. Das heißt, es geht um einen Ausschluss ungewollter Kommunikation bei Erhalt eben der Möglichkeit dieser ungewollten Kommunikation. Das heißt auch, dass Privat-

[19] Sie verweist hier selbst auf Goffman, bei dem die Hinterbühne allerdings immer relativ zum Verhältnis Publikum/Darsteller zu sehen ist. (Eine Differenz die auch von Rössler weiter unten im Text diskutiert wird.)

[20] In der stärksten Fassung von lokaler Privatheit, die Selbstbezüge voraussetzt, die auf Nichtwahrnehmung angewiesen sind, ist die Ermöglichung ihrer Funktionen natürlich direkt an privat kontrollierte Räume gekoppelt. Es ist allerdings davon auszugehen, dass auch in der Öffentlichkeit, Selbsterkundung und Selbstthematisierung in den von Rössler beschriebenen Formen möglich sind. Mir ist nicht einsichtig, wieso die Kontemplation auf der Parkbank oder das Sitzen an einem Gruppentisch im Zug diese Formen der Selbstbezugnahme ausschließen sollte. Wenn Nassehi über Fremdheit schreibt [31, S. 41 ff.] und beschreibt, wie sich beim Zugfahren an seinem Gruppentisch eine gemeinsam geteilte Situationsdefinition einspielt, in der niemand den anderen stört und er sich so der Arbeit widmen kann, wäre es genauso vorstellbar, dass er in dieser Situation in Selbstreflexion die Aussicht genießt.

heit in diesem Sinne auf soziale Regulation angewiesen ist. In einem weiteren Sinne geht es bei dezisionaler Privatheit um den Ausschluss unbewusster oder zumindest ungewollter Information (Beeinflussung) der eigenen Entscheidung.

Bei **informationeller Privatheit** geht es um Kontrolle ungewollter Beobachtung (zur Herstellung von Erwartungssicherheit über das Wissen anderer) und dies ebenfalls bei Erhalt der Beobachtungsmöglichkeiten. Gewünscht ist die Versicherung korrekter Vorstellungen der Person über die Erwartungen in einem interaktiven Zusammenhang an sie, über die Art des interaktiven Zusammenhangs und ebenso die Integrität von Beziehungen und der Sich-beziehenden selbst. (Die Integrität einer Beziehung muss vor Beobachtung durch Dritte geschützt sein, aber auch: die Integrität einer Beziehung muss durch die Aufrichtigkeit der Teilnehmer:innen gewahrt bleiben.)

Bei **lokaler Privatheit** geht es um Kontrolle ungewollter (auch Kommunikations- und Beobachtungs-, aber spezifisch) Wahrnehmungsmöglichkeiten (also eine Radikalisierung, bei der schon die achtsame Anwesenheit anderer einschränkend ist) und so um die Etablierung maximaler subjektiver Erwartungssicherheit und Einschränkungsfreiheit. Auch hier ist der Schutz der Privatheit auf Rechte (Unverletzlichkeit der Wohnung) und Normen (dass man klopft, bevor man einen Raum betritt) angewiesen, aber eben nicht auf eine soziale Regulation der momentären Interaktionssituation oder den Schutz von sozialen Situationen an sich.

Zusammenfassend können wir damit sagen: Mechanismen zum Schutz von Privatheit sind solche, die Nichtkommunikation, Nichtbeobachtung und Nichtwahrnehmung (in je individuell bestimmter Hinsichtnahme) versichern können.

4 Der Wert des Anonymen

Durch die Begriffsrekonstruktion wird ersichtlich, wie Privatheit und Anonymität aufeinander bezogen werden können. Das Differenthalten von Handlungskontexten und damit das Situieren von Selbstdarstellungen macht Anonymisierung zu einer Technik, die informationelle und dezisionale Privatheit schützen kann. Wissen über das Handeln von Personen wird dabei nicht durch eine Verunmöglichung von Beobachtbarkeit geschützt, sondern indirekt, durch eine Verunmöglichung der Aggregation von Wissen. Anonymität schützt die Autonomie der Person (über Privatheit), indem sie ihr Selbstpräsentationen ermöglicht, deren Interpretation durch einen ‚breiteren' Blick auf die ‚Gesamtheit' der Person verstellt ist. Sie ist damit eine kompensatorische Technik zum Erwartungsmanagement, die von sozialer Rücksichtnahme unabhängig ist. Diese ‚praktische Anonymität' ist darauf angewiesen, dass Beobachter kein weiteres Wissen zur Integration von Handlungen aus unter-

schiedlichen Handlungskontexten besitzen (die beobachtete Person also intransparent markiert ist) und sie funktioniert in Interaktionen zwischen Unbekannten auf der Straße und Interaktionen zwischen Unbekannten im Internet gleich. Sie enthebt auch nicht von situativen Rechtfertigungszwängen (da das situative Handeln weiter beobachtbar bleibt). Damit schützt sie dezisionale Privatheit auch nur eingeschränkt.[21] Wenn man sagen kann, dezisonale Privatheit wird durch Anonymität geschützt, dann nur in dem Sinne, dass Wissen zum Hinterfragen einer Entscheidung nicht vorhanden ist. Anonymität erhält also ihren Wert wesentlich im Bezug auf Privatheit und dabei vor allem auch in Bezug auf die Dimension der informationellen Privatheit.[22]

Ich möchte hier jedoch vorschlagen, Anonymität auch als ‚Wert an sich' zu verhandeln. Rössler, die den Wert von Anonymität auf Privatheit engführt, trifft genau den Kern dieses Gedankens, wenn sie zu Beginn ihres Aufsatzes schreibt, dass „man sich als anonyme Person in der Öffentlichkeit bewegen will *als ob man nicht bekannt, als ob man namenlos sei,* als ob man gleichsam das *Schutzschild des Privaten* mit sich herumtrage." [41, S. 29] Die Krux liegt im „als ob". Sozialtechnisch schützt Anonymität Privatheit durch Differenzierung von Handlungskontexten, aus Sicht der Akteure ist aber ein nicht-technischer Effekt dessen wesentlich: Die Wahrnehmung einer Situation als anonym verbürgt eine bestimmte Form von Handlungsfreiheit vor dem Hintergrund des Fehlens personengeschichtlicher Bindungen einerseits und vor dem Hintergrund eines bestimmten Gefühls von Verantwortungsfreiheit (oder vielleicht zutreffender: geänderter Verantwortlichkeit) andererseits. Dieses Gefühl entspringt dabei wesentlich der Wahrnehmung der Interaktionssituation als „anonym" und damit bspw. als eine Situation, in der das eigene Verhalten in dieser Situation nicht im ‚sozialen Gedächtnis' gespeichert wird, sondern mit der Interaktionssituation vergeht. Diese (Wahrnehmung von) Handlungs- und Verantwortungsfreiheit verbürgt Gestaltungs- und Ausdrucksmöglichkeiten different zum alltäglichen Verhalten. Tatsächlich gibt es eine Reihe von Ritualen[23], die Normalitätserwartung aussetzen. Man denke an eine Faschingsfeier und im Rahmen solcher Situation könnten wir sagen: Hier schützt nicht Anonymität Privatheit, sondern Privatheit schützt Anonymität qua Norm. Es ist in diesem Sinne (also in der Wahrnehmung positiv bewerteter konstitutiver Anonymität, die sich im Fehlen von, oder im nicht beharren auf, personengeschichtliche(n) Bindungen und/oder in geänderter

[21] Prima facie ist auch nicht ersichtlich, dass sie vor unbewusster Beeinflussung schützt – wir kommen darauf zurück.

[22] In ihrem Aufsatz „Anonymität und Privatheit" macht Rössler diesen Punkt stark [42, S. 30]; ähnlich u. a. [26, 54].

[23] Im Sinne von Interaktionsritualen, siehe [7].

Verantwortlichkeit zeigt), dass das Internet der 90er in der Hoffnung freier Identitätsgestaltung und egalitärer Kommunikationsmöglichkeiten thematisiert wurde, es ist in diesem Sinne, dass Barlow 1996 „A Declaration of Independence of Cyberspace“ [3] schreibt und es ist auch in diesem Sinne, dass Serres (bzw. sein Übersetzer) 2013 exklamiert: „Erfindet euch neu!“ [45]. Während Anonymität also Privatheit schützt, die sich in Handlungsfreiheit durch autonome Wahl substantialisiert, gilt ebenso umgekehrt Anonymität als Wert, der durch eine Norm von Privatheit geschützt werden kann und sich in Autonomie unter der Annahme erweiterter Handlungsfreiheit zeigt.[24]

Nichtsdestotrotz bleibt Anonymität vornehmlich auch Technik und zwar Technik, die durch das Versichern von Nichterreichbarkeit eine Möglichkeit bietet eigenes Verhalten nicht verantworten zu müssen. An diese Dimension schließt sich dann die Diskussion um das Internet als abrasivem Kommunikationsraum und an das Darknet als Medium für Kriminelle an. Dies bringt uns zur Besprechung der Kommunikationssituation im Internet.

5 Internet

Die folgenden Überlegungen konzentrieren sich auf synchrone und asynchrone schriftliche Interaktionsformen im Internet. Natürlich ist auch Internettelefonie oder Internettelefonie unter der Zugabe von Telepräsenz bzw. Sonderformen wie Spiele über das Internet als Kommunikationsform zu denken, die wesentliche Kommunikation über das Internet findet allerdings textuell, also über Microbloggingdienste und soziale Netzwerke, Foren, *direct messaging* und Kommentarboxen statt.

5.1 Fernkommunikation

Die Kommunikation im Internet ist durch Fernpräsenz charakterisiert. Damit befinden wir uns in einer Kommunikationssituation, die die Interaktion zwischen Teilnehmer:innen, im Gegenzug der von Goffman erarbeiteten Situation der Interaktion in Kopräsenz, unter maßgeblich andere Bedingungen stellt. In Goffmans Interaktionssituation ist körperliche Anwesenheit wesentliches, situativ die Interaktion

[24] Wir behaupten damit, dass die Wahrnehmung von Anonymität bzw. sozialen Verhältnissen als anonyme a) ein Gefühl von Handlungsfreiheit vermittelt und b) eben durch Normen der Zurückhaltung geschützt werden kann. Also, dass ein Konsens zwischen Teilnehmer:innen besteht, die (intransparenten Marker der) Anonymität nicht ‚aufzubrechen‘, sondern im Sinne von Privatheit gewähren zu lassen.

strukturierendes Merkmal. Interaktionspartner:innen befinden sich in kollaborativer Aushandlung, in der a) die Deutung der Situation und b) die Deutung der jeweiligen persönlichen Darstellung je gemeinsam erarbeitet werden [13]. Fehler oder Missverständnisse, die in der Situation auftreten, können ad hoc ‚repariert' werden, wobei dies auch als gemeinsame Leistung zu verstehen ist, in der die Interaktionspartner:innen eben diese Möglichkeit zur Reparatur zuvorderst eröffnen und Normen der Zurückhaltung vorliegen, durch die nicht jede Inkonsistenz explizit zum Thema gemacht wird.

Die so stattfindende Interaktion hat damit immer auch einen situativ-prozessualen Aufbau und eine Geschichte. Gerade auch die Interaktion unter Unbekannten baut sich aus einer Situation wechselseitiger, bestätigender Wahrnehmung des Anderen als Individuum auf (die zumeist zu Nichtinteraktion führt [12, S. 83 ff.]). Beim Eintritt in eine Interaktion und im kollaborativen Aufbau der Situationsdeutung und des Interaktionsprozesses unter körperlicher Anwesenheit, kann sich bei Gelingen auch eine besonders emotiv beflügelte, positiv-produktive Wechselseitigkeit einstellen, in der sich die Körper und ihre Aussagen rhythmisiert verzahnen [7, S. 65 ff.]. Letztlich ist der Körper und vor allem das Gesichtsfeld Werkzeug, um die Authentizität und Wahrhaftigkeit der eigenen Darstellung zu versichern [37, S. 41 ff.].

All diese Aspekte gehen bei textueller Interaktion verloren. Diese Form der Interaktion kapriziert sich auf das einzig Vorliegende: die objektivierte Aussage. Die objektivierte Aussage a) bleibt zeitlich beständig (sie verfliegt nicht wie Aussagen oder körperliche Darstellungen in der kopräsenten Interaktionssituation) und muss b) nicht nur die Information, sondern auch ihre Metakriterien wie Authentizität und Wahrhaftigkeit verbürgen. Im Rückblick auf die immer-objektiviert-dastehende Form des Geschriebenen kann und muss sich die Kommunikation aufhängen.

Dies führt, so könnte man argumentieren, zu einer Überbeanspruchung der Informationsvermittlungskapazitäten von Sprache. Die Aussage muss verstanden werden, ohne Wissen über die Situation in der die Aussage durch die Sprecherin formuliert wurde. Verstehen funktioniert dann unter Bezugnahme auf die Aussageperson in einer als-ob Typik, in einer Form, die Schütz in Bezug auf den Briefverkehr „Pseudotypisierung" genannt hat (siehe dazu [20]), also anhand von Typisierungen, die nicht der Interaktionssituation selbst entstammen. Der notwendige Fokus der Interaktion auf die Inhaltsebene einer dekontextualisierten Aussage und das notwendige Verstehen ohne situativ angemessenes Wissen, führt zu einer Komplexitätssteigerung der Anschlussmöglichkeiten (da die Anschlussmöglichkeiten eben nicht interaktiv, situativ bedingt reduziert werden, also durch die Interaktions*situation* und ihre Deutung selbst schon in eine ‚Bahn' gelenkt sind), die wiederum, wie ich vermuten würde, zumindest bei der Kommunikation unter Unbekannten, zu einer Bevorzugung von Anschlüssen durch Zustimmung oder Ablehnung des Gesagten

in Bezug auf die eigene Meinung führt (anstatt, sagen wir, ein Entfalten alternativer Sichtweisen oder ein inhaltliches Argumentieren anhand zusätzlicher Argumente auszulösen). Dies kann durch fehlende situative Steuerungs- und Korrekturmechanismen leichter zu einer emotiv-konfliziösen Aufladung der Interaktionssituation führen [20, S. 127 ff.].

Wenn man auf Twitter schaut, bekommt man schnell den Eindruck, dass sich die Öffentlichkeit hauptsächlich in Konfliktform abspielt.[25] Vor dem Hintergrund der Kommunikationssituation unter Unbekannten im Internet, also ohne eine zuvorlaufende, gegenseitige, die Präsenz bestätigende Wahrnehmung, die auch eine Art ‚Grundrespekt' vor der Person vermittelt,[26] ist jeder Einstieg in eine Interaktion *online* eine *‚cold open'*. Zudem ist jeder Anschluss an eine Mitteilung durch die Form des Mediums (die meisten Medien zeigen eine deutliche Themenzentrierung, die von ihrer generellen thematischen Ausrichtung und den jeweiligen Erstmitteilungen gestellt wird) dazu angehalten, eine passende, inhaltliche Aussage zu treffen (und dies eben ohne weitere Kenntnis der Person oder der Situation, in der eine Aussage getätigt wurde).

Internetaussagen in Foren und Medien wie Twitter sind fundamental öffentliche Aussagen, oft Aussagen über Privates, aber Aussagen, die keinen bestimmten Rezipientenkreis mit einer bestimmten Haltung festlegen können. Vor dem Hintergrund einer differenzierten Gesellschaft mit ihrer Vielzahl an Haltungen, Wertungen und Normen, ist es nicht verwunderlich, dass dann gerade solche Mitteilungen anschließen, die die zugrundeliegenden Werte einer Aussage thematisieren (und es ist fast unmöglich Aussagen ohne zugrundeliegende Werte zu treffen). Als *‚cold open'*, dekontextualisierte Kommunikation und unter Fehlen körperlicher Möglichkeiten Gutgesinntheit, Wahrhaftigkeit und Authentizität zu vermitteln sowie ohne interaktive ‚Reparaturmechanismen' für Missverständnisse, ist es naheliegend, dass viele Mitteilungen einen konfliziösen Interaktionsverlauf nach sich ziehen.

---

[25] Und entgegen Nagels Vorstellung von *civility*: „My main point is a conservative one: that we should try to avoid fights over the public space which force into it more than it can contain without the destruction of civility" [29, S. 22 f.].

[26] „By according civil inattention, the individual implies that he has no reason to suspect the intentions of the others present and no reason to fear the others, be hostile to them, or wish to attack them. (At the same time, in extending this courtesy he automatically opens himself up to a like treatment from others present.) This demonstrates that he has nothing to fear or avoid in being seen and being seen seeing, and that he is not ashamed of himself or of the place and company in which he finds himself." [12, S. 84]

5.2 Internet als soziales Gedächtnis und technische Beobachtung

Wechseln wir auf die Makroperspektive. Eine der Haupteigenschaften des Internets ist, dass es nicht vergisst. Floridi schreibt: „In history, the problem was what to save (...)(.) In hyperhistory (also unter Bedingung einer dominanten informationstechnischen Durchdringung der Gesellschaft; Anm. RL) saving is the default option“ [10].[27] Jede Selbstdarstellung durch Internetmedien entgleist unserer Kontrolle. Und dies nicht zuvorderst durch die Intransparenz der verwendeten Software (vgl. dazu [15, S. 69 ff.]), sondern allein schon aufgrund der (transparenten) Funktionsweise der Medien in ihrer sozialen Nutzung: Wenn ich eine Chatnachricht über WhatsApp sende, bleibt diese Nachricht in objektivierter Form bei den Empfänger:innen. Sie kann zwar persönlich vergessen werden, bleibt aber technisch erinnert und ich habe keine Kontrolle darüber, mit wem und wann die Nachricht geteilt wird. Natürlich kann sich auch Wissen über Personen durch Hörensagen verbreiten, hierbei kann es jedoch immer zu Fehlerinnern oder Missverständnissen kommen. Die geteilte digitale Nachricht versichert ihre eigene Authentizität durch ihre Existenz. Wenn ich ein Video auf YouTube hochlade, habe ich zwar die Möglichkeit dies zu löschen, aber ich habe keine Ahnung, wer das Video inzwischen heruntergeladen hat und wo es eventuell zur Verfügung gestellt wurde. Wenn ich einen Beitrag in einem Internetforum verfasse, verbürgt mein Profil im Regelfall durch die Architektur des Forums meine Mitteilungsgeschichte (zumindest solange der Account existiert) und mein Profil auf einem Seitensprungportal kann ich nur geheim halten, bis die Accountdatenbank gehackt und ins Internet gestellt wird.[28]

In F2F-Interaktionen verpufft das Gesagte sobald es gesprochen ist. Die Tatsache der Speicherung eigener Selbstdarstellungen bei gleichzeitigem (natürlich auch technischen, aber vor allem auch sozialen) Kontrollverlust steigert somit ungemein das Risiko von Selbstdarstellungen. Die Zukunft ist charakterisiert durch ihre Offenheit. Haltungen, Werte, Wahrnehmungsschemata, Normen und Selbstverständnisse können sich ändern – die eigene Mitteilung hat Konstanz. Aussagen, die in einem bestimmten normativen Klima getätigt wurden, finden sich eventuell 10 Jahre später unter heftiger Kritik. Doch auch weniger radikal: Die eigene Mitteilung wird

[27] Er bindet dies zurück an eine Datenproduktion, die die Speicherkapazitäten immer weiter übersteigt und so kuriert werden muss, was im Gedächtnis bleibt. Dies ist allerdings ein Problem, dass auf einer anderen Ebene angesiedelt ist, als das hier Besprochene und muss uns deshalb nicht weiter interessieren.

[28] Eine Besprechung des prominenten Falls AshleyMadison.com findet sich ebenfalls in [15, S. 143 ff.].

entbettet und somit zum Artefakt. Ein Artefakt, das in unbestimmten zukünftigen Kommunikationen als selbstverbürgt-echte Aussage eingebracht werden kann.[29]

Gesteigert wird diese Problematik durch die Omnipräsenz von Tracking und die Aggregation von Daten. Generell wird dies als Problem der Privatheit verhandelt, entweder als Kontrollverlust über die eigenen Informationen[30] oder im Hinblick auf unbewusste Beeinflussung.[31] Fakt ist, dass Firmen wie Facebook, Amazon und Google wesentlich unser digitales Handlungsfeld, in dem wir uns eben auch als Selbste verwirklichen, mitbestimmen. Facebook entscheidet algorithmisch, welche Posts mir angezeigt werden, um die Chance meiner Teilnahme zu maximieren, Amazon empfiehlt Produkte basierend auf (zumindest) meiner Interaktionsgeschichte und meinem Wohnort und Google zeigt Suchergebnisse und schaltet Werbung eben auch in Bezug auf die automatische Verarbeitung meines persönlichen Verhaltens. In dieser Sichtweise entgleist mir die Kontrolle über die Folgen meines Handelns insofern, dass nicht nur die Folgen unbestimmt sind, sondern auch Intransparenz darüber besteht, was, wie und in welcher Konsequenz überhaupt getrackt wird.[32] Es wird automatisch beobachtet, verarbeitet und aggregiert, durch die Verarbeitung und Nutzung werden digitale Repräsentation meines Verhaltens in ein neues Regime überführt, vielleicht kann man sagen, zu digitalen Artefakten.[33] Die Konsequenz daraus ist im allermindesten eine fundamentale Intransparenz.

6 Privatheit und Anonymität im Internet

Wo stehen wir damit? Wenn Privatheit auf bestimmte Formen der Versicherung von Nichtwahrnehmung, Nichtbeobachtbarkeit und Nichtkommunikation angewiesen ist, stellt die Kommunikation im Internet das Phänomen Privatheit unter völlig neue Bedingungen. In gewisser Weise ist Nichtwahrnehmung aufgrund des Fehlens der

[29] Zur Wichtigkeit des Vergessens in der Pflege sozialer Identität siehe Klemms Aufsatz „Digitalization and Social Identity Formation“ [19], dessen Perspektive die hier vorliegende Argumentation wesentlich beeinflusst hat.

[30] Oft in einer Form normativen Aufschreis. So der bekannte Sicherheitsblogger und -experte Schneier in seinem Buch „David and Goliath“: „Our privacy is under assault from constant surveillance.“ [44]

[31] Eine allgemeine Diskussion zu „online Manipulation“ findet sich in [49], zu Trackingpraxen siehe ausführlich [6], zu einer Diskussion von „digital market manipulation“ spezifisch siehe [5].

[32] Zur Interansparenz durch Informationstechnik schließen Susser et al.: „A world increasingly structured by information technology is a world increasingly removed from view.“ [49, S. 34]

[33] Unterschiedliche Studien wie algorithmische Praxen Kultur prägen finden sich in [46].

Körper (außer in bewusst gewählten visuellen Darstellungsformen) stets versichert. Dies aber natürlich in Interaktionspraxen, die mit der wertbezogenen Idee lokaler Privatheit bei Rössler nicht übereinstimmen, während die typischen Regulationsformen, die *offline* ein Management von Nichtbeobachtbarkeit und Nichtkommunikation garantieren, im weitesten Sinne ausgesetzt sind.[34] Dezisionale Privatheit gerät bei öffentlichen Aussagen ohne eingeschränkten Adressatenkreis prinzipiell unter Druck. Die Form der Diskussion erfolgt durch die Logik des Mediums (öffentlich, asynchron, schriftlich, objektiviert, themenzentriert) und durch die Typik der Interaktionssituation (persönlich, körperlos, ahistorisch) oft als inhaltlicher oder wertbezogener Schlagabtausch, der eher kommunikativ entgleitet, als dass er im Rahmen der Interaktionsentwicklung eingefangen werden kann. Die Selbstdarstellung auf Microbloggingdiensten oder auf YouTube kann sich somit nicht auf Normen der Zurückhaltung verlassen, sondern evoziert stetig Rechtfertigungssituationen.

Ähnliches können wir über informationelle Privatheit sagen: Sie braucht die Möglichkeit eines Managements von in sozialen Kontexten bestehenden Erwartungen. Die generelle Beobachtbarkeit von Mitteilungen verunmöglicht oder erschwert ihre kontextspezifische Zuspitzung (man denke an das persönliche Netzwerk in Facebook und wie die Ausweitung des Netzwerks die eigenen Darstellungsmöglichkeiten begrenzt – wenn flüchtig Bekannte, Freunde und die eigene Familie im persönlichen Netzwerk sind, müssen wohl oder übel qua Mitteilung angebotene Informationen in ihrem Sinngehalt verallgemeinert werden, um Konflikte und unangenehme Nachfragen zu vermeiden). Die Speicherung der Mitteilung und der damit einhergehende Kontrollverlust über das Gesagte, führt so zu erwartbaren Konflikten durch das Entgleisen der Sozialdimension der inhaltlichen Aussage (von wem die Nachricht als zu verstehen intendiert war). Anders gesagt: Das Internet ist ein Alptraum für ein im Sinne informationeller Privatheit relevantes Erwartungsmanagement.

Die technische Beobachtung, algorithmische Verarbeitung und Aggregation von Nutzerdaten stellt ein weiteres Problem. Einerseits historisiert sie Nutzerverhalten auf eine bestimmte Weise, andererseits entsteht völlige Intransparenz über die

[34] Wie Thiel argumentiert: Vor dem Strukturwandel der Öffentlichkeit durch das Internet, bestand *„de-facto-Anonymität“* [50, S. 137 f.].

Folgen dieser technischen Beobachtung, die sich sowohl in unbewusster Beeinflussung[35] als auch in Kontrollverlust über das Gesagte zeigen können.[36]

Damit wird die Autonomie des Subjekts wesentlich eingeschränkt. Öffentliche Kommunikation im Internet ist prinzipiell riskant, sie multipliziert Rechtfertigungssituationen und ist situativ nicht spezifiziert. Wenn Kommunikation wesentlich über das Internet stattfindet und die Architektur des Internets und der über es realisierten Kommunikationsmedien diese Kommunikation unter Bedingungen setzt, in der klassische Regulationsmechanismen für Privatheit nur eingeschränkt funktionieren, brauchen wir eine Alternative. Die technische Umsetzung von Anonymität bietet eine Möglichkeit auf das Kollabieren von Informationskontexten und folgende Probleme im Erwartungsmanagement zu reagieren: technisch realisiert ist die Kommunikation im Internet stets pseudonym (über die IP-Adresse realisiert) und sozial ermöglicht wird pseudonyme Kommunikation ebenfalls (durch die Struktur verfügbarer Kommunikationsmedien und ihre zugehörigen Nutzungsnormen). Pseudonymität kann als Anonymisierungsstrategie verstanden werden und, mächtige, deanonymisierungsfähige Akteure nicht vorausgesetzt, eine alltägliche Differenzierung von Handlungskontexten versichern und damit kompensatorisch (also fehlende ‚Schutz*normen*' kompensierend) informationelle Privatheit erhalten. Insofern die Verschleierung auf technischer Ebene realisiert ist, könnten auch bestimmte Formen des Trackings verunmöglicht werden. Allerdings schränkt technische Anonymisierung maßgeblich die Ausdrucksmöglichkeiten ein: auch wenn Handlungskontexte different gehalten werden, erfordert Anonymisierung doch Anpassung der eigenen Darstellung. Wenn ich unter einem Pseudonym kommuniziere, aber zuviele biographische oder persönliche Informationen teile, hätte ich auch meinen Klarnamen angeben können. Die notwendige Alternative wird damit bevorzugt nicht nur über eine Technik realisiert, sondern zeigt sich idealerweise auch im Entstehen neuer Normen.[37]

---

[35] Susser et al. verhandeln dies als „online manipulation", die die Autonomie der Person angreift, indem sie intentional, gezielt, versteckt und Schwächen ausnutzend in ihrer Entscheidungsfindung beeinflusst wird [49, S. 12 ff.]. Als eindeutige Beispielfälle diskutieren sie das gezielte Bewerben vulnerabler Teenager und die politische Beeinflussung durch Cambridge Analytica [49, S. 27 f.].

[36] Bekannt geworden ist ein Fall, in dem eine schwangere Kundin der amerikanischen Supermarktkette „Target" Werbung über schwangerschaftsbezogene Artikel an ihre Hausadresse erhalten hat, bevor sie die Schwangerschaft in der Familie verkündigte. Eine Darstellung dieses und weiterer Fälle findet sich bei Christl und Spiekermann [6].

[37] Mit einer ähnlichen Festellung schließen Klemm und Staples [20] in ihrem letzten Satz und Hagendorff formuliert im Rahmen des 10. Kapitels in „Das Ende der Informationskontrolle": „An dieser Stelle wird deutlich, dass der Entwurf einer Pragmatik der resilienten Mediennutzung unter den Bedingungen ständiger informationeller Kontrollverlustereignisse stets an

7 Darknet

Nun können wir uns letztlich der Besprechung von Darknets widmen, spezifisch des Tor-Netzwerks. Darknets realisieren Kommunikation im und unter den Bedingungen des Internets, allerdings sind sie radikal dezentral organisiert und Verunmöglichen die digitale Rückverfolgbarkeit von Teilnehmer:innen durch die Verschleierung der IP-Adresse. Durch ihren Aufbau und ihre Organisation erlauben sie Zensur zu umgehen (durch das Ermöglichen anonymer Dienste und das Aufrufen von Diensten durch Nutzer:innen unter anderen IP-Adressen als der eigenen).[38] Der wesentliche Unterschied in der technischen Realisierung des Tor-Netzwerks zum Internet liegt in der Verschleierung der IP-Adresse von Sender:innen und Empfänger:innen,[39] welche bei jeder Datenübertragung über das Internet im *Header* jedes Datenpackets im Klartext mitversandt werden. Die IP-Adresse identifiziert Internetanschlüsse eindeutig.

Allerdings können die zugehörigen Haushalte nur unter bestimmten Bedingungen genau identifiziert werden. Staatliche Akteure oder Rechteinhaber können sich bei berechtigten Anfragen an die Betreiber von Internetanschlüssen wenden und über die IP-Adresse und den Zeitpunkt der Datenübertragung rückverfolgen lassen, welcher Internetanschluss unter welcher Hausadresse beteiligt war. Jeder kann bei Kenntnis der IP-Adresse die ungefähre Geolokation des zugehörigen Haushalts identifizieren.[40] Der Staat kann über Internetbetreiber den Zugang zu bestimmten Diensten verunmöglichen (staatliche Zensur), sowie einzelne Dienstbetreiber den Zugang einzelner Nutzer:innen zu ihren Diensten verbieten können (bspw. einzelne

zwei Polen ansetzen muss, nämlich auf der einen Seite an der individuellen Mediennutzung, welche dergestalt ist, dass sie den Kollaps der Trennung verschiedener Informationskontexte permanent erwartet, sowie auf der anderen Seite an den Empörungs- und Toleranzniveaus der Öffentlichkeit sowie den Sanktionsmechanismen sozialer Institutionen, welche wiederum mehr oder minder angemessene Reaktionsweisen auf geschehene Kontrollverlustereignisse darstellen sollten“ [15, S. 174] und schlägt unter anderem zur Emanzipation der ‚Überwachten‘ exhibitionistische Selbstdarstellung als eine subversive Strategie der Machtübernahme vor.

[38] Für eine kurze Begriffsgeschichte, Begriffsdifferenzierung und längere Definition von Darknets siehe das Whitepaper aus unserem Forschungsprojekt PANDA [39].

[39] Eine genauere Besprechung der Funktionsweise von Tor ist im Rahmen des Papers weder möglich noch nötig. Eine gut verständliche Beschreibung findet sich in folgendem detaillierten Blog-Post: https://hackernoon.com/how-does-tor-really-work-5909b9bd232c (gesehen 31.10.2020), eine technische Beschreibung findet sich u. a. in den *design papers* zu Tor, siehe [8].

[40] Ein Selbsttest der Genauigkeit der örtlichen Identifikation ist einfach unter bspw. https://www.iplocation.net/ (gesehen 31.10.2020) möglich.

User:innen werden aus Chaträumen ausgeschlossen), oder angebotene Inhalte können nach IP-Regionen differenziert werden (Angebote auf Amazon, oder Filme auf Netflix). Genauso können unter Kenntnis der IP-Adresse *denial-of-service* Angriffe ausgeführt werden.[41] Schließlich ist die IP-Adresse Teil des Trackings in Softwareumgebungen zum Tracking und der Analyse von Nutzerdaten – vermutlich ist sie allerdings ‚nur' für die marktwirtschaftliche Differenzierung von Nutzer:innen in Regionen relevant.[42] Sofern für mich zu diesen Zeitpunkt abzusehen ist, sind dies die wesentlichen Handlungsmöglichkeiten in Bezug auf eine IP-Adresse.

Damit verunmöglicht das Tor-Netzwerk wesentlich staatliche Beobachtungsformen. Im Sinne und im Gegensinne von liberal-demokratischen Staaten wird Zensur und die rechtliche Verfolgbarkeit von Handlungen, wenn nicht verunmöglicht so doch wesentlich erschwert. Und es ist so auch nicht verwunderlich, dass sich im öffentlich zugänglichen Teil von Tor[43] hauptsächlich Schwarzmärkte und andere potentiell moralisch oder rechtlich problematische Inhalte finden lassen (siehe die quantitativen Studien aus der Einleitung für empirische Ergebnisse diesbezüglich).

Doch neben solchen Inhalten finden sich auch Kommunikationsräume wie Foren und soziale Netzwerke im Darknet. Und im Kontrast zu den medieneffektiven Ergebnissen, die in Bezug auf das Tor-Netzwerk berichtet werden, wirkt die Kommunikation dort, vor allem im Vergleich mit anonymen Kommunikationsmedien im Clearnet, eher harmlos.[44] Weiterhin besteht in diesen Kommunikationsräumen in Bezug auf ihre Wahrnehmung als anonym, eine bestimmte Haltung zur Einhaltung von Anonymitätsregeln und zum Umgang mit Anonymität.[45] Es ist vielleicht eine sol-

[41] Siehe die Zusammenfassung auf https://en.wikipedia.org/wiki/Denial-of-service_attack (gesehen 31.10.2020).

[42] Allerdings erlaubt die IP-Adresse in Kombination mit anderen Merkmalen durchaus eine eindeutige Identifikation von Personen. Christl und Spierkermann schreiben: „A study from 1990 discovered that the combination of zip code, gender and birth date was unique for 216 of 248 Mio. U.S. citizens (87%) and therefore makes identification possible." [6, S. 22]

[43] Tor hat keine mächtige Suchmaschine wie Google und Dienste müssen über Weitergabe von Wissen oder Linklisten gefunden werden. Aber auch im Internet gilt: nicht alle Dienste sind öffentlich gelistet und werden von Suchmaschinen gefunden.

[44] Hier fordere ich zu einem weiteren schnell realisierbaren Selbsttest auf: Auf der Oberfläche wirken die Mitteilungen im bekannten Darknetforum Hidden Answers (http://answerszuvs3gg2l64e6hmnryudl5zgrmwm3vh65hzszdghbldvfiqd.onion/) oft mundäner als die bigoten Aussagen die sich auf 4Chans Unterforum /pol/ finden lassen (https://boards.4chan.org/pol/) (beide gesehen 31.10.2020). Zum Zusammenhang des Imageboards 4Chan und *alt-right* Ideologie, siehe bspw. Nagles „Kill all Normies" und Tuters und Sals Ausführungen zu (((They))) [30, 51].

[45] Diese Aussage basiert auf eigenen empirischen Untersuchungen, die bisher unveröffentlicht sind, findet sich aber auch in Gehls Studie zum Netzwerk Galaxy 2 [11, S. 243 f.].

che Norm der Anonymität, die Privatheit schützen und aus der die soziale Antwort auf die neue Kommunikationssituation im Internet erwachsen kann.

8 Schlussbemerkung

Zum Schluss möchte ich einige vorläufige Anmerkungen zu einer Kultur der Anonymität machen, wie sie Auerbach beschrieben hat [1, 2]. Wie wir gesehen haben, erlaubt Anonymität Handlungsoffenheit. Damit einher geht die Möglichkeit unverantwortlich zu kommunizieren und ein Entgleisen des öffentlichen Diskurses wie es Nagel in „Concealment and Exposure“ [29] als problematisch ermahnt. Andererseits erlaubt sie aber auch kreativen Ausdruck in symmetrischen Kommunikationsbeziehungen. Es ist nicht erstaunlich, dass in einem Medium wie 4Chan, in dem Nutzer per Default anonym sind und Inhalte nur eine kurze Zeit erhalten bleiben, sich eine Gesprächskultur entwickeln konnte, die juvenil und aggressiv, aber auch chaotisch-kreativ ist. Und es ist nicht erstaunlich, dass sich im Rahmen des Mediums als asynchrone, fortlaufende Kommunikation ohne wiederidentifizierbare Sprecher, Mitteilungen etabliert haben die a) ambig[46] und b) gleichzeitig grenzüberschreitend und semiotisch offen sind.

Mehrdeutig sind sie, da jede darauffolgende Mitteilung ein uneingeschränktes Recht hat, die zuvorlaufenden Mitteilungen in ihrem je eigenen Sinne zu verstehen. Grenzüberschreitend sind sie, um informationswert zu erhalten.[47] Es muss in die Mitteilung ein Grund eingebaut werden, damit auf die Mitteilung reagiert wird. Die Permanenz der Grenzüberschreitung und ihre situative Entbettetheit aus Kontexten, die die eigentliche Bedeutung solcher Grenzüberschreitungen zuvorderst verbürgen könnten, die stetige Wiederholung archetypischer Kommunikationen eingebettet in neue Kommunikationssituationen (Memes, siehe [32]) und die zugrundeliegende für das Internet untypische Ephemeralität, führt notwendigerweise zu einer Verallgemeinerung der Bedeutung interaktiv geschaffener Ausdrucksformen (siehe vgl. [51, S. 2230]).

Doch im Rahmen dieser unzivilen Kommunikation, wird auch ein ungeheures sprachlich-spielerisches und generell kreatives Potential freigesetzt.[48] In gewisser

[46] Siehe dazu [2, 21]; man fühlt sich aber auch an Besprechungen postmoderner Ironie erinnert, die neben Mehrdeutigkeit auch eine bestimmte Art von Literarizität verbürgt, siehe [47].

[47] Im Sinne von Information als Irritation; siehe dazu bspw. [24, S. 68].

[48] Spezifisch 4Chan/pol/ wurde vor allem in den letzten Jahren und zu Recht eindeutig mit der *alt-right* Bewegung in Verbindung gebracht (siehe die bisherigen Referenzen zu 4Chan). Ich möchte hier nicht unterschlagen, dass Memes wie sie in /pol/ entstehen als ironischer Deckmantel unironischer rechter Ideologie dienen (können), vor allem da sie bei einer Ver-

Hinsicht könnte sie sogar als ziviler als die Kommunikation auf Twitter verstanden werden, denn das Prozessieren der radikalisierten, sprachlichen Formen auf 4Chan, die sich an „Memes“ als Interaktionsprodukten abarbeitet, lässt eindeutig ‚persönliches‘ weitestgehend außen vor. Ich denke, dass man in dieser Kommunikation somit auch durch Anonymität verbürgte Freiheit als gesellschaftlichen Wert wiedererkennen kann. In Bezug auf die Videoüberwachung in England schreibt Rössler:

> „(...) (D)ie Gefahr solcher und anderer Überwachungs- und Kontrollmechanismen liegt dann nämlich auch darin, dass Personen, gerade aufgrund einer strukturellen staatlichen oder gesellschaftlichen Geringschätzung des Schutzes informationeller Privatheit, ihre eigene Autonomie und Privatheit als nicht mehr so relevant begreifen“ [41, S. 39].

Dies ist problematisch vor dem Hintergrund, dass eine liberale Demokratie eben diese Autonomie erfordert. Vielleicht findet sich in Darknets als dezidiert technisch anonymen Netzwerken eine Möglichkeit eine Kultur von Anonymität zu normalisieren, indem sie für eine breitere Nutzung popularisiert wird, anstatt sie ‚abzuschalten‘.[49]

Literatur

1. Auerbach, D.: Anonymity as culture; case studies. Triple Canopy **15** (2012). https://www.canopycanopycanopy.com/contents/anonymity_as_culture_treatise
2. Auerbach, D.: Anonymity as culture; treatise. Triple Canopy **15** (2012). https://www.canopycanopycanopy.com/issues/15/contents/anonymity_as_culture_case_studies

breitung in weitere Medienkontexte neue Bedeutungen aufnehmen, während sie dennoch auch ihre ursprüngliche Bedeutung erhalten. Die offene sozialtheoretische Frage ist, inwiefern die Kommunikatoren auf /pol/ als *soziale Gruppe* rechter Ideologen reifiziert werden können. Mein Ziel hier ist andeutungsweise auf den Wert hinzuweisen, den man bei Erhalt alles Gesagten in der Form der Kommunikation selbst und im weiteren Kontext von 4Chan sehen könnte.

[49] Der Leserin mag vielleicht aufgefallen sein, dass wir eine im Eingangskapitel gemachte Differenz nicht mehr thematisiert haben: Ob vielleicht eine Option darin bestünde nur das Anbieten anonymer Dienste im Darknet zu untersagen. Soweit für mich ersichtlich, sind anonyme Dienste nur für die Zensur, also das mögliche Aussetzen dieser Dienste relevant. Für die Nutzer:innen ergibt sich kein Unterschied für ihre technische Anonymität. Der Grund warum ich dazu nicht explizit Stellung beziehe, liegt eben darin, dass ich denke, dass eine zu vorschnelle Verdammung von Anonymisierungstechniken gesellschaftlich problematisch in Bezug auf die hier verhandelten Werte sein kann. Eine inhaltliche Auseinandersetzung mit und Bewertung dieser Regulationsmöglichkeit steht deswegen noch aus.

3. Barlow, J.P.: A declaration of the independence of cyberspace. https://www.eff.org/cyberspace-independence
4. Biryukov, A., Pustogarov, I., Thill, F., Weinmann, R.P.: Content and popularity analysis of tor hidden services. arxiv (2013)
5. Calo, R.: Digital market manipulation. Geo. Wash. L. Rev. **82**, 995 (2014)
6. Christl, W., Spiekermann, S.: Networks of control; a report on corporate surveillance, digital tracking, big data & privacy. Facultas, Wien (2016)
7. Collins, R.: Interaction ritual chains. Princeton University Press, Princeton (2014)
8. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The Second-Generation Onion Router. Tech. Rep, Naval Research Lab, Washington DC (2004)
9. Faizan, M., Khan, R.A.: Exploring and analyzing the dark web: a new alchemy. First Monday (2019). https://doi.org/10.5210/fm.v24i5.9473
10. Floridi, L.: The Fourth Revolution. How the Infosphere is Reshaping Human Reality. OUP, Oxford (2014)
11. Gehl, R.W.: Weaving the Dark Web. MIT Press Ltd, Cambridge/London (2018)
12. Goffman, E.: Behavior in Public Places; Notes on the Social Organization of Gatherings. Simon and Schuster, New York (2008)
13. Goffman, E., et al.: The Presentation of Self in Everyday Life. Harmondsworth, London (1978)
14. Guitton, C.: A review of the available content on tor hidden services: t the case against further development. Comput. Hum. Behav. **29**(6), 2805–2815 (2013). https://doi.org/10.1016/j.chb.2013.07.031
15. Hagendorff, T.: Das Ende der Informationskontrolle; Zur Nutzung digitaler Medien jenseits von Privatheit und Datenschutz, Bd. 15. transcript, Bielefeld (2017)
16. Joas, H.: Die Kreativität des Handelns. Suhrkamp, Frankfurt am Main (1992)
17. Kaufmann, J.C.: Die Erfindung des Ich: Eine Theorie der Identität. UVK-Verlag-Ges, Konstanz (2005)
18. Kersten, J.: Anonymität in der liberalen demokratie. Jurist. Schulung JuS **3**, 193–203 (2017)
19. Klemm, M.: Digitalization and social identity formation. In: Casanova, P., Sartor, G. (Hrsg.) Remembering and Forgetting in the Digital Age, S. 69–187. Law, Governance and Technology Series. Springer, New York (2018)
20. Klemm, M., Staples, R.: Warten auf antwort. In: Hahn, K., Stempfhuber, M. (eds.) Präsenzen 2.0: Körperinszenierung und Medienkulturen, pp. 113–134. Springer, Wiesbaden (2015)
21. Ludemann, D.: /pol/emics: ambiguity, scales, and digital discourse on 4chan. Discourse Context & Media **24**, 92–98 (2018)
22. Luhmann, N.: Die form „person". In: Luhmann, N. (Hrsg.) Soziologische Aufklärung 6; Die Soziologie und der Mensch, S. 142–154. Westdeutscher GmbH, Opladen (1987)
23. Luhmann, N.: Die gesellschaftliche differenzierung und das individuum. In: Luhmann, N. (Hrsg.) Soziologische Aufklärung 6; Die Soziologie und der Mensch, S. 125–141. Westdeutscher GmbH, Opladen (1987)
24. Luhmann, N.: Soziale Systeme. Suhrkamp, Frankfurt am Main (1987)
25. Luhmann, N.: Die Kontrolle von Intransparenz. Suhrkamp, Berlin (2017)

26. Marx, G.: Identity and anonymity: some conceptual distinctions and issues for research. In: Caplan, J., Torpey, J. (Hrsg.) Documenting Individual Identity. Princeton University Press, Princeton (2001)
27. Matthews, S.: Anonymity and the social self. Am. Philos. Q. **47**(4), 351–363 (2010)
28. Moore, D., Rid, T.: Cryptopolitik and the darknet. Survival **58**(1), 7–38 (2016). https://doi.org/10.1080/00396338.2016.1142085
29. Nagel, T.: Concealment and exposure. Philos. Public Aff. **27**(1), 3–30 (1998)
30. Nagle, A.: Kill All Normies: Online Culture Wars from 4chan and Tumblr to Trump and the Alt-right. John Hunt Publishing, Winchester/Washington (2017)
31. Nassehi, A.: Mit dem Taxi durch die Gesellschaft: Soziologische Storys. Murmann Publishers GmbH, Hamburg (2010)
32. Nissenbaum, A., Shifman, L.: Internet memes as contested cultural capital: the case of 4chan's/b/board. New Media Soc. **19**(4), 483–501 (2017)
33. Nissenbaum, H.: The meaning of anonymity in an information age. Inf. Soc. **15**(2), 141–144 (1999)
34. Owen, G., Savage, N.: The tor dark net. Ser. Glob. Comm. Internet Gov. Pap. Ser. **20** (2015)
35. Owen, G., Savage, N.: Empirical analysis of tor hidden services. IET Inf. Secur. **10**(3), 113–118 (2016). https://doi.org/10.1049/iet-ifs.2015.0121
36. Pabst, S.: Unbeobachtete Kommunikation. Springer, Wiesbaden (2018)
37. Pabst, S.: Die entdifferenzierung des privaten. privatheit und öffentlichkeit unter den bedingungen einer medial und funktional differenzierten gesellschaft. ṠPIEL **4**(1), 35–59 (2019)
38. Papsdorf, C.: Kritik im hidden web. technisch anonymisierte kommunikation als basis emanzipativer praktiken. In: Kybernetik. Kapitalismus, Revolutionen, S. 211–235. Paul Buckermann, Anne Kopppenburger, Simon Schaupp. UNRAST-Verlag Münster (2017)
39. Platzer, F., Landwirth, R., Wittmer, S., Yannikos, Y.: Was ist das darknet? Tech. rep, FraunhoferSIT and TU-Darmstadt (2020)
40. Rìos, S.A., Muñoz, R.: Dark web portal overlapping community detection based on topic models. In: Proceedings of the ACM SIGKDD Workshop on Intelligence and Security Informatics - ISI-KDD 12. ACM Press (2012). lDOIurl10.1145/2331791.2331793
41. Rössler, B.: Anonymität und privatheit. In: Anonymität im Internet, S. 27–40. Springer, Wiesbaden (2003)
42. Rost, M.: Zur gesellschaftlichen funktion von anonymität. anonymität im soziologischen kontext. Datenschutz und Datensicherheit **27**(3), 155–158 (2003)
43. Rössler, B.: Der Wert des Privaten. Suhrkamp, Frankfurt am Main (2001)
44. Schneier, B.: Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. WW Norton & Company, New York/London (2015)
45. Serres, M.: Erfindet euch neu!: eine Liebeserklärung an die vernetzte Generation. Suhrkamp, Berlin (2013)
46. Seyfert, R., Roberge, J.: Algorithmic Cultures: Essays on Meaning,Performance and New Technologies. Taylor & Francis, London/New York (2016)
47. Shugart, H.A.: Postmodern irony as subversive rhetorical strategy. West. J. Commun. (Commun. Rep.) **63**(4), 433–455 (1999)
48. Spitters, M., Verbruggen, S., van Staalduinen, M.: Towards a comprehensive insight into the thematic organization of the tor hidden services. In: 2014 IEEE Joint Intelligence and

Security Informatics Conference. IEEE, 220–223 (2014). https://doi.org/10.1109/jisic.2014.40
49. Susser, D., Roessler, B., Nissenbaum, H.F.: Online manipulation: hidden influences in a digital world. SSRN Electron. J. (2018). https://doi.org/10.2139/ssrn.3306006
50. Thiel, T.: Anonymität und demokratie. Forschungsjournal Soz. Beweg. **30**(2), 152–161 (2017)
51. Tuters, M., Hagen, S.: (((they))) rule: memetic antagonism and nebulous othering on 4chan. New Media Soc. **22**(12), 2218–2237 (2020)
52. Tzanetakis, M.: The darknet's anonymity dilemma. Encore 2017. In: The Annual Magazine on Internet and Society Research, S. 118–125 (2018)
53. Tzanetakis, M., von Laufenberg, R.: Harm reduction durch anonyme drogenmärkte und diskussionsforen im internet? In: akzept e. V. Bundesverband, I. (Hrsg.) Alternativer Drogen- und Suchtbericht 2016, S. 189–194. Pabst Science Publishers, akzept e. V., Deutsche AIDS-Hilfe, JES e. V., Lengerich (2016)
54. Wallace, K.A.: Anonymity. Eth. Inf. Technol. **1**(1), 21–31 (1999)

Online-Privatheitskompetenz und Möglichkeiten der technischen Umsetzung mit dem Anonymisierungsnetzwerk Tor

Alexandra Lux und Florian Platzer

Zusammenfassung

Ziel der vorliegenden Arbeit ist die Erstellung einer Anonymitätsmatrix. Der Fokus liegt hierbei insbesondere in der Verbindung der technischen und psychologischen Komponenten der Betrachtung. Ausgangssituation ist die Verwendung einer Privacy Enhancing Technology, konkret dem Tor-Browser. So ist das Ziel, die Tor-Nutzergruppe in Bezug auf ihre Online-Privatheitskompetenz, Nutzungsweise und Grad der Anonymität zu erforschen. Hierzu wurde eine Online-Befragung ($N = 120$) sowie ein Leitfadeninterview mit einem Experten aus der IT-Sicherheitsforschung durchgeführt.

Schlüsselwörter

Anonymität • Privatheitskompetenz • Tor

1 Online-Privatheitskompetenz zur Erstellung und Wiederaufhebung anonymer Internetkommunikation

Im vorliegenden Abschnitt werden wir zunächst zentrale Begrifflichkeiten von Privatsphäre im Online-Kontext klären. Internetnutzer sind zwar oft um ihre Privat-

A. Lux (✉)
TU Darmstadt, Darmstadt, Deutschland
E-mail: alexandra.lux@sit.fraunhofer.de

F. Platzer
Fraunhofer SIT, Darmstadt, Deutschland
E-mail: florian.platzer@sit.fraunhofer.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_7

sphäre besorgt, besitzen jedoch nicht die entsprechenden Kompetenzen, um ihr Verhalten entsprechend anzupassen und so ihre Privatsphäre zu schützen.

Eine Möglichkeit, die Privatsphäre der Internetnutzer zu schützen, bietet das Anonymitäts-Netzwerk *Tor*[1]. Tor erlaubt eine anonyme Kommunikation über das Internet. Der dafür benötigte Tor-Browser kann zum Surfen sowohl des Clearnets als auch des Darknets, also für den Zugriff auf anonym bereitgestellte Internetdienste, sog. Hidden Services, verwendet werden.

Im Rahmen dieser Arbeit untersuchen wir einen Erklärungsansatz, welcher sich mit der Online-Privatheitskompetenz der Nutzer beschäftigt. Am Beispiel von Tor gehen wir auf *Privacy Enhancing Technologies* (PETs) ein, die eine Möglichkeit bieten, eigene Daten besser zu schützen und eine anonyme Internetkommunikation aufzubauen. Wir zeigen auf, welche Akteure einen Tor-Nutzer potenziell deanonymisieren können und welche zusätzlichen Technologien ein Tor-Nutzer hinzunehmen kann, um eine solche Deanonymisierung zu erschweren.

1.1 Privatsphäre im Online-Kontext

Das Verlangen nach Privatsphäre im Online-Kontext wird in Zeiten von Massenspeicherung und den Überwachungsmöglichkeiten des Internetverkehrs immer stärker. Bei der Definition von Privatsphäre wird in der Regel auf drei zentrale Arbeiten zurückgegriffen: Westin [31], Altman [2] sowie Burgoon [5]. Trepte und Dienlin führen die zentralen Aspekte dieser drei Ansätze wie folgt zu einer Definition zusammen:

> „Privatsphäre ist ein individueller Zustand der Abgeschiedenheit und Intimität (Westin 1967), der einer stetigen Regulierung von Zuviel und Zuwenig Privatsphäre unterliegt (Altman 1975), wobei sich zu jedem Zeitpunkt vier verschiedene Privatsphäredimensionen unterscheiden lassen: informationale, soziale, psychische und physische Privatsphäre“ (Burgoon, 1982) [5, S. 56].

Zwei entscheidende Faktoren sind in diesem Zusammenhang das *Privatsphäreverhalten* sowie der *Privatsphärekontext*. Dabei beschreibt das Privatsphäreverhalten eine Verhaltensweise, die die eigene Selbstauskunft anderen gegenüber einschränkt oder sich der Interaktion mit anderen entzieht [8]. Der Privatsphärekontext wiederum beschreibt die Situation, in der die Interaktion stattfindet. Dieser ist abhängig von der individuellen Wahrnehmung der Teilnehmer der Interaktion [28]. Immer wieder konstatieren Forschungsergebnisse eine Dissonanz zwischen Bedenken rund

[1] Tor Project, https://torproject.org, Zugegriffen am 15.10.2020

um Privatheit und dem Verhalten im Umgang mit den eigenen Daten [1, 20, 32]. Dieser Umstand wird auch als *Privacy Paradox* bezeichnet [3, 8]. Einer der angeführten Erklärungsansätze, wie es zu dieser Dissonanz kommen kann, ist die *Knowlegde Gap Hypothesis*. Sie beschreibt den Zustand, dass Personen zwar um ihre Privatsphäre besorgt sind, jedoch nicht die entsprechenden Kompetenzen besitzen, um ihr Verhalten entsprechend anzupassen und so ihre Privatsphäre zu schützen [6, 29].

Online-Privatheitskompetenz ist somit eine Möglichkeit das Online-Verhalten kohärenter zu den jeweiligen Privatsphärebedürfnissen der Nutzer zu gestalten [29]. Auf dieser Basis werden Nutzer in die Lage versetzt, Kontrolle über ihre digitale Identitäten zu erlangen [21]. Online-Privatheitskompetenz umfasst das Wissen um technische Möglichkeiten sowie diesbezügliche Regularien und institutionelle Praktiken zur Erreichung von Online-Privatheit als auch das Wissen um deren korrekte Anwendung [29]. Umfassende Forschungsergebnisse zeigen verschiedene Einflussfaktoren auf die Online-Privatheitskompetenz, wie demografische Variablen, digitale Kompetenz, das Bewusstsein für institutionelle Überwachungspraktiken und das Verständnis von vorgegebenen Richtlinien [21].

Entgegen bisherigen Arbeiten, in denen das Privacy Paradox vorrangig im Kontext der Nutzung sozialer Netzwerke betrachtet wurde [3, 8], beziehen wir uns auf die Nutzungsweise im Internet allgemein. Die Nutzungsweise von Tor kann in Bezug auf verschiedene Aspekte variieren. In Anlehnung an aktuelle Forschung [12] haben wir die Nutzung von Tor unter anderem durch die Erhebung der Nutzungshäufigkeit erfasst. Des Weiteren erfassten wir in diesem Rahmen die Themen, die bei der Nutzung vorrangig von Interesse sind [4, 19], sowie in welchem Privatsphärekontext, also Clearnet, Darknet oder dual, Tor verwendet wird. Außerdem erfragten wir noch die Art der Hidden Services, die besucht werden. Vor diesem Hintergrund möchten wir uns in einem ersten Schritt die Nutzungsweise von Tor und die Online-Privatheitskompetenz genauer anschauen. Erste Untersuchungen diesbezüglich zeigten, dass Tor-Nutzer eine höhere Online-Privatheitskompetenz besitzen, als reguläre Clearnet-Nutzer. So beantworteten diese im Schnitt 78,78 % der Fragen richtig [12]. So lautet unsere erste Forschungsfrage:

Forschungsfrage F1: Inwiefern variiert die Online-Privatheitskompetenz der Nutzer in Abhängigkeit ihrer Nutzungsweise von Tor?

Hypothese H1a: Abhängig von der Nutzungshäufigkeit von Tor variiert die Online-Privatheitskompetenz der Nutzer.

Hypothese H1b: Abhängig davon, ob Tor im Clearnet, Darknet oder beidem verwendet wird, variiert die Online-Privatheitskompetenz der Nutzer.

Hypothese H1c: Abhängig davon, für welche Themengebiete Tor vorrangig verwendet wird, variiert die Online-Privatheitskompetenz der Nutzer.

Hypothese H1d: Abhängig davon, welche Art von Hidden Services vorrangig genutzt wird, variiert die Online-Privatheitskompetenz der Nutzer.

Eine Möglichkeit, seine Daten besser zu schützen, ist der Einsatz von *Privacy Enhancing Technologies.* Doch auch hier bedarf es entsprechender Kompetenzen, wobei das Wissen um das Bestehen der Technologie nicht ausreicht. Vielmehr bedarf es zudem auch notwendiges Wissen um die Anwendung. Ergebnisse früherer Forschung belegen, dass Personen keine akkurate Introspektion betreffend ihres Wissens um Technologien zum Schutz der eigenen Privatsphäre haben [16]. Weitere Forschungen zeigen, dass das Wissen um technische Möglichkeiten nach demographischen Aspekten variiert [11]. Eine Umfrage ergab, dass 86 % der amerikanischen Teilnehmer Maßnahmen zur Erhöhung ihrer Anonymität ergriffen haben (bspw. Cookies löschen 64 %, Cookie-Blocker 41 %). Nur ein geringer Anteil der Befragten (14 %) gab an, Technologien wie bspw. VPN, Proxy-Server oder Tor zu verwenden. Außerdem indizierten die Ergebnisse, dass eine Nutzergruppe zwischen 18 und 29 Jahren sowie Personen mit höherem Bildungsabschluss tendenziell mehr Anonymisierungstechnologien verwendet. [22]. Wie zuvor bereits dargestellt, fokussiert die vorliegende Arbeit auf der Untersuchung der Tor-Nutzergruppe. Da allerdings auch mit der Verwendung von Tor eine Deanonymisierung nicht ausgeschlossen werden kann, bieten zusätzliche PETs potentiell einen höheren Schutz vor Deanonymisierung.
Vor diesem Hintergrund stellen wir die folgende Forschungsfrage:

Forschungsfrage F2: Inwiefern variieren die in Kombination zu Tor verwendeten Anonymisierungstechnologien in Abhängigkeit von der individuellen Nutzungsweise von Tor?

Hypothese H2a: Abhängig von der Häufigkeit der Nutzung von Tor variieren die zusätzlich in Kombination zu Tor verwendeten Anonymisierungstechnologien.

Hypothese H2b: Abhängig davon, ob Tor im Clearnet, Darknet oder beidem verwendet wird, variieren die in Kombination zu Tor verwendeten Anonymisierungstechnologien.

Hypothese H2c: Abhängig davon, für welche Themengebiete Tor vorrangig verwendet wird, variieren die in Kombination zu Tor verwendeten Anonymisierungstechnologien.

Hypothese H2d: Abhängig davon, welche Art von Hidden Services vorrangig genutzt wird, variieren die in Kombination zu Tor verwendeten Anonymisierungstechnologien.

Forschungsergebnisse [25] haben gezeigt, dass ein Großteil der Personen sich etwaiger weiterer Technologien, die zum Schutz ihrer Privatsphäre genutzt werden können, nicht bewusst ist. Betreffend der aktiven Verwendung von zusätzlichen Maßnahmen indizierten 13 % der Befragten keine Kenntnis von alternativen Suchmaschinen, welche keine Suchverläufe der Nutzer speichern (bspw. DuckDuckGo). 54 % der Befragten gaben an, Suchmaschinen dieser Art nicht zu verwenden. Ferner hatten 33 % keine Kenntnis über die Möglichkeit der Verwendung von Proxyservern zum Schutz der Privatsphäre. 41 % gaben wiederum an, Proxyserver nicht zu verwenden. 39 % der befragten Personen hatten keine Kenntnis von Anonymisierungsnetzwerken, wie beispielsweise Tor. Weitere 40 % gaben an, diese nicht zu verwenden [25]. Konform dazu fanden Weinberg et al. [30], dass der allgemeine Kenntnisstand über technische Möglichkeiten zur Verbesserung der Privatsphäre moderat ist. Die Anzahl der Personen, die entsprechende technische Möglichkeiten anwendet, ist gering.

Zudem bedarf es im Fall einer Anwendung auch die notwendige Kompetenz, da im Falle einer inkorrekten Anwendung sich der Privatsphäreschutz im Vergleich zum Verzicht auf die PET gar verschlechtern kann. Auf dieser Basis widersprechen wir der Argumentation früherer Arbeiten [12], wonach der Erklärungsansatz der Knowledge Gap Hypothesis alleinig auf Basis der Installation und Nutzung einer PET als Erklärungsansatz für das Privacy Paradox angesehen wird. Wie oben dargestellt, handelt es sich bei Online-Privatheitskompetenz um ein vielschichtiges Konstrukt, das nicht alleinig in dem Wissen um PETs besteht [29]. Um die Differenz zwischen Wissen um weitere technische Möglichkeiten in Form von PETs und der tatsächlichen Anwendung aktiv zu berücksichtigen, möchten wir den Effekt der zusätzlichen Verwendung von Anonymisierungstechnologien auf die Online-Privatheitskompetenz untersuchen und stellen hierfür die folgende Forschungsfrage:

Forschungsfrage F3: Inwiefern sagt die Online-Privatheitskompetenz der Nutzer die in Kombination mit Tor verwendete Anonymisierungstechnologien voraus?

Hypothese H3a: Nutzer, die eine höhere Online-Privatheitskompetenz besitzen, verwenden zusätzliche Anonymisierungstechnologien in Kombination zu Tor.

Hypothese H3b: Nutzer, die eine höhere Online-Privatheitskompetenz besitzen, haben Kenntnis von zusätzlichen Anonymisierungstechnologien in Kombination zu Tor.

Durch die Verwendung von Tor erhält man eine grundsätzliche Anonymität beim Surfen des Clear- und des Darknets. Trotzdem sind die Tor-Nutzer einer möglichen Deanonymisierung leicht ausgesetzt.

Nach Westin [31] wird unter Anonymität der Zustand verstanden, in welchem Freiheit von Identifikation und Überwachung an öffentlichen Orten oder während öffentlicher Handlungen besteht. Hayne und Rice [14] unterscheiden weiter zwischen sozialer und technischer Anonymität. *Soziale Anonymität* impliziert hierbei, dass keine Kontextinformationen zur Verfügung stehen, um die Identität zu enthüllen. Hier sind insbesondere Informationen gemeint, die durch Kommunikation und Verhalten mit anderen geteilt werden. *Technische Anonymität* hingegen impliziert, dass eine Rückverfolgbarkeit auf technischer Basis nicht möglich ist. Analog dazu wird technisch weiter zwischen Verbindungs- und Datenanonymität unterschieden. *Verbindungsanonymität* beschreibt hierbei die Identifikation des Senders bzw. des Empfängers während des Datentransfers. *Datenanonymität* beschreibt das Filtern und Identifizieren der gesendeten Daten [7].

Über die Nutzergruppe von Tor ist, wie für ein Anonymitätsnetzwerk zu erwarten, nicht viel bekannt. Bisherige Beschreibungen der Nutzergruppe orientieren sich vordergründig an der Motivation, die die Nutzer aufgrund ihrer Verortung haben, sich mit der Verwendung von Tor schützen zu wollen. Diesen Beschreibungen zufolge, besteht diese aus Personen verschiedener sozioökonomischer Hintergründe. So werden beispielsweise Journalisten, Strafverfolgungsbeamte, Whistleblower und Aktivisten aber auch Blogger (u. a.) als aktive Nutzergruppen genannt[2]. Gleichermaßen variieren auch die Motive zur Nutzung von Tor. Während die einen das Ziel haben, nicht identifiziert werden zu können, möchten andere primär ihre Daten schützen. In einer Online-Befragung von Harborth et al. wurde Anonymität als Hauptgrund für die Verwendung von PETs, wie bspw. Tor, angegeben [13]. Eine Dimension ist hierbei die Angst vor Deanonymisierung durch bspw. staatliche Akteure. Andere Arbeiten nennen als Motivation zur Nutzung von Tor das Bedürfnis, seine Daten

[2] Users of Tor. https://2019.www.torproject.org/about/torusers.html, Zugegriffen am 21.10.2020

zu schützen, das Bedürfnis, sich mit einer bestimmten Zielgruppe auszutauschen, politische Gründe oder den Konsum potentiell illegalen Materials [9, 10, 15].
Um zu klären, welche Technologie welchen Grad an Anonymität gegenüber welchem Akteur bietet, formulieren wir die folgende qualitative Forschungsfrage:

Forschungsfrage F4: Inwiefern schützen zusätzliche Anonymisierungstechnologien in Kombination mit Tor vor einer potentiellen Deanonymisierung?

Im Folgenden werden wir nun auf die technischen Grundlagen von Tor eingehen, um anschließend in einem nächsten Schritt potentielle Akteure der Deanonymisierung sowie zusätzliche Technologien zum Schutz der Anonymität zu extrahieren.

1.2 Das Tor-Netzwerk

Tor ist das größte und bekannteste Anonymitäts-Netzwerk. Durch das im Tor-Netzwerk verwendete Onion-Routing wird der gesamte Datenverkehr verschlüsselt durch einen Pfad bestehend aus mindestens drei Tor-Knoten geleitet, sodass keiner nachvollziehen kann, wer mit wem und über was kommuniziert. Der erste Knoten in einem solchen Pfad wird als „Guard-Knoten“ bezeichnet. Der mittlere Knoten im Datenpfad wird als „Middle-Knoten“ und der letzte als „Exit-Knoten“ bezeichnet. Abb. 1 zeigt einen Datenpfad, der durch das Tor-Netzwerk aufgebaut wird. Die IP-Adressen dieser Tor-Knoten selbst sind alle öffentlich bekannt. Dadurch kann

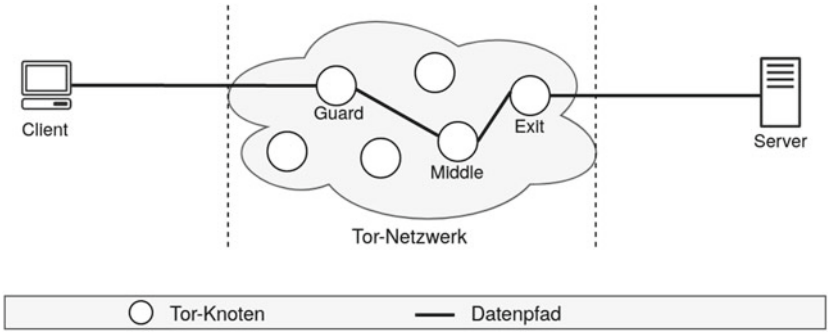


Abb. 1 Datenpfad durch das Tor-Netzwerk

der erwähnte Datenpfad aufgebaut werden, sodass die IP-Adressen der Tor-Nutzer verschleiert werden können und die Tor-Nutzer dadurch anonym sind. Der vom Tor-Nutzer angesprochene Server erfährt nur die IP-Adresse des Exit-Knotens anstatt die des Tor-Nutzers. Es ist allerdings trotz anonymer Kommunikation möglich zu erkennen, ob sich jemand mit dem Tor-Netzwerk verbindet und darüber kommuniziert. Um anonym über das Tor-Netzwerk surfen zu können, kann der Tor-Browser verwendet werden. Der Tor-Browser ist ein modifizierter Web-Browser, der durch die Tor-Software alle Daten durch das Tor-Netzwerk schickt.

1.3 Akteure als mögliche Angreifer

Die Angriffsmöglichkeiten gegen ein beliebiges System sind unzählig. Wir haben uns daher in Anlehnung an frühere Forschung darauf beschränkt, einen Überblick über mögliche Akteure zu geben, die die Anonymität der Tor-Nutzer angreifen können. Ries et al. bewerteten und stufen mögliche Angreifer nach deren subjektiven Einschätzung hinsichtlich auf verfügbare Ressourcen ein [23]. In unserer Arbeit betrachten wir folgende Akteure als Angreifer einer möglichen Deanonymisierung von Tor-Nutzern:

Regierung (R). Eine Regierung ist die höchste Instanz eines Staates und hat am meisten Ressourcen zur Verfügung, um einen beliebigen Angriff gegen die Anonymität eines Tor-Nutzers durchzuführen. Hierzu zählen staatliche Organisationen wie zum Beispiel Geheimdienste.
Internetknoten-Betreiber (IKB). Ein Internetknoten dient als Austauschpunkt des Internet-Datenverkehrs mehrerer Netzwerke. Internetknoten können einen beträchtlichen Teil des Datenverkehrs beobachten [18] und somit auch Datenverkehr zwischen den einzelnen Tor-Knoten.
Internet-Service-Provider (ISP). Der Internet-Service-Provider, oder auch Internetdienstanbieter, stellt den Internetanschluss der Internetnutzer zur Verfügung. Der ISP bekommt alle Internetpakete übermittelt, die von diesem Internetanschluss versendet oder empfangen werden.
Web-Service-Provider (WSP). Der Web-Service-Provider stellt einen Web-Service, wie z. B. eine Internet-Webseite über das Internet zur Verfügung.
Netzwerk-Administrator (NA). Ein Netzwerk-Administrator administriert ein Computernetzwerk und hat Einsicht in den gesamten Datenverkehr des betrachteten Netzwerkes.
Tor-Knoten-Betreiber (TKB). Tor-Knoten-Betreiber stellen Tor-Knoten (Guard- Middle- oder Exit-Knoten) dem Tor-Netzwerk zur Verfügung.

Externe Partei (EP). Eine externe Partei ist eine Einheit außerhalb des Anonymisierungssystem, die jedoch versucht, ein Teil dieses zu werden. Ein Beispiel wäre ein klassischer Hacker.

1.4 Technologien gegen eine Deanonymisierung

Durch das Benutzen des Tor-Browsers kann eine Verbindung zum Tor-Netzwerk hergestellt werden. Dieser verhindert allerdings nicht die Erkennung, dass man sich mit dem Tor-Netzwerk verbunden hat. Demzufolge können die Internetanschlüsse zurückverfolgt werden, die sich mit dem Tor-Netzwerk verbunden haben. Auf Basis von extensiver und allumfassender Literaturrecherche wurden Technologien extrahiert, die man zusätzlich zu der Tor-Software hinzunehmen kann, um eine potentielle Deanonymisierung zu erschweren. Nachfolgend beschreiben wir kurz alle Technologien, die wir in unserer Arbeit betrachten:

VPN. Bei einem ***V****irtual* ***P****rivate* ***N****etwork* wird ein virtueller Tunnel zu einem VPN-Anbieter aufgebaut, durch welchen alle Internetdatenpakete verschlüsselt geleitet werden. Der VPN-Anbieter schickt anschließend alle Datenpakete zum eigentlichen Ziel weiter. Das Vorschalten eines VPNs vor das Tor-Netzwerk kann zusätzlichen Schutz vor dem Guard-Knoten bieten, während ein VPN nach dem Tor-Netzwerk geschaltet zusätzlichen Schutz vor dem Exit-Knoten bieten kann. Hierbei verwendet man allerdings eine zusätzliche Instanz, der man vertrauen muss - den VPN-Anbieter.
Live-(Betriebs-)Systeme. Bei einem Live-(Betriebs-)System wie z. B. Tails oder Whonix werden alle Internet-Verbindungen standardmäßig über das Tor-Netzwerk geleitet. Wie in Abb. 2 zu sehen ist, werden, falls man nicht solche Betriebssysteme verwendet, nur die Daten über das Tor-Netzwerk anonym verschickt, die der Tor-Nutzer direkt über den Tor-Browser versendet. Alle anderen Daten werden weiterhin über Verbindungen des Clearnets verschickt und sind somit nicht anonymisiert.
Bridges und Pluggable Transports (PTs). Bridge-Knoten, sind Tor-Knoten, die nicht öffentlich gelistet werden und so als zusätzliche Einstiegspunkte in das Tor-Netzwerk dienen können, wenn bspw. eine Regierung alle öffentlich bekannten Tor-Knoten blockiert. Durch Pluggable Transports kann der Datenverkehr verschleiert werden, sodass es nicht mehr ersichtlich ist, dass dieser Datenverkehr Tor-Pakete (die eine eindeutige Struktur aufweisen [24]) beinhaltet. Somit kann man eine anonyme Verbindung zum Tor-Netzwerk herstellen.
Eigener Tor-Knoten als Guard-Knoten. Wie in Abb. 1 gezeigt, ist der Guard-Knoten der erste Tor-Knoten in einem Datenpfad, zu dem man sich direkt verbindet.

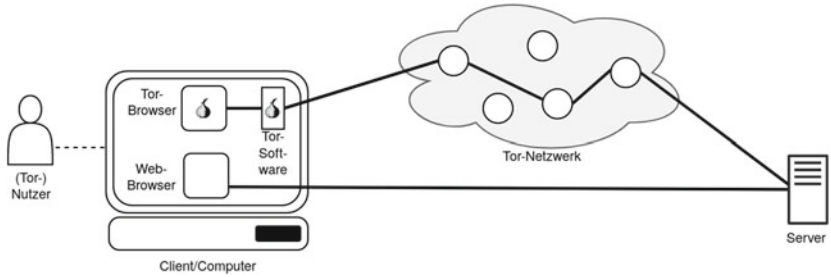


Abb. 2 Verbindungsaufbau über den Tor-Browser vs. Web-Browser

Durch die direkte Verbindung kennt der Guard-Knoten die IP-Adresse des Tor-Nutzers. Demzufolge besitzt der Guard-Knoten eine potentielle Gefahr, Tor-Nutzer angreifen und deanonymisieren zu können. Eine Abhilfe hierfür wäre das Aufsetzen eines eigenen Tor-Knotens und diesen als Guard-Knoten für alle Tor-Verbindungen zu wählen.

PGP. PGP steht für Pretty Good Privacy und wird benutzt, um u. a. digitale Dateien oder Nachrichten zu verschlüsseln und digital zu signieren.

TorChat. TorChat ist ein dezentrales Chatprogramm, das alle Chat-Nachrichten über das Tor-Netzwerk leitet. Neben verschlüsselten Textnachrichten bietet TorChat auch eine sichere Übertragung von Dateien.

Die Verwendung des Tor-Browsers bietet einen Grad an Anonymität auf technischer Basis. Aufgrund unterschiedlicher Ressourcen, die verschiedenen Akteuren zur Verfügung stehen, variiert der Grad der Anonymität allerdings gegenüber unterschiedlichen Akteuren. Die Verwendung von zusätzlichen Technologien kann hier punktuell Abhilfe schaffen.

2 Design und Methode

Für die Beantwortung der Forschungsfragen erfolgt eine Datenerhebung in Form eines Online-Fragebogens (FF1-3) sowie eines Leitfadeninterviews (FF4) mit einem Experten aus dem Bereich der IT-Sicherheitsforschung. Im nachfolgenden Abschnitt werden wir zuerst die Erhebung mittels eines Online-Fragebogens sowie die entsprechenden Variablen erläutern. Daran anschließend werden wir das Vorgehen im Rahmen des Leitfaden-Experteninterviews beschreiben.

2.1 Online-Befragung der Tor-Nutzer

Die Erhebung von Nutzerinformationen, wie Online-Privatheitskompetenz sowie Nutzungsweise ist im Rahmen einer Online-Befragung von Tor-Nutzern erfolgt.

Analysen der Sprache der Inhalte des Tor-Netzwerks zeigen, dass über 75 % des Angebots in englischer Sprache, gefolgt von u. a. Russisch und Deutsch, vorhanden ist [26, 27]. Um ein möglichst großes Publikum zu erreichen, wurde der Fragebogen auf Englisch und Deutsch zur Verfügung gestellt. Der Fragebogen wurde auf den Servern der Fraunhofer Gesellschaft gehostet und via LimeSurvey administriert. Die Einstellungen wurden so getroffen, dass auch eine Teilnahme mit dem Tor-Browser, ohne JavaScript, möglich war. Die Verteilung des Fragebogens erfolgte sowohl im Clear- als auch im Darknet.

Insgesamt bestand der Fragebogen aus 31 Fragen, wobei die erste Frage erfasste, ob die Person den Tor-Browser schon einmal verwendet hatte. Wurde diese Frage verneint, war der Fragebogen an dieser Stelle zu Ende. Um bei den Fragen voranzuschreiten, war die Beantwortung aller Fragen verpflichtend. Einzig die Fragen zur Soziodemografie waren optional.

2.2 Experteninterview

In einem ersten Schritt wurden anhand extensiver Literaturrecherche Technologien aus der Literatur extrahiert, die zusätzlich zur Verwendung des Tor-Browsers eine mögliche Deanonymisierung erschweren. Da sich die Möglichkeit einer potentiellen Deanonymisierung maßgeblich an den vorhanden Ressourcen bemisst, die dem Angreifer zur Verfügung stehen, wurden diese in Anlehnung an frühere Forschung [23] auf die folgenden Ausprägungen festgelegt: Regierung, Internetknoten-Betreiber, Internet-Service-Provider, Web-Service-Provider, lokaler Netzwerkadministrator, Tor-Knoten-Betreiber, externe Partei. In einer Matrix wurde den Technologien dann für jeden oben genannten potentiellen Angreifer auf der Basis eines Experteninterviews eine Gewichtung zugeteilt. Diese orientiert sich an dem Aufwand, mit dem es hinsichtlich der Ressourcen des Angreifers zu einer Deanonymisierung kommen kann.

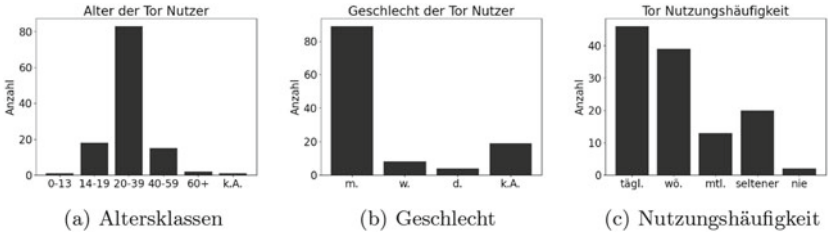
3 Ergebnisse

Nachfolgend werden wir zuerst eine deskriptive Beschreibung des Datensets sowie der soziodemografischen Daten präsentieren. Daran anschließend analysieren wir

die Fragen auf die von uns gestellten Hypothesen hin. Abschließend präsentieren wir das Ergebnis des Experteninterviews zur Erstellung einer Anonymitätsmatrix.

3.1 Datenbeschreibung

Der Fragebogen wurde insgesamt 238 Mal aufgerufen, wovon 120 Personen ihn komplett ausfüllten. Dabei gaben $N = 206$ Nutzer (86,55 %) an, den Tor-Browser schon einmal verwendet zu haben. $N = 11$ (4,62 %) Personen gaben an, den Tor-Browser noch nie verwendet zu haben und beendeten dadurch die Umfrage. $N = 21$ Nutzer (8,82 %) beendeten die Umfrage, ohne die Frage zu beantworten.
Von den 120 Personen, die den Fragebogen komplett ausgefüllt haben, konstituierte die Altersgruppe zwischen 20 bis 39 Jahren mit $N = 83$ (69,17 %) den Großteil der Teilnehmer. $N = 18$ (15,0 %) gehörten der Altersgruppe 14 bis 19 an, gefolgt von $N = 15$ (12,5 %) für die Gruppe der 40 bis 59 jährigen. Eine Person (0,83 %) gab an unter 14 zu sein, $N = 2$ (1,67 %) weitere über 60. $N = 1$ Person enthielt sich der Angabe (vgl. Abb. 3a).
Von den Personen, die freiwillig Angaben zu ihrem Geschlecht gemacht haben, sind $N = 89$ (74,17 %) männlichen Geschlechts, $N = 8$ (6,67 %) weiblich sowie $N = 4$ (3,33 %), die sich mit der Kategorie „anderes“ identifiziert haben (vgl. Abb. 3b).
$N = 46$ (38,33 %) Personen gaben an, Tor täglich zu nutzen. $N = 39$ (32,5 %) nutzen Tor wöchentlich, $N = 13$ (10,83 %) monatlich und $N = 20$ (16,67 %) nutzen Tor seltener. $N = 2$ (1,67 %) Personen gaben an, Tor nie zu verwenden (vgl. Abb. 3c).



(a) Altersklassen (b) Geschlecht (c) Nutzungshäufigkeit

Abb. 3 Teilnehmer der Umfrage

3.2 Analyse

Die Online-Privatheitskompetenz der Tor-Nutzer wurde anhand der Online-Privatheitskompetenzskala OPLIS [17] gemessen. Hierbei wurde der Fragenblock zu „Wissen über Datenschutzrecht" aufgrund der Tatsache ausgelassen, dass dieser auf Basis von deutschem/europäischem Recht entstanden ist, sich die vorliegende Umfrage jedoch an Tor-Nutzer weltweit richtete. Somit umfasste die Erhebung der Online-Privatheitskompetenz 15 statt 20 Fragen. Um eine Vergleichbarkeit der Ergebnisse zu erreichen, wurde im Rahmen der Analyse, angelehnt an neueste Untersuchungen, der Score von 15 auf 20 Fragen extrapoliert [12].

Die Ergebnisse indizieren, dass Tor-Nutzer im Schnitt 81,65 % der Fragen richtig beantwortet haben. Weitere Analysen betreffend soziodemografischer Aspekte zeigten in einer Varianzanalyse keinen signifikanten Effekt des Alters der Tor-Nutzer auf ihre Online-Privatheitskompetenz ($F(2,113) = 1.92$, $p = .152$). Betreffend dem Bildungsgrad hat eine Varianzanalyse ergeben, dass es einen signifikanten Effekt des Bildungsabschlusses auf die Online-Privatheitskompetenz gab ($F(4,112) = 2.98$, $p = .022$). Eine anschließende post-hoc Analyse mit paarweise durchgeführten t-Tests zeigt, dass Personen, die das Abitur abgeschlossen haben ($M = 13.14$, $SD = 1.53$), eine höhere Privatheitskompetenz zeigen, als solche, die studiert haben (($M = 12.12$, $SD = 1.65$), $t(36.53) = 2.60$, $p = .013$, $d = 0.63$), oder auch als solche, die keinen Schulabschluss haben (($M = 11.59$, $SD = 1.80$), $t(31.45) = 2.83$, $p = .08$, $d = 0.9$).

H1a-d postulieren einen Effekt der Nutzungsweise von Tor auf die Online-Privatheitskompetenz. Die Ergebnisse von *H1a* zeigen auf Basis der Berechnung einer einfaktoriellen ANOVA, dass es keinen statistisch signifikanten Effekt der Häufigkeit der Nutzung des Tor-Browsers auf die Online-Privatheitskompetenz der Nutzer gibt ($F(4,115) = 0.239$, $p = .916$). Die Ergebnisse von *H1b* zeigen auf Basis der Berechnung einer einfaktoriellen ANOVA, dass es keinen statistisch signifikanten Effekt des Kontexts der Nutzung des Tor-Browsers auf die Online-Privatheitskompetenz der Nutzer gibt ($F(2,117) = 1.443$, $p = .24$). Die Ergebnisse von *H1c* indizieren, dass Personen, die am Themenbereich „Anonymität" interessiert sind, höhere Werte auf der Online-Privatheitskompetenz-Skala ($M = 12.59$, $SD = 1.58$) erreichten, als solche, die am Themenbereich „Anonymität" nicht interessiert sind (($M = 11.96$, $SD = 1.77$), $t(95.69) = -2.01$, $p = .047$, $d = 0.38$). Die Ergebnisse für *H1d* zeigen, dass Personen, die Tor für „Marktplätze/Handelsseiten" nutzen, niedrigere Werte ($M = 11.32$, $SD = 1.57$) auf der Online-Privatheitskompetenzskala erreichten, als solche, die Tor nicht für „Marktplätze/Handelsseiten" nutzen (($M = 12.52$, $SD = 1.64$), $t(26.01) = 3.065$, $p = .005$, $d = 0.74$).

H2a-d postulieren einen Effekt der Nutzungsweise von Tor auf die in Kombination zu Tor genutzten Anonymisierungstechnologien. Die Ergebnisse zu *H2a* haben auf Basis einer Varianzanalyse ergeben, dass es einen signifikanten Effekt der Nutzungshäufigkeit gab ($F(3,114) = 5.20$, $p = .02$). Eine anschließende post-hoc Analyse mit paarweise durchgeführten t-Tests zeigt, dass Personen, die täglich Tor benutzen ($M = 5.50$, $SD = 1.22$), mehr Technologien kennen, als solche, die Tor wöchentlich (($M = 4.69$, $SD = 1.52$), $t(72.61) = 2.66$, $p = .01$, $d = 0.71$), monatlich (($M = 4.62$, $SD = 1.33$), $t(72.61) = 2.66$, $p = .01$, $d = 0.59$) oder noch seltener (($M = 4.10$, $SD = 1.74$), $t(27.49) = 3.26$, $p = .003$, $d = 1.00$) benutzen. Da die Gruppen im Rahmen der Analyse von *H2b* nicht normalverteilt waren, wurde ein Kruskal-Wallis Rangsummentest durchgeführt. Dieser zeigt, dass es einen signifikanten Effekt des Netzwerktyps auf die Anzahl der bekannten Technologien gab ($H(2) = 22.229$, $p < .001$). Eine anschließende post-hoc Analyse mit paarweise durchgeführten t-Welch-Tests zeigt, dass Personen, die beide Netzwerke ansteuern ($M = 5.39$, $SD = 1.16$), mehr Technologien kennen, als solche Personen, die Tor nur für das Clearnet benutzen (($M = 4.09$, $SD = 1.75$), $t(47.15) = -3.951$, $p < .001$, $d = -0.88$), oder als solche, die Tor nur für das Darknet benutzen (($M = 4.29$, $SD = 1.54$), $t(47.15) = -3.951$, $p = .022$, $d = -0.81$). Für *H2c* hat eine Varianzanalyse gezeigt, dass Personen, die am Themenbereich „Pornographie“ interessiert sind, weniger Anonymisierungstechnologien ($M = 3.94$, $SD = 1.75$) kennen, als diejenigen, die am Themenbereich „Pornographie“ nicht interessiert sind (($M = 5.05$, $SD = 1.42$), $t(19.62) = 2.480$, $p = .022$, $d = 0.76$). Darüber hinaus kennen Personen mit Interesse am Bereich „Software“ mehr Anonymisierungstechnologien ($M = 5.80$, $SD = 0.56$), die zusätzlich zu Tor verwendet werden können, als diejenigen, die am Themenbereich „Software“ nicht interessiert sind (($M = 4.76$, $SD = 1.56$), $t(53.31) = 24.42234$, $p < .001$, $d = -0.70$). Die Analyse von *H2d* hat gezeigt, dass Personen, die „Krypto“-Dienste in Anspruch nehmen, mehr Anonymisierungstechnologien kennen ($M = 5.61$, $SD = 0.76$) als solche, die „Krypto“-Dienste nicht in Anspruch nehmen (($M = 4.64$, $SD = 1.63$), $t(108.10) = 19.56$, $p < .001$, $d = -0.67$). Personen, die „Filesharing“-Dienste nutzen, kennen mehr Anonymisierungstechnologien ($M = 5.43$, $SD = 1.03$) als solche, die „Filesharing“-Dienste nicht nutzen (($M = 4.78$, $SD = 1.58$), $t(42.71) = 5.62$, $p = .022$, $d = -0.43$). Personen, die „Foren“ benutzen, kennen mehr Anonymisierungstechnologien ($M = 5.28$, $SD = 1.25$) als diejenigen, die „Foren“ nicht benutzen (($M = 4.49$, $SD = 1.65$), $t(108.08) = 8.59$, $p = .004$, $d = -0.54$).

Tab. 1 zeigt, dass insgesamt 27 der Befragten angaben, ein VPN als zusätzliche Anonymisierungstechnologie vor das Tor-Netzwerk schalten. 17 der Befragten

Tab. 1 Tor-Nutzer, die angaben, eine Technologie zusätzlich zu Tor zu nutzen

Technologie	VPN (vor)	VPN (nach)	Tails Whonix	Bridges und PTs	Eigener Guard-Knoten	PGP
Anzahl	27	17	54	27	11	67

gaben an, ein VPN hinter das Tor-Netzwerk zu schalten. Live-Betriebssysteme wie Tails oder Whonix nutzen 54 der Befragten. Über Bridge-Knoten verbinden sich 27 Nutzer mit dem Tor-Netzwerk und 11 gaben an, einen eigenen Guard-Knoten für die Verbindung in das Tor-Netzwerk zu nutzen. PGP wird von 67 Nutzern zusätzlich verwendet. Eine Mehrfachnennung war möglich.

In Abb. 4 werden die prozentualen Anteile der Tor-Nutzer, die eine zusätzliche Technologie zu der Verwendung von Tor hinzunehmen, illustriert. Konkret wurden hier die zusätzlichen Anonymisierungstechnologien auf die Variablen der a) Nutzungshäufigkeit, b) Art der Hidden Services, c) Nutzungsweise und d) Themengebiete dargestellt. Beispielsweise nutzen von den 67 Personen, die angeben PGP zu verwenden, ca. 51 % Tor täglich, 28 % wöchentlich und 21 % seltener (vgl. Abb. 4a). Am meisten werden zusätzliche Technologien hinzugenommen, wenn Foren oder soziale Netzwerke im Darknet angesurft werden. Für den Aufruf von pornografischen Seiten wird hingegen weniger zusätzliche Technologien hinzugenommen (vgl. Abb. 4b). Nutzer, die Tor zum Surfen sowohl ins Clearnet als auch ins Darknet verwenden, nutzen vermehrt zusätzliche Technologien, als Nutzer, die Tor nur für das Darknet oder nur für das Clearnet nutzen (vgl. Abb. 4c). Am häufigsten werden zusätzliche Technologien bei Tor-Nutzern hinzugenommen, die sich für die Themen „Anonymität" und „(IT-) Sicherheit" interessieren. Am wenigsten von Nutzern, die sich für Themen wie zum Beispiel Kunst, Online-Spiele, Sport oder Wissenschaft interessieren. Diese werden in Abb. 4d nicht mit angegeben.

H3a-b postuliert einen kausalen Effekt der Online-Privatheitskompetenz der Nutzer auf die in Kombination zu Tor verwendeten Anonymisierungstechnologien. Die Ergebnisse von *H3a* zeigen auf Basis der Berechnung einer linearen Regressionsanalyse keine statistisch signifikanten Ergebnisse ($F = 0.9737$). Auf Basis unserer Werte kann somit nicht von einem derartigen Effekt ausgegangen werden.

H3b Die Ergebnisse von *H3b* zeigen auf Basis der Berechnung einer linearen Regressionsanalyse keine statistisch signifikanten Ergebnisse ($F = 0.2299$). Es besteht somit auf Basis unserer Werte kein linearer Effekt der Online-Privatheitskompetenz der Nutzer auf die Anzahl der einem Nutzer bekannten Anonymisierungstechnologien.

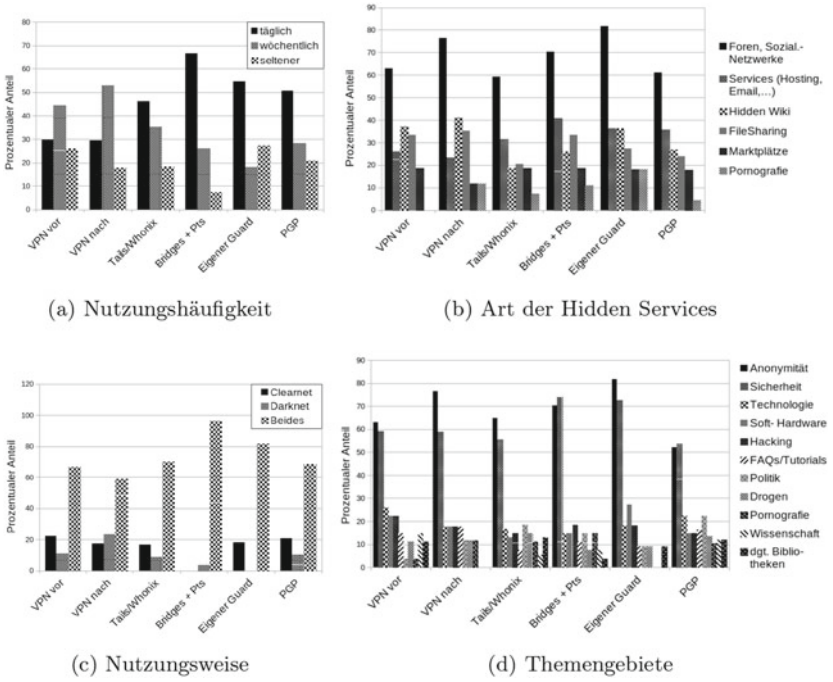


Abb. 4 Prozentualer Anteil der Tor-Nutzer, die eine weitere Technologie zusätzlich zu Tor nutzen

3.3 Anonymitätsmatrix

Forschungsfrage 4 untersucht, inwiefern zusätzliche Anonymisierungstechnologien in Kombination mit Tor vor einer potentiellen Deanonymisierung schützen. Die erstellte Matrix gibt an, welcher Akteur aus Kap. 1.3 erkennen kann, ob ein bestimmter Tor-Nutzer mit den jeweiligen eingesetzten Technologien

a) Tor benutzt und
b) welche Aktivität der Tor-Nutzer über das Tor-Netzwerk durchführt.

Die Einstufung erfolgt mittels der Skala

● schwer, ◑ mittel, ○ leicht

Tab. 2 Anonymitätsmatrix R

Akteur / Technologie	R (a)/(b)	IKB (a)/(b)	ISP (a)/(b)	NA (a)/(b)	TKB_G (a)/(b)	TKB_M (a)/(b)	TKB_E (a)/(b)	WSP (a)/(b)	EP (a)/(b)
Tor-Browser	○/◑	○/●	○/●	○/●	○/●	●/●	⊛/⊛	⊛/⊛	●/●
VPN (vor)	○/◑	◑/●	●/●	●/●	●/●	●/●	⊛/⊛	⊛/⊛	●/●
VPN (nach)	○/◑	○/●	○/●	○/●	○/●	●/●	●/●	⊛/⊛	●/●
Tails, Whonix	○/◑	○/●	○/●	○/●	○/●	●/●	⊛/⊛	⊛/⊛	●/●
Bridges, PTs	◑/◑	●/●	●/●	●/●	○/●	●/●	⊛/⊛	⊛/⊛	●/●
Eigenen Guard-Knoten	○/◑	○/●	○/●	○/●	n/a	●/●	⊛/⊛	⊛/⊛	●/●
TorChat	○/◑	○/●	○/●	○/●	○/ ●	●/●	●/●	●/●	●/●

Regierung. IKB: Internetknoten-Betreiber. ISP: Internet-Service-Provider. NA: Netzwerk-Administrator. TKB_G: Tor-Knoten-Betreiber (Guard). TKB_M: Tor-Knoten-Betreiber (Middle). TKB_E: Tor-Knoten-Betreiber (Exit). WSP: Web-Service-Provider. EP: Externe Partei.
Aufheben der Verbindungsanonymität: ● schwer, ◑ mittel, ○ leicht
Aufheben der Datenanonymität: ⊛

In dieser Skala wird nur die Verbindungsanonymität berücksichtigt, also Informationen, die ausgewertet werden können, die aufgrund des Verbindungsaufbaus selbst anfallen. Die Datenanonymität, also die Dateninhalte, die über diese Verbindung verschickt werden, werden in der angegebenen Skala nicht berücksichtigt. All diese Informationen könnte aber der Exit-Knoten auslesen, sollte der Tor-Nutzer anstatt einer HTTPS-Verbindung nur eine unverschlüsselte HTTP-Verbindung zum Server im Clearnet aufbauen. Gibt der Tor-Nutzer dann u. a. personenbezogene Daten wie beispielsweise den Namen, die Adresse oder andere kritische Informationen über sich selbst bekannt, ist dadurch auch die soziale Anonymität gefährdet. Gleiches gilt für den Web-Service-Provider, der einen Tor-Nutzer identifizieren kann, wenn dieser sich z. B. auf einer Plattform mit seinen Benutzernamen anmeldet. In der Matrix werden solche Aspekte mit

⊛ (Datenanonymität)

gekennzeichnet. Tab. 2 zeigt die erstellte Matrix.

Zu Beachten ist, dass eine Regierung immer die Möglichkeit einer Quellen-TKÜ (Telekommunikationsüberwachung) hat. Durch einen sog. Bundestrojaner kann eine Regierung immer ausspähen, welcher Tor-Nutzer mit wem über was kommuniziert, da dieser Trojaner alle Daten vor dem Verschlüsseln und dem Verschicken in das Tor-Netzwerk direkt auf dem Anwender-PC ausliest. Sollte eine TKÜ zum Einsatz kommen, wird dies hier als *mittel* eingestuft.

4 Diskussion

Ziel der vorliegenden Arbeit war es, die Tor-Nutzergruppe auf ihre Online-Privatheitskompetenz, die Nutzungsweise und Grad der Anonymität zu erforschen. Außerdem wurde eine Anonymitätsmatrix erstellt, in welcher aufgezeigt wurde, inwieweit diverse PETs in Kombination zu Tor vor einer Deanonymisierung vor entsprechenden Akteuren schützt. Die vorliegende Analyse zeigt eine höhere Online-Privatheitskompetenz im Vergleich zu regulären Internetnutzern. Hier gilt es allerdings zu beachten, dass unsere Werte auf Basis von 15 Fragen der OPLIS-Skala auf 20 extrapoliert wurden. Allerdings sind diese Ergebnisse übereinstimmend mit jüngsten Forschungsergebnissen [12]. Einflussfaktoren sind hierbei der Bildungsabschluss, Interessengebiete wie „Anonymität“ sowie die Nutzungsweise für „Marktplätze“. Im Gegensatz zu früheren Arbeiten konnte kein Einfluss des Alters der Nutzer auf die Online-Privatheitskompetenz festgestellt werden. Einflussfaktoren betreffend des Wissens bzw. der Verwendung zusätzlicher Anonymisierungstechnologien sind die Interessensbereiche der Verwendung, wie „Pornografie“ und „Software“, sowie der Kontext der Anwendung. Die Nutzergruppen, die am meisten zusätzliche Technologien verwenden, interessieren sich für die Themen Anonymität und Sicherheit und rufen Foren oder soziale Netzwerke im Darknet auf. Jedoch ist es fraglich, inwieweit Personen, die nicht gesetzeskonformes Material anbieten oder konsumieren wollen, an einer solchen Umfrage teilnehmen und, wenn sie teilnehmen, inwieweit sie diese Informationen angeben.

Betreffend der Anonymitätsmatrix kann generell gesagt werden, dass der Grad der Anonymität davon abhängig ist, welche Ressourcen einem Angreifer zur Verfügung stehen. Ob und wie gut ein Akteur einen Tor-Nutzer deanonymisieren kann, hängt maßgeblich von den Ressourcen des Angreifers ab. Auf Basis dieser Ergebnisse kommen wir zu dem Schluss, dass es einen 100-prozentigen Schutz vor einer möglichen Deanonymisierung nicht geben wird. In Anlehnung an frühere Arbeiten werden dem Akteur „Regierung“ die meisten Ressourcen attribuiert [23]. So hat sie die meisten Möglichkeiten, das Internet flächendeckend überwachen zu können. Insbesondere wäre eine Regierung in der Lage, andere Akteure zum Kooperieren anzuweisen und demzufolge alle Ressourcen der anderen Akteure zu nutzen.

Danksagung Das dieser Publikation zugrunde liegende Verbundprojekt PANDA wurde vom Bundesministerium für Bildung und Forschung unter den Förderkennzeichen 13N14355 und 13N14356 gefördert. Für den Inhalt dieser Publikation sind die Autoren verantwortlich. Die Autoren bedanken sich insbesondere bei York Yannikos für wertvollen Input zur Durchführung der Studie. Außerdem bedanken sie sich bei Oskar Rudolf für die Unterstützung bei der Auswertung der Studie sowie Adrian Worring Pozo und Adrian Kailus für die Unterstützung

bei der Vorbereitung der Durchführung. Schließlich bedanken sie sich bei Charlotta Jacobsen für das Korrekturlesen und ihre Unterstützung beim Editieren.

Literatur

1. Acquisti, A., Gross, R.: Imagined communities: awareness, information sharing, and privacy on the Facebook. In: International Workshop on Privacy Enhancing Technologies. S. 36–58. Springer, Berlin (2006)
2. Altman, I.: The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. Irvington, New York (1975)
3. Barnes, S.B.: A privacy paradox: social networking in the United States. First Monday (2006)
4. Biryukov, A., Pustogarov, I., Thill, F., Weinmann, R.P.: Content and popularity analysis of tor hidden services. In: 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW). S. 188–193. IEEE (2014)
5. Burgoon, J.K.: Privacy and communication. Ann. Int. Commun. Assoc. **6**(1), 206–249 (1982)
6. Debatin, B., Lovejoy, J.P., Horn, A.K., Hughes, B.N.: Facebook and online privacy: attitudes, behaviors, and unintended consequences. J. Comput. Mediat. Commun. **15**(1), 83–108 (2009)
7. Diaz, C., Seys, S., Claessens, J., Preneel, B.: Towards measuring anonymity. In: International Workshop on Privacy Enhancing Technologies. S. 54–68. Springer, Berlin (2002)
8. Dienlin, T., Trepte, S.: Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur. J. Soc. Psychol. **45**(3), 285–297 (2015)
9. Gehl, R.W.: Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P. MIT Press, Cambridge (2018)
10. Gehl, R.W., Synder-Yuly, J.: The need for social media alternatives. Democratic Commun. **27**(1), 78–78 (2016)
11. Graeff, T.R., Harmon, S.: Collecting and using personal data: consumers' awareness and concerns. J. Consum. Market. (2002)
12. Harborth, D., Pape, S.: How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies: The case of Tor. ACM SIGMIS Database: The DATABASE Adv. Inf. Syst. **51**(1), 51–69 (2020)
13. Harborth, D., Pape, S., Rannenberg, K.: Explaining the technology use behavior of privacy-enhancing technologies: The case of Tor and Jondonym. Proc. Priv. Enhancing Technol. **2020**(2), 111–128 (2020)
14. Hayne, S.C., Rice, R.E.: Attribution accuracy when using anonymity in group support systems. Int. J. Hum.-Comput. Stud. **47**(3), 429–452 (1997)
15. Jardine, E.: Privacy, censorship, data breaches and internet freedom: the drivers of support and opposition to dark web technologies. New Media Soc. **20**(8), 2824–2843 (2018)
16. Jensen, C., Potts, C., Jensen, C.: Privacy practices of internet users: self-reports versus observed behavior. Int. J. Hum.-Comput. Stud. **63**(1–2), 203–227 (2005)
17. Masur, P.K., Teutsch, D., Trepte, S.: Entwicklung und validierung der online-privatheitskompetenzskala (oplis). Diagnostica (2017)

18. Murdoch, S.J., Zieliński, P.: Sampled traffic analysis by internet-exchange-level adversaries. In: International Workshop on Privacy Enhancing Technologies. S. 167–183. Springer, Berlin (2007)
19. Owen, G., Savage, N.: Empirical analysis of tor hidden services. IET Inf. Secur. **10**(3), 113–118 (2016)
20. Paine, C., Reips, U.D., Stieger, S., Joinson, A., Buchanan, T.: Internet users' perceptions of „privacy concerns" and „privacy actions". Int. J. Hum.-Comput. Stud. **65**(6), 526–536 (2007)
21. Park, Y.J.: Digital literacy and privacy behavior online. Commun. Res. **40**(2), 215–236 (2013)
22. Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., Dabbish, L.: Anonymity, privacy, and security online. Pew Res. Center **5** (2013)
23. Ries, T., Panchenko, A., Engel, T. et al.: Comparison of low-latency anonymous communication systems-practical usage and performance. In: Ninth Australasian Information Security Conference. S. 77–86. ACS, Australia (2011)
24. Saputra, F.A., Nadhori, I.U., Barry, B.F.: Detecting and blocking onion router traffic using deep packet inspection. In: 2016 International Electronics Symposium (IES). S. 283–288. IEEE, New Jersey (2016)
25. Shelton, M., Rainie, L., Madden, M.: Americans' privacy strategies post-snowden. Pew Research Center (2015), http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/
26. Spitters, M., Verbruggen, S., van Staalduinen, M.: Towards a comprehensive insight into the thematic organization of the tor hidden services. In: 2014 IEEE Joint Intelligence and Security Informatics Conference. S. 220–223. IEEE, California (2014)
27. Steinebach, M., Schäfer, M., Karakuz, A., Brandl, K., Yannikos, Y.: Detection and analysis of tor onion services. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, S. 1–10. ACM, New York (2019)
28. Trepte, S., Dienlin, T.: Privatsphäre im internet. Neue Medien und deren Schatten. Mediennutzung, Medienwirkung und Medienkompetenz, , S. 53–79 (2014)
29. Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhöfer, A., Lind, F.: Do people know about privacy and data protection strategies? towards the „online privacy literacy scale" (oplis). In: Reforming European data protection law, S. 333–365. Springer, Dordrecht (2015)
30. Weinberger, M., Zhitomirsky-Geffet, M., Bouhnik, D.: Factors affecting users' online privacy literacy among students in Israel. Online Inf. Rev. **41**, 655–671 (2017)
31. Westin, A.: Privacy and freedom new york atheneum, 1967. Privacy and Personnel Records, The Civil Liberties Review (Jan./Feb., 1976) S. 28–34 (1967)
32. Wills, C., Zeljkovic, M.: A personalized approach to web privacy-awareness, attitudes and actions. Worcester Polytechnic Institute, Worcester (2010)

Deanonymisierung im Tor-Netzwerk – Technische Möglichkeiten und rechtliche Rahmenbedingungen

Sandra Wittmer, Florian Platzer, Martin Steinebach und York Yannikos

Zusammenfassung

Eine anonyme Nutzung des Internets wird durch die Verwendung sogenannter „Darknet-Technologien“ wie der Tor-Software ermöglicht und ist hierzulande grundrechtlich geschützt. Neben zahlreichen positiven Verwendungszwecken werden solche Technologien allerdings oft auch zur anonymen Begehung von Straftaten eingesetzt. Da ein Verbot von Anonymisierungstechnologien sowohl aus technischer, als auch aus rechtlicher Sicht abzulehnen ist, wendet sich dieser Beitrag den Möglichkeiten der Strafverfolgung im Tor-Netzwerk zu. Es werden Vorgehensweisen zur Identifizierung tatverdächtiger Personen vorgestellt und aus rechtlicher Perspektive bewertet, ob diese von den derzeit existierenden Ermittlungsbefugnissen der Strafverfolgungsbehörden gedeckt wären. Anhand dieser Erkenntnisse soll eine Diskussionsgrundlage für strafrechtliche Ermittlungen im Tor-Netzwerk geschaffen werden, ohne die Legitimität einer anonymen Nutzung des Internets grundsätzlich in Frage zu stellen.

S. Wittmer (✉)
TU Darmstadt, Darmstadt, Deutschland
E-mail: sandra.wittmer@sit.fraunhofer.de

F. Platzer · M. Steinebach · Y. Yannikos
Fraunhofer SIT, Darmstadt, Deutschland
E-mail: florian.platzer@sit.fraunhofer.de

M. Steinebach
E-mail: martin.steinebach@sit.fraunhofer.de

Y. Yannikos
E-mail: york.yannikos@sit.fraunhofer.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_8

Schlüsselwörter

Tor • Deanonymisierung • Technische Möglichkeiten • Rechtliche Rahmenbedingungen • Strafverfolgung • Darknet • Cybercrime

1 Einleitung

Tor – ursprünglich ein Akronym für „The Onion Router" – ist eine Darknet-Technologie zur Anonymisierung von Internet-Datenverkehr.[1] Die Tor-Software hat zum Ziel, ihren Nutzer*innen Anonymität und Zensurfreiheit im Internet bereitzustellen. In diesem Kapitel werden die technischen Grundlagen der Software erläutert und auf die Rolle des Tor-Netzwerks bei der Begehung von Straftaten eingegangen. Außerdem wird die Bedeutung einer anonymen Nutzung des Internets diskutiert.

1.1 Was ist das Tor-Netzwerk?

Anonyme Netzwerke wie Tor ermöglichen eine hinsichtlich zuordenbarer IP-Adressen anonyme Internet-Kommunikation und mittels der im Tor-Protokoll unterstützten „hidden services" auch den Betrieb von anonymen Servern. Dies wird dadurch erreicht, dass der gesamte Datenverkehr mehrfach verschlüsselt und über Datenpfade geleitet wird, die aus mindestens drei Tor-Knoten bestehen.[2] Dieses mehrlagige Verschlüsselungsschema – jeder Tor-Knoten „schält" eine Schicht der Verschlüsselung ab und leitet den entschlüsselten Teil an den nächsten Tor-Knoten weiter – ist dabei namensgebend für das Onion Routing (zu deutsch „Zwiebelrouting", vgl. Abb. 1). Bei den verwendeten Tor-Knoten, welche auch Tor-Relays oder Tor-Nodes genannt werden, handelt es sich um Rechner, die von Unterstützer*innen des Tor-Netzwerks freiwillig für die Weiterleitung des Datenverkehrs zur Verfügung gestellt werden. Jeder Tor-Knoten erhält dabei nur die Information, von welchem Tor-Knoten die aktuellen Datenpakete gesendet wurden und an welchen Tor-Knoten die Datenpakete als nächstes weitergeleitet werden müssen. Auf diese Weise wird verhindert, dass Dritte nachvollziehen können, wer mit wem und über was im Internet kommuniziert.

[1] Zur Kritik am Präfix „dark" und den damit einhergehenden negativen Assoziations- und Deutungsrahmen vgl. *Bovermann* (2019) [6], Framing-Check: Darknet, Süddeutsche Zeitung (03.05.2019), https://www.sueddeutsche.de/kultur/framing-darknet-tor-anonym-internet-silk-road-1.4367011 (letzter Zugriff: 10.10.2020).

[2] Hierzu ausführlich *Dingledine/Mathewson/Syverson* (2004) [9], Tor: The second-generation onion router, Naval Research Lab Washington DC 2004.

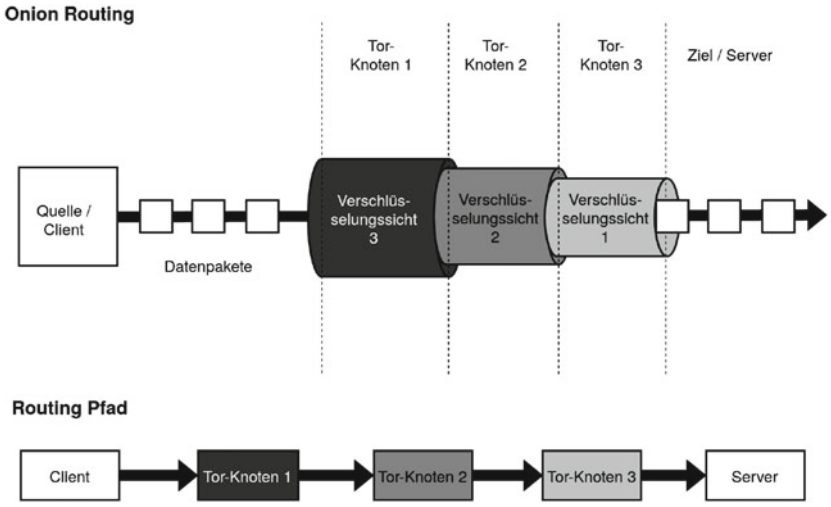


Abb. 1 Prinzip des Onion-Routings

1.2 Grundrechtlicher Schutz von Anonymität im Internet

Zu den positiven Verwendungszwecken von Anonymisierungstechnologien wie der Tor-Software zählt der freie Zugriff auf Informationen in autoritären politischen Umgebungen, wodurch etwa die Arbeit von Journalist*innen und Whistleblower*innen weltweit erleichtert wird. Außerdem lässt sich von der in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG durch das Grundrecht auf informationelle Selbstbestimmung geschützten Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen, durch den Einsatz der Tor-Software ideal Gebrauch machen.[3] Verfassungsrechtlich wird die Vertraulichkeit von Telekommunikationsvorgängen darüber hinaus auch durch das Fernmeldegeheimnis aus Art. 10 Abs. 1 Var. 3 GG gewährleistet, worunter neben den konkreten Inhalten der Kommunikation auch die näheren Umstände – also ob, wann und vor allem wer mit wem kommuniziert hat – fallen.[4] Hinzu kommt, dass sogenannte „chilling effects", welche die Nichtausübung von Grund- und Freiheitsrechten aus Furcht vor staatlicher Überwachung bezeichnen, durch die Verwendung von Anonymisierungssoftware

[3] Siehe hierzu bereits *Rückert* (2018) [24], Politische Studien 479/2018, S. 17.

[4] Vgl. BVerfGE 125, 260, 309 (Vorratsdatenspeicherung).

vermieden werden können.[5] Der Einsatz von Anonymisierungsdiensten wie der Tor-Software ist hierzulande demnach grundrechtlich geschützt und hat zahlreiche gesellschaftlich wünschenswerte Verwendungszwecke vorzuweisen.

1.3 Missbrauch der Tor-Software zur Begehung von Straftaten

Oftmals wird die Tor-Software jedoch auch dazu genutzt, Straftaten im Internet möglichst anonym zu begehen. In den letzten Jahren hat sich im Tor-Netzwerk daher eine Vielzahl neuartiger Kriminalitätsphänomene etabliert, die Strafverfolgungsbehörden auf der ganzen Welt vor Herausforderungen stellen. Webseiten mit tausenden Mitgliedern, über die verschiedene illegale Handelsgüter angeboten werden, sind hierfür bekannte Beispiele. Diese Webseiten funktionieren wie konventionelle E-Commerce-Plattformen im Clearnet, wohingegen dort praktisch alles gehandelt wird, was sich im legalen Marktgeschehen nicht veräußern lässt.[6] Die staatliche Verpflichtung, solche strafbare Aktivitäten effektiv zu verfolgen, wird durch den Einsatz der Tor-Software jedoch erheblich erschwert. Identifizierungsansätze, die bei Ermittlungen im Internet standardmäßig zur Anwendung kommen, bleiben im Tor-Netzwerk infolge des Onion-Routing erfolglos. Klassische Ermittlungsinstrumente – wie zum Beispiel Datenabfragen nach den §§ 14, 15 TMG oder strafprozessuale Auskunftsverlangen i. S. v. § 100j StPO – stehen den Ermittler*innen daher nicht zur Verfügung. So kommt es, dass auf Webseiten im Tor-Netzwerk ganz offen illegale Inhalte angeboten werden, ohne dass die betreffenden Plattformen von den Strafverfolgungsbehörden abgeschaltet werden können.

1.4 Ablehnung der Forderung nach einem „Darknet-Verbot"

Der Vorschlag, eine Nutzung von Anonymisierungstechnologien aus diesem Grund gänzlich zu verbieten, ist allerdings abzulehnen. Einerseits wäre ein solches Verbot bereits aus technischer Sicht nicht realisierbar, da neben der Tor-Software weitere Anonymisierungsdienste wie I2P, Freenet oder JonDo existieren, die alle auf unterschiedlichen Technologien basieren. Man müsste für jedes dieser anonymen Netzwerke eine eigene Strategie entwerfen, um sie „abschalten" zu können. Anonyme

[5] Hierzu ausführlich *Bartl/Moßbrucker/Rückert* (2019) [2], Angriff auf die Anonymität im Internet, S. 18–19.

[6] Vgl. *Fünfsinn/Ungefuk/Krause* (2017) [11], Kriminalistik 2017, 440 (442).

Netzwerke sind jedoch gerade darauf ausgerichtet, zensurresistent zu sein und werden aus diesem Grund dezentral betrieben. Die technische Infrastruktur von Tor basiert beispielsweise auf über 6.500 verschiedenen Tor-Knoten, die über die ganze Welt verteilt sind.[7] Ein Verbot von Darknet-Technologien könnte in der Praxis daher nur umgesetzt werden, indem versucht wird, den Zugriff auf die betreffenden Netzwerke zu blockieren.[8] Hinzu kommt, dass ein Verbot von Anonymisierungstechnologien auch aus rechtlicher Perspektive abzulehnen wäre. Dass das Darknet in freiheitlich-demokratischen Rechtsordnungen „keinen legitimen Nutzen" haben kann,[9] ist in Anbetracht des grundrechtlichen Schutzes von anonymer Internetkommunikation entschieden zurückzuweisen. Es ist gerade als Privileg freiheitlich-demokratischer Gesellschaften anzusehen, dass Menschen fernab von staatlicher Überwachung im Internet miteinander kommunizieren können.[10] Das Spannungsfeld zwischen der staatlichen Verpflichtung, strafbare Aktivitäten im Tor-Netzwerk effektiv zu verfolgen und dem Recht darauf, sich im Internet durch den Einsatz von Darknet-Technologien anonym zu bewegen, kann daher nicht einseitig durch ein Verbot von Anonymisierungsdiensten gelöst werden.

2 Technische Möglichkeiten der Strafverfolgung im Tor-Netzwerk und deren rechtliche Bewertung

Da ein Verbot von Darknet-Technologien sowohl aus technischer, als auch aus rechtlicher Perspektive abzulehnen ist, wendet sich dieser Beitrag den Möglichkeiten einer effektiven Strafverfolgung im Tor-Netzwerk zu. Zu diesem Zweck werden

[7] Vgl. Tor Metrics, Number of relays, abrufbar unter https://metrics.torproject.org/networksize.html (letzter Zugriff: 28.09.2020).

[8] Im Falle von Tor wäre es zwar möglich, die IP-Adressen der öffentlich gelisteten Tor-Knoten zu blockieren, allerdings bietet die Software genau aus diesem Grund sogenannte „Bridge-Knoten" an, die in diesen Konstellationen als nicht-öffentliche Einstiegspunkte in das Netzwerk genutzt werden können. Diese können außerdem mit sogenannten „Pluggable Transports" kombiniert werden, um sich mit dem Tor-Netzwerk verbinden zu können, ohne dass die Nutzung der Software für Dritte – beispielsweise staatliche Stellen – überhaupt erkennbar ist.

[9] So etwa der parlamentarische Staatssekretär beim Bundesinnenministerium Günter Krings (CDU); zitiert nach *Borchers* (2019) [5], Europäischer Polizeikongress: Weg mit dem Darknet, Heise Online (20.02.2019), abrufbar unter https://www.heise.de/newsticker/meldung/Europaeischer-Polizeikongress-Weg-mit-dem-Darknet-4313276.html (letzter Zugriff: 06.09.2019).

[10] Ausführungen zur Bedeutung von Anonymität in liberalen Verfassungsstaaten finden sich bei *Kersten* (2017) [15], JuS 2017, 193–203.

Ermittlungsansätze vorgestellt, die aus technischer Sicht zur Identifizierung tatverdächtiger Personen beitragen können. Da strafrechtliche Ermittlungen dem Prinzip vom Vorbehalt des Gesetzes genügen müssen, werden diese Ansätze sodann aus rechtswissenschaftlicher Perspektive bewertet und hinterfragt, ob sie von den derzeit existierenden Ermittlungsbefugnissen der Strafverfolgungsbehörden gedeckt wären. Ziel ist es, eine Diskussionsgrundlage für mögliche Vorgehensweisen bei der Strafverfolgung im Tor-Netzwerk zu schaffen, ohne die Legitimität einer anonymen Nutzung des Internets grundsätzlich in Frage zu stellen.

2.1 Betrieb von Honeypot-Servern

Eine Möglichkeit zur Identifizierung von tatverdächtigen Personen im Tor-Netzwerk ist in dem Aufsetzen und Betreiben von Honeypot-Servern zu sehen. Ein Honeypot ist eine gefälschte Computerressource, mit deren Hilfe Angreifer*innen angelockt werden sollen. Da Honeypot-Server durchgängig überwacht werden können, kommen sie häufig zum Einsatz, um Informationen über Angriffsmuster einzuholen.[11]

2.1.1 Technische Beschreibung

Über einen Honeypot-Server könnten Ermittlungsbehörden einen gefälschten Darknet-Marktplatz aufsetzen, über den zum Schein Drogen oder Waffen angeboten werden. Dadurch wären sie in der Lage, zu beobachten, welche Plattform-Mitglieder sich für welche illegalen Produkte interessieren, welche Versandart ausgewählt wird und welche Kontakt- beziehungsweise Lieferadressen auf den Webseiten angegeben werden. Diese Informationen könnten sodann als Anknüpfungspunkte für weitergehende strafrechtliche Ermittlungen herangezogen werden. Allerdings können sich Handelsplattformen im Tor-Netzwerk nur etablieren, wenn tatsächlich inkriminierte Güter über die in Rede stehenden Webseiten gehandelt werden. Plattformen, über die nur zum Schein illegale Waren angeboten werden, würden in der Praxis daher schnell als „Fake-Marktplätze“ enttarnt werden. Möglich wäre es jedoch, echte Plattformen von zuvor bereits ermittelten Tatverdächtigen zu übernehmen und zum Zwecke der Strafverfolgung über Honeypot-Server weiterzubetreiben, wie es etwa bei der Übernahme des Online-Marktplatzes „Hansa Market“ durch niederländische Ermittler*innen der Fall war.[12] Bis zur Abschaltung der Webseite ließen die

[11] Siehe hierzu *Moore* (2016) [10], Detecting ransomware with honeypot techniques.

[12] Vgl. *Europol* (2017) [10], Massive blow to criminal Dark Web activities after globally coordinated operation, abrufbar unter https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation (letzter Zugriff: 24.01.2020).

Behörden sämtliche über „Hansa Market“ angebahnte Handelsgeschäfte weiterlaufen, wodurch tausende Informationen über ausländische Plattform-Kund*innen gesammelt und an Europol übergeben werden konnten.[13]

2.1.2 Rechtliche Einordnung

Hierzulande wäre eine Übernahme von echten Darknet-Plattformen wie „Hansa Market“ und deren Weiterführung über behördliche Honeypot-Server rechtlich allerdings nicht möglich. Durch den Betrieb von Online-Plattformen, auf denen tatsächlich ein Austausch krimineller Waren stattfindet, werden nämlich verschiedene Straftatbestände aus dem Kern- und Nebenstrafrecht verwirklicht.[14] Wer Drogen-Marktplätze und andere kriminell ausgerichtete Online-Plattformen im Tor-Netzwerk betreibt, macht sich folglich strafbar. Hierzulande sind Ermittlungsbeamt*innen jedoch grundsätzlich nicht berechtigt, zum Zwecke der Strafverfolgung selbst Straftaten zu begehen. Zwar kennt auch die deutsche Rechtsordnung gesetzliche Ausnahmeregelungen von diesem Grundsatz. Für das Betreiben von Online-Plattformen im Tor-Netzwerk ist dies jedoch nicht der Fall. In den Niederlanden, USA und Australien sind solche Ermittlungshandlungen hingegen zulässig. Dass ein Weiterbetrieb krimineller Plattformen über Honeypot-Server jedoch auch im Ausland erhebliche rechtliche Schwierigkeiten mit sich bringt, hat der Fall der Kinderporno-Tauschbörse „Childsplay“ deutlich gemacht. Die Webseite wurde für ganze elf Monate nach der Verhaftung des Plattform-Administrators von australischen Ermittlungsbehörden weiterbetrieben.[15] Da in dieser Zeit kinderpornografische Dateien von den Plattform-Mitgliedern weltweit verbreitet und ausgetauscht werden konnten, wurde das Vorgehen der Ermittler*innen vom Kinderhilfswerk der Vereinten Nationen als ein Verstoß gegen die UN-Kinderrechtskonvention gewertet.[16] Auch Vertreter*innen von Amnesty International verurteilten das Vorgehen der australischen Ermittler*innen als menschenrechtswidrig und inakzepta-

[13] Vgl. *Böhm* (2017) [4], Ermittler zerschlagen zwei der größten Darknet-Marktplätze, Spiegel Online vom 20.07.2017, abrufbar unter https://www.spiegel.de/netzwelt/netzpolitik/darknet-ermittler-zerschlagen-grosse-marktplaetze-alphabay-und-hansa-a-1158933.html (letzter Zugriff 29.09.2020).

[14] Hierzu ausführlich *Greco* (2019) [12], ZIS 2019, 435–450; *Safferling/Rückert* (2018) [27], Analysen & Argumente 291 (2018), S. 1–15; *Ceffinato* (2017) [7], JuS 2017, 403–408; *Bachmann/Nergiz* (2019) [1], NZWiSt 2019, 241–248.

[15] Vgl. *Schulz* (2017) [28], Australiens Polizei betrieb riesige Kinderporno-Plattform, Spiegel Online vom 11. 10. 2017, abrufbar unter http://www.spiegel.de/panorama/justiz/australien-polizei-ermitteltemit-eigener-kinderporno-plattform-a-1172503.html (letzter Zugriff: 15.09.2020).

[16] Vgl. *Knoph Vigsnæs* et al. (2017) [16], VG vom 9.10.2017, UNICEF: Clear violation of UN children’s convention. International humanitarian organizations express strong reaction to

bel.[17] In Deutschland wäre eine Übernahme und Weiterführung von kriminellen Online-Marktplätzen und Kinderporno-Tauschbörsen über Honeypot-Server jedenfalls unzulässig.

2.2 Betrieb von Phishing-Webseiten

Eine Alternative zum Aufsetzen und Betreiben von Honeypot-Servern könnte das Abgreifen von Login-Informationen über sogenannte Phishing-Webseiten darstellen. Beim Phishing werden sensible persönliche Daten ausgespäht, indem sich ein*e Angreifer*in als vertrauenswürdige*r Dritte*r ausgibt[18] und eine gefälschte Webseite aufsetzt. Werden auf dieser Webseite Login-Informationen wie Account-Namen und Passwörter eingegeben, können die Betreiber*innen der Phishing-Webseiten die Daten ausspähen und selbst verwenden.

2.2.1 Technische Beschreibung

Ermittlungsbehörden könnten die Webseiten bekannter Darknet-Plattformen fälschen und die Kund*innen dieser Plattformen auf die manipulierten Phishing-Webseiten locken. Sollten sie dort ihre Login-Informationen eingeben, würden diese nicht an den Darknet-Dienst geschickt, sondern direkt an die Ermittler*innen weitergeleitet werden. Mit den ausgespähten Login-Informationen könnten sich diese sodann auf den echten kriminellen Plattformen und Marktplätzen anmelden und auf die Accounts der Plattform-Kund*innen zugreifen. Dadurch könnten die Ermittler*innen an beweiserhebliche Informationen gelangen, wie zum Beispiel in der Vergangenheit getätigte Käufe und Verkäufe, Lieferadressen oder Bitcoin-Wallets der Plattfom-Kund*innen.

2.2.2 Rechtliche Einordnung

Aus rechtlicher Perspektive ermächtigt die Online-Durchsuchung i. S. v. § 100b StPO Ermittlungsbehörden zwar unter besonderen Voraussetzungen dazu, in informationstechnische Systeme tatverdächtiger Personen einzugreifen, um an deren

---

Australia's undercover police operation, abrufbar unter https://www.vg.no/nyheter/utenriks/i/L8ly4/unicef-clear-violation-of-un-childrens-convention (letzter Zugriff 15.09.2020).

[17] Vgl. *Knoph Vigsnæs* et al. (2017) [16], VG vom 9.10.2017, UNICEF: Clear violation of UN children's convention. International humanitarian organizations express strong reaction to Australia's undercover police operation, abrufbar unter https://www.vg.no/nyheter/utenriks/i/L8ly4/unicef-clear-violation-of-un-childrens-convention (letzter Zugriff 15.09.2020).

[18] Hierzu ausführlicher *Jagatic/Johnson/Jakobsson/Menczer* (2007) [13], Social phishing, in: Communications of the ACM 50(10) (2007), S. 64–100.

Zugangsdaten und Passwörter zu gelangen.[19] Beim Aufsetzen von Phishing-Webseiten wird jedoch nicht mithilfe von forensischer Software in ein informationstechnisches System i. S. v. § 100b Abs. 1 StPO *eingegriffen.* Vielmehr würden die Betroffenen durch eine technische Manipulation dazu gebracht werden, ihre Login-Informationen täuschungsbedingt an die ermittelnden Behörden weiterzuleiten. Für das Betreiben von Phishing-Webseiten kann § 100b Abs. 1 StPO daher nicht als Ermächtigungsgrundlage herangezogen werden. Ebenso wenig könnte das Abgreifen von Zugangsdaten und Passwörtern auf § 100 h Abs. 1 S. 1 Nr. 2 StPO gestützt werden, welcher die Verwendung technischer Mittel zu Observationszwecken regelt. Denn der Betrieb der beschriebenen Phishing-Webseiten würde gerade nicht der Lokalisierung oder Beobachtung der ausgespähten Personen dienen, sondern lediglich das Abgreifen ihrer Login-Informationen bezwecken, um diese im Anschluss für weitergehende Ermittlungen auf den Plattformen zu verwenden. Auch ein Rückgriff auf die Ermittlungsgeneralklausel aus §§ 161 Abs. 1 S. 2 i. V. m. 163 Abs. 1 S. 2 StPO könnte die ermittelnden Beamt*innen nicht pauschal zum Aufsetzen und Betreiben von Phishing-Webseiten ermächtigen. Ein solches Vorgehen würde in vielen Fällen auch Personen betreffen, gegen die kein Anfangsverdacht i. S. v. § 152 Abs. 2 StPO besteht. Wie etwa die 2016 vom Netz genommene Webseite „Deutschland im DeepWeb“ deutlich macht, werden einige der Webseiten, über die im Tor-Netzwerk Straftaten angebahnt und abgewickelt werden, nämlich auch als Treffpunkte für den anonymen Austausch über Nachrichten aus Politik und Wirtschaft, IT-Sicherheit und andere strafrechtlich irrelevante Themen genutzt.[20] Die Registrierung als Nutzer*in auf einer solchen Webseite ist daher allein nicht ausreichend, um einen Anfangsverdacht i. S. v. § 152 Abs. 2 StPO gegen sämtliche auf einer Plattform registrierten Personen zu begründen. Das pauschale Abgreifen von Login-Informationen über Phishing-Webseiten wäre nach geltender Rechtslage daher unzulässig.

2.3 Automatisierte Auswertung öffentlich zugänglichen Informationsquellen (Open Source Intelligence)

Neben dem Betrieb behördlicher Honeypot-Server und Phishing-Webseiten stellt die automatisierte Auswertung öffentlich zugänglicher Informationsquellen einen

[19] *Soiné* (2018) [32], NStZ 2018, 497 (502).

[20] Siehe hierzu auch die Ausführungen des LG Karlsruhe, Urteil vom 19.12.2018, 4 KLs 608 Js 19.580/17, Rn. 431 = StV 2019, 400 (402).

weiteren technischen Ermittlungsansatz dar, der zur Identifizierung tatverdächtiger Personen im Tor-Netzwerk beitragen könnte.

2.3.1 Technische Beschreibung

Zur Identifizierung von tatverdächtigen Personen im Tor-Netzwerk kann es zielführend sein, Informationen wie verwendete Account-Namen, E-Mail-Adressen oder öffentliche Forenbeiträge zusammenzutragen und diese Datensätze mit Hilfe spezieller Analysesoftware auszuwerten.[21] Im Rahmen dieses Verfahrens, das als Open Source Intelligence (kurz OSINT) bezeichnet wird, werden sämtliche Informations- und Datenquellen verwendet, die im Internet – also sowohl im Clear- als auch im Darknet – frei zugänglich sind und für deren Zugriff keine besondere Legitimation benötigt wird.[22] Auf diese Weise können detaillierte Bewegungs- und Persönlichkeitsprofile über gesuchte Personen erstellt werden, die Ansatzpunkte für weitergehende Ermittlungsmaßnahmen bieten. Unter Umständen lassen sich sogar eindeutige Verknüpfungen zwischen den verwendeten Online-Profilen und der tatsächlichen Identität der gesuchten Personen herstellen, wie es etwa im Falle des Betreibers der Handelsplattform „Silk Road" der Fall war.[23]

2.3.2 Rechtliche Einordnung

In welchen Grenzen hierzulande personenbezogene oder personenbeziehbare Daten aus dem Clear- und Darknet in strafprozessualen Ermittlungsverfahren erhoben und verarbeitet werden dürfen, ist eine in der strafrechtlichen Praxis relevante, rechtswissenschaftlich jedoch bislang nur spärlich diskutierte Frage.[24] Feststeht, dass für die automatisierte Sammlung und Auswertung von OSINT-Daten eine Ermächtigungsgrundlage erforderlich ist, da hierdurch in das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG eingegriffen wird. Auch wenn dies auf den ersten Blick nahe liegt, kommt § 98a StPO (Rasterfahndung) als strafprozessuale Befugnisnorm für die Sammlung und Auswertung von OSINT-Daten allerdings nicht in Betracht.[25] Zwar ergibt sich eine gewisse „Verwandtschaft" zu § 98a StPO vor allem daraus, dass im Rahmen beider Verfahren

[21] Siehe hierzu bereits *Sinn* (2019) [30], Ermittlungen im Darknet, S. 148.

[22] Siehe hierzu *Day/Gibson/Ramwell* (2016) [8], Fusion of OSINT and non-OSINT data, in: Open Source Intelligence Investigation 2016, S. 133–152.

[23] Zu den Ermittlungen des FBI im Falle von „Silk Road" siehe *Tanriverdi* (2013) [26], Drogenhandel, Mordversuch – und den Klarnamen angegeben, Süddeutsche Zeitung vom 4.10.2013, abrufbar unter https://www.sueddeutsche.de/digital/mutmasslicher-betreiber-der-drogen-plattform-silk-road-drogenhandel-mordversuch-und-den-klarnamen-angegeben-1.1786870 (letzter Zugriff: 08.10.2020).

[24] Siehe hierzu *Rückert* (2017) [25], ZStW 2017, 302–333.

[25] *Rückert* (2017) [25], ZStW 2017, 302 (316).

verschiedene Datensätze zu Ermittlungszwecken maschinell miteinander abgeglichen werden.[26] Allerdings werden im Rahmen von § 98a StPO keine öffentlich zugänglichen Datensätze verwendet, während bei der Auswertung von OSINT-Daten ausschließlich auf Informationen zugegriffen wird, die von jedermann im Internet aufgerufen und eingesehen werden können. Obwohl auf die Ermittlungsgeneralklausel aus §§ 161 Abs. 1 S. 2 i. V. m. 163 Abs. 1 S. 2 StPO bloß geringfügige Grundrechtseingriffe gestützt werden können, ist diese daher grundsätzlich als Rechtsgrundlage für die automatisierte Auswertung von OSINT-Informationen in Betracht zu ziehen. Erwähnenswert ist in diesem Zusammenhang beispielsweise die von der niederländischen Forschungseinrichtung TNO entwickelte Analysesoftware „Dark Web Monitor", die seit Juli diesen Jahres durch die Zentralstelle Cybercrime Bayern (ZCB) in Bamberg getestet wird.[27]

2.4 Ausnutzen von Dokument-Exploits

Eine weitere Möglichkeit, um Personen im Tor-Netzwerk zu identifizieren, stellt das Ausnutzen von Dokument-Exploits dar. Lässt sich beispielsweise eine Datei im Microsoft-Word-Format mit einem unsichtbar eingebetteten Link präparieren, der beim Öffnen des Dokuments ohne Rückfrage an die betrachtende Person aufgerufen wird, so kann dieses Dokument als Angriffswerkzeug zur Deanonymisierung von Tor-Nutzer*innen eingesetzt werden.

2.4.1 Technischer Hintergrund

Im Rahmen strafrechtlicher Ermittlungsverfahren ist das Ausnutzen solcher Dokument-Exploits als „IP-Tracking" bekannt. Dabei stellen Ermittlungsbehörden Dateien über das Internet zum Abruf bereit, die mit einer Lesebestätigungsfunktion versehen sind.[28] Diese Lesebestätigungsfunktion besteht aus funktionslosen, transparenten Bildern oder anderen Dateieinbettungen.[29] Wird das präparierte Dokument geöffnet, werden die Dateieinbettungen von einem externen Server nachgeladen, ohne dass der dabei anfallende Datenverkehr von der Tor-Software anonymisiert wird. Die IP-Adresse des Internetanschlusses, von dem aus die Datei aufgerufen

[26] *Rückert* (2017) [25], ZStW 2017, 302 (316).

[27] Vgl. *Bayerisches Staatsministerium der Justiz,* Pressemitteilung vom 27.07.2020, Mehr Licht ins Darknet: Dark Web Monitor soll Strafverfolgungsbehörden bei Ermittlungen im Darknet verstärken, abrufbar unter https://www.justiz.bayern.de/presse-und-medien/pressemitteilungen/archiv/2020/69.php? (letzter Zugriff: 08.10.2020).

[28] Vgl. *Krause* (2016) [17], NStZ 2016, 139.

[29] Vgl. *Krause* (2016) [17], NStZ 2016, 139.

wurde, kann daher an den externen Server übertragen und schließlich an die Ermittlungsbehörden weitergeleitet werden. Typischerweise eignen sich für derartige Einbettungen Dokumentenformate wie Word oder PDF eher als reine Multimediaformate für Bild und Video wie JPG oder MP4. Aber auch für Multimediaformate beziehungsweise für Software, die zur Verarbeitung und Betrachtung von Bildern und Videos eingesetzt wird, sind in der Vergangenheit Schwachstellen bekannt geworden, die theoretisch zu Deanonymisierungszwecken ausgenutzt werden könnten.

2.4.2 Rechtliche Betrachtung

Aus rechtlicher Perspektive besteht Uneinigkeit darüber, ob das „IP-Tracking" zum Zwecke der Strafverfolgung als Verwendung eines sonstigen für Observationszwecke bestimmten technischen Mittels i. S. v. §100 h StPO[30] oder als Erhebung von Verkehrsdaten i. S. v. §100 g StPO[31] anzusehen ist. Dennoch bleibt festzuhalten, dass für ein entsprechendes Vorgehen bereits nach geltender Rechtslage eine ausreichende rechtliche Grundlage besteht, die in der Strafverfolgungspraxis vielseitige Ermittlungsansätze bietet. Beispielsweise hat der Bundestag im Januar 2020 der Verwendung künstlicher kinderpornografischer Dateien im Rahmen strafrechtlicher Ermittlungsverfahren zugestimmt.[32] Seither können Ermittlungsbeamt*innen computergenerierte Abbildungen verwenden, um sich Zugriff auf entsprechend gesicherte Webseiten im Tor-Netzwerk zu verschaffen.[33] Denkbar wäre es, diese computergenerierten Abbildungen mit entsprechenden Dokument-Exploits zu versehen, sodass die IP-Adressen derjenigen Personen, die auf die von den Ermittlungsbehörden hochgeladenen Dateien zugreifen, dokumentiert und als Anknüpfungspunkte für weitere Ermittlungsmaßnahmen genutzt werden können.

[30] So etwa *Krause* (2016) [17], NStZ 2016, 139 (144); *Bär* (2020) in: BeckOK-StPO [17], §100 g, Rn. 22; *Bruns* (2019) in: KK-StPO [14], §100 g, Rn. 20.

[31] So etwa der BGH-Ermittlungsrichter mit Beschl. v. 23.9.2014 - 1 BGs 210/14 = BeckRS 2015, 17557 (allerdings auf der Grundlage von §100 g aF.).

[32] Ausführlich zu den Neuregelungen der §184b Abs. 5 S. 2 StGB und §110d StPO siehe *Rückert/Goger* (2020) [23], MMR 2020, 373–378.

[33] Zum Phänomen der sogenannten „Keuschheitsproben" auf Online-Plattformen im Tor-Netzwerk siehe *Wittmer/Steinebach* (2019) [33], MMR 2019, 650–653.

2.5 Quellen-Telekommunikationsüberwachung und Online-Durchsuchung

Zudem kann eine Anonymisierung von Kommunikationsdaten im Tor-Netzwerk dadurch umgangen werden, dass die betreffenden Daten abgefangen werden, bevor sie verschlüsselt oder nachdem sie entschlüsselt wurden.

2.5.1 Technischer Hintergrund

Über das Tor-Netzwerk geroutete Datenpakete werden so verschlüsselt, dass jeder Tor-Knoten nur die Information erhält, von welchem Tor-Knoten die aktuellen Datenpakete gesendet wurden und an welchen Tor-Knoten die Datenpakete weitergeleitet werden müssen. Auf diese Weise wird der über das Tor-Netzwerk geleitete Datenverkehr anonymisiert. Dieser Effekt kann jedoch umgangen werden, wenn die Datenpake abgefangen und ausgewertet werden, bevor sie verschlüsselt oder nachdem sie entschlüsselt wurden. Aus technischer Sicht kann dies erreicht werden, indem auf den Rechnern der zu überwachenden Personen eine forensische Software installiert wird, die unbemerkt Bildschirmaufnahmen tätigt oder Tastatureingaben protokolliert.

2.5.2 Rechtliche Bewertung

Aus rechtlicher Perspektive ist es denkbar, ein solches Vorgehen auf die im Sommer 2017 neu in die StPO aufgenommenen Ermittlungsbefugnisse der §§ 100a, b StPO zu stützen. § 100a Abs. 1 S. 2 StPO (Quellen-Telekommunikationsüberwachung) ermächtigt Ermittlungsbehörden etwa dazu, in informationstechnische Systeme verdächtiger Personen einzugreifen, wenn dies notwendig ist, um die Überwachung und Aufzeichnung von telekommunikationsbezogenen Daten in unverschlüsselter Form zu ermöglichen. Unter den Voraussetzungen des § 100b StPO (Online-Durchsuchung) dürfen die Ermittler*innen darüber hinaus auch sonstige, nicht kommunikationsbezogene Daten der Betroffenen erheben. Insofern kann eine Umgehung der Anonymisierung von Kommunikationsdaten im Tor-Netzwerk bereits auf Grundlage der geltenden strafprozessualen Ermittlungsbefugnisse erreicht werden. Um die genannten Ermittlungsmaßnahmen einzuleiten, müssen den Behörden allerdings bereits diejenigen Personen bekannt sein, deren Geräte überwacht werden sollen. Daher ist weder die Quellen-Telekommunikationsüberwachung aus § 100a StPO, noch die Online-Durchsuchung aus § 100b StPO dazu geeignet, zu einer initialen Identifizierung von tatverdächtigen Personen im Tor-Netzwerk beizutragen. Dennoch können Ermittlungsbehörden durch Maßnahmen i.S.d. §§ 100a, b StPO Informationen erhalten, die eine Identifizierung weiterer tatverdächtiger Personen ermöglichen.

2.6 Monitoring von Datenpaketen

Ein gänzlich anderer Ermittlungsansatz, der eine initiale Identifizierung von Tor-Nutzer*innen ermöglichen könnte, ist das Monitoring von Datenpaketen. Dabei werden versandte Datenpakete überwacht und nachvollzogen, wie diese Pakete über das Netzwerk weitergeleitet werden. Stehen ausreichend viele Tor-Knoten unter der Kontrolle ein und derselben – beispielsweise staatlichen – Stelle, können die versendeten Datenpakete sodann anhand statistischer Analysen korreliert und unter Umständen sowohl deren Versender*innen als auch Empfänger*innen ausfindig gemacht werden.

2.6.1 Technische Beschreibung

Diese Angriffe werden in der Informatik als Korrelationsangriffe oder „Timing-Analysen" bezeichnet und sind ein bekanntes Problem im Tor-Netzwerk.[34] Allerdings kann durch ein solches Vorgehen nur in Erfahrung gebracht werden, welche Personen über Tor miteinander kommunizieren. Wird von den Beteiligten eine Ende-zu-Ende-Verschlüsselung eingesetzt, bleiben die Kommunikationsinhalte selbst wiederum geheim. Hinzu kommt, dass nur eine global agierende, äußerst einflussreiche Institution im Stande wäre, ausreichend viele Tor-Knoten zu betreiben, um solche Korrelationsangriffe erfolgreich umsetzen zu können. Nach derzeitigem Stand ist dies allerdings nicht der Fall. Selbst geheimdienstliche Allianzen wie die „Five Eyes" wären nur in der Lage, einen kleinen, zufälligen Teil der über das Tor-Netzwerk gerouteten Datenpakete zu überwachen.[35] Die NSA äußerte sich in den von Edward Snowden geleakten „Tor-Stinks"-Dokumenten sogar dahingehend, dass es in der Praxis wohl niemals möglich sein wird, alle Tor-Nutzer*innen im Rahmen von „Timing-Analysen" gleichzeitig überwachen zu können.[36]

2.6.2 Rechtliche Einordnung

Auch aus rechtlicher Perspektive wäre das Monitoring von Datenpaketen zu Strafverfolgungszwecken als unzulässig einzustufen. Dies liegt daran, dass in einer globalen Überwachung und Rückverfolgung von Datenpaketen bereits keine strafprozessuale Maßnahme gesehen werden kann. Voraussetzung für die Einleitung eines strafrechtlichen Ermittlungsverfahrens ist gem. §152 Abs. 2 StPO nämlich das

[34] Siehe hierzu etwa *Platzer/Schäfer/Steinebach* (2020) [22]), Critical traffic analysis on the tor network, in: Proceedings of the 15th International Conference on Availability, Reliability and Security 2020, S. 1–10.

[35] Siehe hierzu *Nurmi/Niemelä* (2017) [21], Tor de-anonymisation techniques. In: International Conference on Network and System Security, S. 657–671.

[36] Vgl. „Tor-Stinks" -Präsentation der NSA, abrufbar unter https://edwardsnowden.com/docs/doc/tor-stinks-presentation.pdf (letzter Zugriff: 09.10.2020).

Vorliegen tatsächlicher Anhaltspunkte dafür, dass die von einer Ermittlungsmaßnahme betroffenen Personen eine verfolgbare Straftat begangen haben. In Anbetracht dessen, dass die Verwendung von Anonymisierungstechnologien wie der Tor-Software hierzulande ein grundrechtlich geschütztes Verhalten darstellt und zahlreichen positiven Verwendungszwecken dient, können die Nutzer*innen der Tor-Software jedoch nicht pauschal verdächtigt werden, das Tor-Netzwerk zur Anbahnung und Abwicklung von Straftaten zu nutzen.

2.7 Sonstige Ansätze

Neben den bisher aufgezeigten Ermittlungsmöglichkeiten existieren noch weitere Ansätze, die zur Identifizierung tatverdächtiger Personen im Tor-Netzwerk herangezogen werden können. Aus technischer Perspektive sind etwa Methoden des Forensic Hackings zu nennen. Hierunter ist eine Form des „ethical hackings“ zu verstehen, das eng verwandt mit Strategien wie dem Penetration Testing ist.[37] Analog zu bekannten Hackingangriffen werden dabei Systemschwachstellen wie Implementierungs- oder Protokollfehler ausgenutzt, was dazu führen kann, dass eine Anonymisierung von IP-Adressen im Tor-Netzwerk scheitert. Hinzu kommen zahlreiche Ermittlungsansätze, die über keinen technischen Hintergrund verfügen und in diesem Beitrag daher nicht erwähnt wurden. Hierzu zählt beispielsweise der Einsatz von verdeckt ermittelnden Beamt*innen, die auf den Plattformen und Foren Testkäufe von illegalen Waren tätigen oder versuchen, verdächtige Personen im Rahmen angeblicher An- und Verkaufsgespräche zum Umstieg auf nicht-anonyme Kommunikationsmittel zu bewegen.[38]

3 Zusammenfassung

Eine anonyme Nutzung des Internets wird durch die Verwendung sogenannter „Darknet-Technologien“ wie der Tor-Software ermöglicht und ist hierzulande grundrechtlich geschützt. Neben zahlreichen positiven Verwendungszwecken werden Anonymisierungstechnologien allerdings oft auch zur Begehung von Straftaten eingesetzt. Da ein Verbot von Darknet-Technologien jedoch sowohl aus technischer, als auch aus rechtlicher Sicht abzulehnen ist, wendet sich dieser Beitrag den Mög-

[37] Siehe hierzu *Simpson/Backman/Corley* (2020) [29], Hands-on ethical hacking and networkdefense.

[38] Siehe hierzu *Krause* (2018) [18], NJW 2018, 678–681.

lichkeiten der Strafverfolgung im Tor-Netzwerk zu. Es wurden Vorgehensweisen zur Identifizierung tatverdächtiger Personen im Tor-Netzwerk vorgestellt und aus rechtlicher Perspektive beurteilt, ob diese von den derzeit existierenden Ermittlungsbefugnissen der Strafverfolgungsbehörden gedeckt wären. Das Betreiben behördlicher Honeypot-Server und Phishing-Webseiten zur Überwachung von Darknet-Plattformen wurde dabei als technisch möglich, aber in Deutschland rechtlich unzulässig eingestuft. Das Monitoring von Datenpaketen zu Strafverfolgungszwecken wurde sowohl aus technischen, als auch aus rechtlichen Gründen abgelehnt. Im Gegensatz dazu wurde der Einsatz von OSINT-Technologien zu Ermittlungszwecken als technisch möglich und rechtlich zulässig angesehen. Gleiches gilt hinsichtlich der Standortermittlung von verdächtigen Personen mittels „IP-Tracking". Zudem kann eine Verschleierung von IP-Adressen auch durch Ermittlungshandlungen wie der Quellen-Telekommunikationsüberwachung umgangen werden. Obwohl die Verwendung der Tor-Software strafrechtliche Ermittlungen erheblich erschwert, konnte gezeigt werden, dass technische Ermittlungsansätze existieren, die zur Deanonymisierung von tatverdächtigen Personen im Tor-Netzwerk herangezogen werden können. Die aufgezeigten Vorgehensweisen sollen als Diskussionsgrundlage für zukünftige Ermittlungshandlungen im Tor-Netzwerk dienen, ohne jedoch die Legitimität einer anonymen Nutzung des Internets grundsätzlich in Frage zu stellen.

Danksagung Das dieser Veröffentlichung zugrundeliegende Verbundprojekt „Parallelstrukturen, Aktivitätsformen und Nutzerverhalten im Darknet" (PANDA) wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter den Förderkennzeichen 13N14355 und 13N14356 gefördert. Die Verantwortung für den Inhalt dieses Beitrags liegt bei den Autor*innen.

Literatur

1. Bachmann, M., Arslan, N.: „Darknet"-Handelsplätze für kriminelle Waren und Dienstleistungen: Ein Fall für den Strafgesetzgeber? S. 241–248. NZWiSt (2019)
2. Moritz, B., Moßbrucker, D., Rückert, C.,: Angriff auf die Anonymität im Internet, Reporter ohne Grenzen e.V., Berlin 2019. https://www.reporter-ohne-grenzen.de/uploads/tx_lfnews/media/20190630_Darknet_Paragraf_StN-Bartl-Mossbrucker-Rueckert.pdf. Zugegriffen: 31. Juli 2020
3. Graf, P. (Hrsg.): Beck'scher Online-Kommentar zur StPO mit RiStBV und MiStra, 37. Aufl. 1.7.2020 (zitiert: *Bearbeiter*in* in: BeckOK-StPO). Verlag C.H. Beck, München 2020
4. Böhm, M.: Ermittler zerschlagen zwei der größten Darknet-Marktplätze, Spiegel. https://www.spiegel.de/netzwelt/netzpolitik/darknet-ermittler-zerschlagen-grosse-marktplaetze-alphabay-und-hansa-a-1158933.html. Zugegriffen: 20. Juli 2017

5. Borchers, D.: Europäischer Polizeikongress: Weg mit dem Darknet, Heise. https://www.heise.de/newsticker/meldung/Europaeischer-Polizeikongress-Weg-mit-dem-Darknet-4313276.html. Zugegriffen: 20. Febr. 2019
6. Bovermann, P.: Framing-Check: „Darknet", Süddeutsche Zeitung. www.sueddeutsche.de/kultur/framing-darknet-tor-anonym-internet-silk-road-1.436701. Zugegriffen: 3. Mai 2019
7. Ceffinato, T.: Die strafrechtliche Verantwortlichkeit von Internetplattformbetreibern. JuS 403–408 (2017)
8. Day, T., Gibson, H., Ramwell, S.: Fusion of OSINT and non-OSINT data. In: Open Source Intelligence Investigation , S. 133–152. Springer International Publishing, Basel (2016)
9. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The Second-Generation Onion Router. Naval Research Lab, Washington DC (2004)
10. Europol: Pressemitteilung vom 20.07.2017, Massive blow to criminal Dark Web activities after globally coordinated operation. https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation. Zugegriffen: 20. Juli 2017
11. Fünfsinn, H., Ungefuk, G., Krause, B.: Das Darknet aus Sicht der Strafverfolgungsbehörden. Kriminalistik **7**, 440–445 (2017)
12. Greco, L.: Strafbarkeit des Unterhaltens einer Handels- und Diskussionsplattform insbesondere im sog. Darknet ZIS 2019, 434–450 (2019)
13. Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F.: Social phishing. Communications of the ACM 50(10), 64–100 (2007)
14. Hannich, R. (Hrsg.): Karlsruher Kommentar zur StPO, 8. Aufl. (zitiert: *Bearbeiter*in* in: KK-StPO). C. H. Beck, München (2019)
15. Kersten, J.: Anonymität in der liberalen Demokratie. JuS 193–203 (2017)
16. Knoph Vigsnæs, M., Høydal, H.F., Einar, O.S., Remøe Hansen, N.: VG , UNICEF: Clear violation of UN children's convention. International humanitarian organizations express strong reaction to Australia's undercover police operation, abrufbar unter. https://www.vg.no/nyheter/utenriks/i/L8ly4/unicef-clear-violation-of-un-childrens-convention. Zugegriffen: 9. Okt. 2017
17. Krause, B.: IP-Tracking durch Ermittlungsbehörden: Ein Fall für §100g StPO?–Zugleich Besprechung des BGH-Beschl. v. 23. Sept. 2014–1 BGs 210/14, S. 139–144, NStZ (2016)
18. Krause, B.: Ermittlungen im Darknet – Mythos und Realität. NJW 678–681. C. H. Beck, München (2018)
19. Locker, T., Hoppenstedt, M.: Jagd auf 'Elysium': Das Ende der größten deutschen Kinderporno-Plattform, VICE. https://www.vice.com/de/article/panv87/jagd-auf-elysium-das-ende-der-grossten-deutschen-kinderporno-plattform Zugegriffen: 7 März 2019
20. Moore, C.: Detecting ransomware with honeypot techniques. In: Cybersecurity and Cyberforensics Conference (CCC), S. 77–81, IEEE (2016)
21. Nurmi, J., Niemelä, M.S.: Tor de-anonymisation techniques. In: International Conference on Network and System Security, S. 657–671. Springer International. Basel (2017)
22. Platzer, F., Schäfer, M., Steinebach, M.: Critical traffic analysis on the tor network. In: Proceedings of the 15th International Conference on Availability, Reliability and Security, S. 1–10 (2020)

23. Rückert, C., Goger, T.: Neue Waffe im Kampf gegen Kinderpornografie im Darknet. MMR 373–378 (2020)
24. Rückert, C.: Blick in eine Schattenwelt. Schaden und Nutzen des „anonymen" Internets, Politische Studien 479/2018, S. 12–21, abrufbar unter https://www.hss.de/download/publications/PS_479_Digitale_Revolution_03.pdf
25. Rückert, C.: Zwischen Online-Streife und Online-(Raster-)Fahndung – Ein Beitrag zur Verarbeitung öffentlich zugänglicher Daten im Ermittlungsverfahren, S. 302–333, ZStW (2017)
26. Tanriverdi, H.: Drogenhandel, Mordversuch–und den Klarnamen angegeben, Süddeutsche Zeitung, abrufbar unter www.sueddeutsche.de/digital/mutmasslicher-betreiber-der-drogen-plattform-silk-road-drogenhandel-mordversuch-und-den-klarnamen-angegeben-1.1786870. Zugegriffen: 4. Okt. 2013
27. Safferling, C., Rückert, C.: Das Strafrecht und die Underground Economy. In: Konrad-Adenauer-Stiftung e.V. (Hrsg.), Analysen & Argumente, Ausgabe 291, abrufbar unter https://www.kas.de/documents/252038/253252/7_dokument_dok_pdf_51506_1.pdf/5f5a7ec0-2bb8-6100-6d65-b3ba55564d72?version=1.0&t=1539647924448. Zugegriffen: Febr. 2018
28. Schulz, B.: Australiens Polizei betrieb riesige Kinderporno-Plattform, Spiegel, abrufbar unter http://www.spiegel.de/panorama/justiz/australien-polizei-ermitteltemit-eigener-kinderporno-plattform-a-1172503.html. Zugegriffen: 11. Okt. 2017
29. Simpson, M.T., Backman, K., Corley, J.: Hands-on Ethical Hacking and Network Defense. Cengage Learning. Course Technology, Boston, MA (2010)
30. Sinn, A.: Ermittlungen im Darknet. In: Gest, G.M., Sinn, A. (Hrsg.) Organisierte Kriminalität und Terrorismus im Rechtsvergleich, Schriften des Zentrums für europäische und internationale Strafrechtsstudien, Bd. 10, S. 141–159. V&R Unipress, Universitätsverlag Osnabrück (2019)
31. Snowden, E.: „Tor Stinks"-Präsentation der National Security Agency of the United States of America. https://edwardsnowden.com/docs/doc/tor-stinks-presentation.pdf
32. Soiné, M.: Die strafprozessuale Online-Durchsuchung. NStZ 497–504 (2018)
33. Wittmer, S., Steinebach, M.: Computergenerierte Kinderpornografie zu Ermittlungszwecken im Darknet. Rechtliche Rahmenbedingungen und technische Umsetzbarkeit, MMR 650–653 (2019)

Anonymisierte Daten brauchen keinen Datenschutz – wirklich nicht?

Ralf Kneuper

Zusammenfassung

Gesetzliche Regelungen zum Datenschutz wie die DSGVO gehen davon aus, dass ein Schutzbedarf nur für personenbezogene Daten gilt, und anonymisierte Daten damit nicht dem Datenschutz unterliegen. Anonymität ist aber eine relative Eigenschaft, die u. a. vom Dateneigentümer abhängt. Daher kann sie auch in vielen Fällen wieder aufgehoben werden, wie einige in den letzten Jahren bekannt gewordene Beispiele zeigen. Die derzeitige Beschränkung des Datenschutzes auf personenbezogene Daten erscheint daher nicht angemessen, und es gibt verschiedene Ansätze, diese Herausforderung anzugehen. Zuerst einmal könnten auch anonymisierte Daten in der Gesetzgebung zum Datenschutz als schützenswert definiert werden, woraus sich die Forderung nach entsprechenden Maßnahmen wie einer Beschränkung der Weitergabe oder der Durchführung einer Datenschutz-Folgenabschätzung ergibt. Ein anderer bisher allerdings wenig verbreiteter Ansatz ist das gesetzliche Verbot einer Re-Identifikation. Ein gravierender Nachteil der Anonymisierung ist, dass sie dazu führt, dass die Betroffenenrechte wie das Recht auf Auskunft oder auf Löschung nicht mehr umsetzbar sind. Das führt zum dritten möglichen Lösungsansatz, der die Anonymisierung als Maßnahme zum Datenschutz komplett ablehnt. Als Grundlage für eine Lösung dieser Herausforderungen wird ergänzend eine Definition von „im erweiterten Sinne personenbezogenen Daten“ eingeführt.

R. Kneuper (✉)
IU Internationale Hochschule – Fernstudium, Bad Reichenhall, Deutschland
E-mail: ralf.kneuper@iu.org

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_9

Schlüsselwörter

Anonymisierung • Re-Identifikation • Datenschutz • DSGVO.

1 Einführung und Hintergrund

Die Anonymisierung von personenbezogenen Daten führt, abgesehen von den technischen Herausforderungen, auch zu einer Reihe von komplexen rechtlichen Fragen im Rahmen des Datenschutzes. Dazu gehören u. a. die im Rahmen eines Konsultationsverfahrens des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) betrachteten Fragen nach der Notwendigkeit einer Rechtsgrundlage sowie ggf. nach einer angemessenen solchen Rechtsgrundlage (siehe [2]).

In diesem Beitrag soll dagegen die Frage betrachtet werden, inwiefern Datenschutz noch eine Rolle spielen sollte, *nachdem* Daten anonymisiert wurden. Die Betrachtung orientiert sich dabei an der DSGVO, aber die wesentlichen Aussagen lassen sich problemlos auch auf andere Regelwerke zum Datenschutz übertragen. Gemäß EG 26 DSGVO verstehen wir dabei unter anonymen Daten solche Daten, die nicht personenbezogen sind, sich also nicht auf eine identifizierte oder identifizierbare Person beziehen. Anonymisierte Daten sind Daten, die personenbezogen waren, bei denen dieser Personenbezug aber entfernt wurde, d. h. es handelt sich um einen speziellen Fall anonymer Daten.

Im Datenschutzrecht, insbesondere auch in der DSGVO, gibt es eine Reihe von Aussagen zum Umgang mit derartigen anonymisierten Daten, die jede für sich schlüssig sind, die in der Kombination aber Probleme verursachen. Einerseits wird bei der Beurteilung, ob bestimmte Daten anonym sind, keine absolute Anonymität gefordert, die also unter allen Umständen und Rahmenbedingungen gegeben wäre, sondern eine relative Anonymität, ausgehend von einer Bewertung der Wahrscheinlichkeit einer Re-Identifizierung auf Basis von Kosten, Zeitaufwand und verfügbarer Technologie (EG 26 Sätze 3, 4 DSGVO).[1] Andererseits handelt es sich bei Daten, die als (relativ) anonym bewertet wurden, definitionsgemäß nicht mehr um personenbezogene Daten, und sie unterliegen damit auch nicht mehr den Vorgaben des Datenschutzes (EG 26 Satz 5 DSGVO).

In der Praxis hängt die Wahrscheinlichkeit einer Re-Identifikation aber stark davon ab, wer Zugang zu den Daten hat und welche Methoden und Hilfsmittel hierfür eingesetzt werden, und die anzuwendenden Kriterien Kosten, Zeitaufwand und Technologie ändern sich mit der Zeit. Es gibt viele Beispiele, dass anonymi-

[1] Für eine ausführlichere Diskussion der Unterscheidung zwischen absoluter und relativer Anonymität siehe beispielsweise [1, 6].

sierte Daten wieder re-identifiziert werden konnten; bekannte Beispiele sind der in [17] beschriebene Fall einer Krankenversicherung in Massachusetts, sowie der in [8] beschriebene Fall von Netflix-Daten. Mit den wachsenden Möglichkeiten von Disziplinen wie Data Science, Big Data und künstlicher Intelligenz wächst auch die Wahrscheinlichkeit, dass eine solche Re-Identifizierung möglich wird.

Das führt zur folgenden Hypothese:

Hypothese 1 *Anonymität ist eine Eigenschaft nicht alleine der Daten, sondern der Kombination von Daten und Datenbesitzer.*

Die gleichen Daten, die bei einem Besitzer anonym sind, sind bei einem anderen Besitzer möglicherweise personenbezogen. Wenn man keine Einschränkungen in Bezug auf den Besitzer der Daten macht, ist sogar zweifelhaft, inwieweit es anonymisierte Daten überhaupt geben kann.[2]

Angedeutet ist diese Hypothese bereits in EG 26 Satz 3 DSGVO („Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, …"), aber danach wird die Abhängigkeit der Anonymität vom Datenbesitzer nicht weiter berücksichtigt.

Da anonymisierte Daten aber nicht dem Datenschutz unterliegen, gibt es nach einer Bewertung der Daten als anonym auch keine rechtlichen Einschränkungen mehr, die verhindern könnten, dass die Daten einem anderen Besitzer übermittelt werden, bei dem sie nicht anonym sind. Voraussetzung für diese Bewertung ist eine angemessene Risikoanalyse auf Basis von EG 26, die die Anonymität der Daten bestätigt, aber auch bei gründlicher Durchführung kann sich eine solche Analyse im Nachhinein als falsch erweisen.

Damit können anonymisierte Daten auch veröffentlicht werden und dadurch bei einem Unternehmen landen, das sie mit anderen Daten verketten kann und dadurch eine Re-Identifikation ermöglicht. Eventuell gilt das auch erst zu einem späteren Zeitpunkt mit den dann neuesten Methoden der Datenanalyse. Man kann daher davon ausgehen, dass eine Re-Identifizierung in vielen Fällen möglich sein wird, selbst wenn die ursprüngliche Bewertung der Daten als anonym unter den damaligen Rahmenbedingungen angemessen und damit rechtskonform war, vgl. [6]. Naturgemäß ist diese Wahrscheinlichkeit gerade bei den großen Datensammlern besonders

[2] So beginnt beispielsweise [1] mit der Aussage „Im Zeitalter von Big Data sind alle Daten personenbezogen. Analyse-Algorithmen machen jede Anonymisierung auf Dauer unmöglich."

hoch, bei denen sowieso schon sehr viele personenbezogene Daten vorliegen und bei denen der potentielle Schaden für die Betroffenen dadurch relativ hoch ist.

Gleichzeitig ist es aber für viele Zwecke wichtig, dass geeignete Daten für Auswertungen zur Verfügung stehen, wobei diese Daten häufig ursprünglich personenbezogen sind und teilweise sehr hohen Schutzbedarf haben, beispielsweise in der medizinischen Forschung. Eine wesentliche Beschränkung dieser Auswertungen würde die Forschung wie auch viele auf Open Data basierende Anwendungen unangemessen einschränken. Um aber die betroffenen Personen zu schützen, ist es wünschenswert und aus Sicht des Datenschutzrechtes auch gefordert, dass diese Daten vor der Nutzung anonymisiert werden, wann immer in der Auswertung auf den Personenbezug verzichtet werden kann.

Die beschriebenen Herausforderungen wurden bereits von Ohm 2010 in [10] diskutiert, sind aber auch heute in Regelwerken wie der DSGVO nicht berücksichtigt. Ziel dieses Beitrags ist es daher, den aktuellen Stand dieser Herausforderungen und möglicher Lösungsansätze zusammenzutragen, um eine neue Diskussion zum angemessenen Umgang mit anonymisierten Daten unterstützen.

Zum Aufbau dieses Beitrags: Abschn. 2 analysiert die genannten Herausforderungen ausführlicher. Die Konsequenzen und offenen Fragen, die sich daraus ergeben, werden in Abschn. 3 betrachtet. Mögliche Ansätze zur Lösung dieser Herausforderungen werden in Abschn. 4 vorgestellt, Abschn. 5 stellt die Definition von im erweiterten Sinn personenbezogenen Daten vor, und Abschn. 6 fasst schließlich die Ergebnisse zusammen.

2 Anonymisierung als Maßnahme zum Datenschutz

2.1 Gefahr der Re-Identifizierung

Aus den genannten Argumenten ergibt sich, dass ein vollständiger Verzicht auf Datenschutzanforderungen bei anonymisierten Daten zu kurz greift, da in diesem Fall kein Schutz gegen die Folgen einer Re-Identifizierung gegeben ist. Deutlich abweichend von der heute üblichen rechtlichen Bewertung folgt stattdessen:

Hypothese 2 *Auch für anonymisierte Daten kann aus Datenschutzsicht ein Schutz erforderlich sein.*

Auch wenn das selten so explizit formuliert wird, ist ein restriktiver Umgang mit anonymisierten Daten auch heute schon (gelegentlich) gelebte Praxis. So werden beispielsweise anonymisierte Gesundheitsdaten nur für Forschungsorganisationen

unter Einschränkungen (über die evtl. vorhandenen kommerziellen Einschränkungen hinaus) zur Verfügung gestellt, aber nicht veröffentlicht, obwohl das für garantiert anonyme Daten unproblematisch wäre. Ähnliches ist beispielsweise in [7, S. 5] für Daten zur Bildungsforschung zumindest als Empfehlung formuliert.

Um diese Forderung nach Schutz auch für anonymisierte Daten umzusetzen, sollte Anonymisierung als eine Maßnahme (von mehreren möglichen) zum Datenschutz verstanden werden. Diese Maßnahme trägt in vielen Fällen wesentlich zum Schutz der Daten und damit der Betroffenen bei, gewährleistet aber keinen vollständigen Schutz der Betroffenen. Allgemein hat Anonymisierung aus Datenschutzsicht zwei verschiedene Rollen, die beide parallel berücksichtigt werden müssen, siehe [5]: Einerseits handelt es sich um eine Form der Verarbeitung personenbezogener Daten und muss entsprechende Anforderungen gemäß DSGVO berücksichtigen. Andererseits handelt es sich um eine Maßnahme zum Datenschutz, die gerade selbst dazu beitragen kann, Anforderungen der DSGVO zu erfüllen.

Eine andere Sichtweise auf die Notwendigkeit eines Schutzes anonymisierter Daten ist, dass die im Datenschutzrecht verankerte binäre Unterteilung in anonyme bzw. anonymisierte Daten einerseits und personenbezogene Daten andererseits zu einfach ist oder, wie beispielsweise schon 2012 von der FTC in [4, S. 19] formuliert: „Overall, the comments reflect a general acknowledgment that the traditional distinction between PII and non-PII has blurred …“. Daten sind in vielen praktischen Fällen eben weder eindeutig personenbezogen noch eindeutig anonym, sondern liegen in einem Graubereich dazwischen, denn sie können mit einem mehr oder weniger großen Aufwand auf eine bestimmte Person bezogen werden. Die oben beschriebenen Aussagen aus EG 26 DSGVO zur relativen Anonymität zeigen, dass der Gesetzgeber sich dessen in gewissem Rahmen bewusst ist, eine strenge Trennung zwischen personenbezogenen und anonymen Daten im Gesetz aber trotzdem als in jedem Einzelfall gegeben postuliert.

Beim Risiko der Re-Identifizierung ist auch zu berücksichtigen, dass selbst eine *fehlerhafte* Re-Identifikation zu Schaden für die (tatsächlich oder scheinbar) Betroffenen führen kann, solange sie glaubwürdig erscheint.

2.2 Weitere Gefährdungen der Anonymität

Neben der angesprochenen Hauptgefährdung der Anonymität, der Re-Identifizierung, gibt es noch weitere Gefährdungen, insbesondere die Aufdeckung einer Gruppenzugehörigkeit sowie die Aufdeckung eines Attributs. Dabei werden die Daten nicht explizit einer Person zugeordnet und sind somit weiterhin im Sinne der DSGVO anonym. Dennoch können sich daraus erhebliche Gefährdungen für die

Freiheiten und Rechte betroffener Personen ergeben, wie beispielsweise in [11, S. 29] beschrieben. So kann schon das Wissen, dass eine bestimmte Person auf der Mitgliederliste der Anonymen Alkoholiker enthalten ist, problematisch sein, auch ohne die Person auf der Liste genau identifizieren zu können.

Eine eng verwandte Gefährdung, auch wenn sie sich genau genommen nicht direkt auf die Anonymität bezieht, wurde bereits von [16, S. 245] beschrieben: Schon die Verarbeitung von gruppenbezogenen und damit anonymisierten, nicht personenbezogenen Daten kann aus Sicht des Persönlichkeitsschutzes problematisch sein. Als Beispiel hierfür kann ein Bankkunde dienen, der in einer Gegend wohnt, in der viele Bewohner ihre Kredite nicht bedienen können, und daher keinen Bankkredit bekommt, obwohl er selbst eigentlich kreditwürdig wäre.

2.3 Gefährdungen durch Anonymität

Während die Anonymisierung oft als Lösung vieler Probleme des Datenschutzes gesehen wird, gibt es andere Probleme, die durch die Anonymisierung gerade erst entstehen. Darunter fällt insbesondere die Erfüllung der Betroffenenrechte, die nach einer Anonymisierung weder rechtlich einforderbar noch technisch umsetzbar ist [12, 18]. Die Betroffenenrechte nach Art. 12–23 DSGVO entfallen bei einer Anonymisierung, da die Zuordnung zwischen Daten und Betroffenen nicht mehr möglich ist. Der Verantwortliche ist gemäß Art. 11 Abs. 2 DSGVO lediglich verpflichtet, die Betroffenen darüber zu informieren, dass eine Zuordnung nicht möglich ist.

3 Konsequenzen und offene Fragen

Wenn man auch anonyme Daten aus Datenschutzsicht als schutzbedürftig bewertet, ergeben sich daraus einige zu berücksichtigende Konsequenzen und offene Fragen, die im Folgenden betrachtet werden sollen.

3.1 Informationspflichten und Auskunftsrechte

Für personenbezogene Daten gelten die Informationspflichten und Auskunftsrechte nach Art. 12–15 DSGVO ebenso wie die sonstigen Rechte der Betroffenen nach Art. 16–21. Für anonymisierte Daten können diese Rechte aber nicht mehr erfüllt werden, da die Daten nicht korrekt zugeordnet werden können.

Die DSGVO berücksichtigt diesen Aspekt zwar bereits in Art. 11 mit der Festlegung, dass in diesem Fall die Identifizierungsdaten nicht alleine zur Erfüllung dieser Rechte aufbewahrt werden müssen. Dies ändert aber nichts an der grundsätzlichen Problematik, und einige Autoren, beispielsweise Zibuschka et al. in [18], sehen die resultierenden Einschränkungen der Betroffenenrechte als wesentlichen Kritikpunkt an Anonymisierung als Datenschutzmaßnahme.

3.2 Anonymisierung als Ersatz für die Löschung von personenbezogenen Daten

Es ist bereits umstritten, ob und inwieweit die Anonymisierung von Daten dem Recht auf Löschung (Art. 17 DSGVO) sowie der aus dem Grundsatz der Datenminimierung abgeleiteten Löschpflicht Genüge tut. Eine Festlegung, dass anonymisierte Daten dem Datenschutz unterliegen, würde eindeutig klären, dass das nicht der Fall ist.

3.3 Anonyme und anonymisierte Daten

Bisher betrachtete dieser Beitrag den Schutzbedarf anonymisierter Daten, also von Daten, die einen Personenbezug hatten, wobei dieser aber durch geeignete Maßnahmen entfernt wurde. Daneben gibt es aber auch Daten, die von vornherein keinen Personenbezug haben, eine Anonymisierung also nicht erforderlich war.

Hier stellt sich nun die Herausforderung zu unterscheiden, wann solche anonymen Daten einen Schutzbedarf haben und wann nicht. Einerseits gibt es Daten, bei denen Datenschutz eindeutig nicht relevant scheint, weil es nicht um Personen oder Personengruppen geht, beispielsweise „ein Pfund Butter kostet …“. Andererseits gibt es Daten, die zwar anonym und nicht anonymisiert sind, bei denen aber die gleichen potentiellen Probleme wie bei anonymisierten Daten vorliegen, beispielsweise weil sie von vornherein ohne identifizierende Attribute erfasst wurden. Natürlich wäre es unangemessen, diese Daten anders zu behandeln als Daten, bei denen die Identifizierer nachträglich entfernt wurden.

Einige Autoren, so z. B. Boehme-Neßler in [1], gehen sogar noch einen Schritt weiter und argumentieren, das *alle* Daten letzten Endes einen Personenbezug haben. Am Beispiel eben: Wenn ich weiß, wie viel ein Pfund Butter kostet, kann ich ableiten, wie viel eine Person, die diese Butter gekauft hat, für derartige Produkte auszugeben bereit ist.

3.4 Auswirkung von Datenschutzverletzungen

Zusätzlich zu den bisher betrachteten Herausforderungen kann eine Datenschutzverletzung, beispielsweise eine unbeabsichtigte Veröffentlichung von Daten, dazu führen, dass andere, bereits vorhandene anonyme Daten durch Verknüpfung re-identifiziert werden können, vgl. [15]. Indirekt führt eine Veröffentlichung anonymer Daten also dazu, dass der potentiell entstehende Schaden bei einer Datenschutzverletzung deutlich größer wird.

4 Lösungsansätze

Verschiedene Autoren haben die genannten Probleme bereits diskutiert, mit unterschiedlichen Schlussfolgerungen. Die folgende Beschreibung gibt einen Überblick über einige Ansätze, um die beschriebenen Probleme zu lösen, wobei diese Ansätze sich zum Teil überschneiden, oder zumindest kombinieren lassen.

4.1 Risiko-orientierte Ansätze

Viele vorgeschlagene Lösungsansätze verzichten nicht ganz auf Anonymisierung, betrachten sie aber als nur einen Teil der Lösung und stellen daher eine Analyse der mit den Daten verbundenen Risiken für die Betroffenen in den Mittelpunkt. Anonymisierung ist in diesem Sinne eine Maßnahme, die den Schutz der Daten und damit der Betroffenen unterstützt, aber nicht den weiteren Datenschutz ersetzt oder überflüssig macht.

Im Folgenden werden einige Varianten dieser Sichtweise betrachtet.

4.1.1 Risikobetrachtung

In ihrem Bericht [4, S. 20 f.] beschreibt die US-amerikanische *Federal Trade Commission* einen Ansatz zur Risikominderung bei anonymisierten Daten, der aus folgenden drei Schritten besteht:

1. Der Verantwortliche (im Bericht als Unternehmen („company“) bezeichnet) unternimmt angemessene („reasonable“) Anstrengungen, um sicherzustellen, dass die Daten anonymisiert sind.
2. Der Verantwortliche verpflichtet sich öffentlich, die Daten nur in anonymisierter Form zu verwenden und sie nicht zu re-identifizieren.

3. Wenn der Verantwortliche die Daten anderen Verantwortlichen zur Verfügung stellt, seien es Dienstleister oder andere Drittparteien, dann muss vertraglich festgelegt werden, dass auch diese anderen Verantwortlichen nicht versuchen, die Daten zu re-identifizieren. Der ursprüngliche Verantwortliche hat die Verpflichtung, diese vertragliche Festlegung in angemessenem Umfang zu überwachen. Implizit ergibt sich daraus, dass die anonymisierten Daten nicht breit veröffentlicht werden dürfen, sondern noch schutzbedürftig sind und daher nur kontrolliert an ausgewählte Dritte auf Basis eines Vertrags weitergegeben dürfen.

Rubinstein und Hartzog gehen in [14] von diesem Ansatz aus, kritisieren allerdings, dass er sich nur auf das Risiko der Re-Identifizierung bezieht und nicht die anderen relevanten Gefährdungen betrachtet. Sie empfehlen eine Risikobetrachtung vergleichbar mit dem Vorgehen in der Informationssicherheit, die u. a. von den potentiellen Angreifern und deren Zielen ausgeht.

4.1.2 Forderung nach einer Datenschutz-Folgenabschätzung für Anonymisierung

Einen ähnlichen Lösungsansatz beschreiben Pohle und Hölzel in ihrer Stellungnahme [12] zum Konsultationsverfahren des BfDI. Auch hier betonen die Autoren, dass Anonymisierung zum Verlust der Betroffenenrechte führt, und folgern daraus, dass Anonymisierung als Form der Verarbeitung betrachtet werden muss, für die eine Risikobetrachtung in Form einer Datenschutz-Folgenabschätzung (DSFA) erforderlich ist. Diese DSFA sollte die verschiedenen oben beschriebenen Gefährdungen der Anonymität und der Verarbeitung anonymer Daten adressieren und die dabei entstehenden bzw. verbleibenden Risiken analysieren und bewerten.

In deutlich geringerem Umfang gilt diese Forderung bereits heute durch die allgemeine Forderung in Art. 35 DSGVO nach Durchführung einer DSFA bei einer Verarbeitung mit hohem Risiko. Es ist aber zu bezweifeln, dass in der Praxis wirklich in relevantem Umfang DSFA für Anonymisierungen durchgeführt werden, bzw. ob die tatsächlich durchgeführten DSFA ausreichend auf die *nach* einer Anonymisierung bestehenden Risiken eingehen.

4.1.3 Erweiterte Rechte der Aufsichtsbehörden

In [15] wird der Umgang mit anonymen Daten aus Sicht der Datenschutz-Aufsichtsbehörden betrachtet und angeregt, die Befugnisse der Aufsichtsbehörden so zu erweitern, dass diese bei einem hohem Risiko einer Re-Identifizierung die betroffenen Datenbestände prüfen und deren weitere Verarbeitung beschränken können.

4.2 Regulierung der großen „Entropie-Reduzierer" nach Ohm

Unter „Entropie-Reduzierern" im Bereich von Daten versteht Ohm solche Organisationen, die sehr große Datenmengen mit vielen Verlinkungen ansammeln und durch diese Verlinkungen die Entropie der Daten reduzieren, also beispielsweise Finanzdienstleister, kommerzielle Daten-Makler (data brokers) oder Internet-Suchmaschinenbetreiber [10, S. 1760]. Durch die angesammelten Datenmengen und deren Verlinkung sind solche Organisationen häufig in der Lage, auch anonymisierte Daten zu re-identifizieren, vergleiche Hypothese 1 oben.

Ohm orientiert sich an dieser Stelle an der US-amerikanischen Sichtweise, die bei der Regulierung zum Datenschutz nicht in erster Linie von den Daten selbst ausgeht, sondern sich stark an den Branchen der Verantwortlichen orientiert und daher auf branchenspezifische Regelungen fokussiert. Da in den Branchen der großen Entropie-Reduzierer das Risiko für die Betroffenen relativ groß ist, fordert Ohm für sie eine entsprechende Regulierung durch den Gesetzgeber, ausgehend von einer Bewertung der Wahrscheinlichkeit einer Re-Identifizierung. Für diese Bewertung definiert Ohm fünf Faktoren, die bei der Regulierung berücksichtigt werden sollten [10, S. 1765–1768]:

- Verwendete Anonymisierungstechniken: Hier geht es insbesondere um eine (möglichst quantitative) Bewertung der Wahrscheinlichkeit, mit der Daten re-identifiziert werden können, wie sie beispielsweise mit dem Parameter k bei der k-Anonymität, oder dem Parameter ε im Fall der ε-differentiellen Privatheit verfügbar sind.
- Private vs. öffentliche Verfügbarkeit der Daten: Solange auch anonymisierte Daten nur einem eingeschränkten Kreis von Benutzern zur Verfügung gestellt werden, ist das Risiko eine Re-Identifizierung wesentlich geringer.
- Datenmenge: Mit der Datenmenge wächst auch das Risiko einer Re-Identifizierung oder eines anderen Datenmissbrauchs, und eine Regulierung sollte daher laut Ohm die Datenmenge begrenzen.
- Motivation: In der Regulierung sollte auch die Motivation der Datenbesitzer an einer Re-Identifizierung berücksichtigt werden.
- Vertrauen: Eng verbunden mit der Motivation ist das Vertrauen in die Datenbesitzer, was natürlich noch schwieriger allgemeingültig zu bewerten ist als die Motivation.

Allerdings beschreibt Ohm konkrete Maßnahmen, die bei einer hohen Wahrscheinlichkeit einer Re-Identifizierung bzw. bei sensitiven Daten zu treffen sind, nur an

zwei Beispielanwendungen. Bei Gesundheitsdaten mit einem hohen Gefährdungspotential, gleichzeitig aber auch hohem potentiellen Nutzen für die Forschung, schlägt er die Einrichtung eines Entscheidungsgremiums vor, das über die Weitergabe derartiger Daten, auch in anonymisierter Form, entscheidet, bei hohem Risiko bis hin zu einem Verfahren mit Klassifizierung von Daten und Datenempfängern analog dem Umgang mit Verschlusssachen. Bei IP-Adressen argumentiert Ohm, dass nicht die Frage, ob es sich um personenbezogene oder anonyme Daten handelt, im Vordergrund stehen sollte, sondern der Schaden, der potentiell aus der Nutzung dieser Daten entstehen kann.

4.3 Verwaltung der Originaldaten durch eine vertrauenswürdige Partei

Ebenfalls von Ohm stammt die Beschreibung des üblichen Vorgehens als *Release-and-Forget*-Anonymisierung. Als Lösungsmöglichkeit für bestimmte Anwendungsfälle beschreibt Ohm in [10, S. 1755 f.] ein Verfahren, das sich an (zentraler) differentieller Privatheit orientiert und darauf aufbaut, dass es eine vertrauenswürdige Partei gibt, die die Originaldaten verwaltet. Anonymität wird bei diesem Vorgehen in der Form erreicht, dass öffentlich verfügbare Auswertungen fast keine Informationen über einzelne Personen enthalten. Die personenbezogenen Daten selbst existieren aber weiterhin und müssen als solche geschützt werden.

4.4 Definition einer Beobachtungspflicht

Ein gelegentlich diskutierter Lösungsansatz ist die Definition einer Beobachtungspflicht, d. h. der Verantwortliche wird verpflichtet, die Entwicklung in Bezug auf neue Verfahren oder andere Daten, mit deren Hilfe eine Re-Identifikation möglich wäre, zu beobachten und bei Bedarf die bereitgestellten anonymen Daten zurückzuziehen.

Auch wenn dieser Ansatz sicher eine sinnvolle Ergänzung anderer Lösungen beschreibt, wird er nicht als eigenständige Lösung ausreichen, da eine Veröffentlichung von Daten, seien sie anonymisiert oder personenbezogen, nicht mehr rückgängig gemacht werden kann. Dieser Lösungsansatz deckt also nur den Fall ab, dass immer wieder neue, aktualisierte Fassungen der anonymisierten Daten veröffentlicht werden, was dann bei Bedarf gestoppt werden kann. Darüber hinaus sind Einzelfälle denkbar, in denen die Daten nur für begrenzte Zeit Schutz erfordern, so

dass die Veröffentlichung zwar nicht rückgängig gemacht werden kann, später aber keinen Schaden mehr verursacht.

4.5 Formulierung konkreter Anforderungen an den Grad der Anonymität

Es gibt einige Ansätze, um den Grad der Anonymität von Daten bzw. den Grad der Anonymisierung durch entsprechende Anonymitätsmodelle zu bewerten. Die wohl bekanntesten dieser Modelle sind die k-Anonymität mit dem Parameter k, die l-Diversität mit dem Parameter l, und die ε-Differentielle Privatheit mit dem Parameter ε.

Statt nun allgemeingültig einen Schutz der anonymisierten Daten zu fordern, können diese Bewertungsverfahren genutzt werden, um ein Mindestmaß an erreichter Anonymität zu fordern, abhängig vom mit einem Bruch der Anonymität verbundenen Risiko. Erforderlich wären dafür Regeln der Form „Um anonymisierte Daten zu veröffentlichen, die höchstens ein mittleres Risiko darstellen und deren Urbild keine personenbezogenen Daten besonderer Kategorien enthält, muss mindestens eine l-Diversität mit einem Wert $l = \ldots$ nachgewiesen werden".

Diese Lösung würde damit weiterhin eine Bereitstellung von anonymisierten Daten beispielsweise für Forschungszwecke erlauben, gleichzeitig aber auch ein gewisses Mindestmaß an Anonymität sicherstellen.

Eine ähnliche, wenn auch weniger konkrete, Forderung enthalten die *Safe Harbor*-Vorgaben der US-amerikanischen HIPAA-Regelungen für Gesundheitsdaten in [9] (nicht zu verwechseln mit der gleichnamigen ehemaligen EU-US-Vereinbarung zum Datenexport). Diese Vorgaben erlauben zwei Varianten für die Anonymisierung von Gesundheitsdaten: Die erste Variante besteht aus der Forderung nach einer Expertenbewertung der Anonymisierung, typischerweise basierend auf Anonymitätsmodellen, ohne dabei aber konkrete Modelle oder Parameter vorzugeheben. Alternativ werden als zweite Variante konkrete Attribute definiert, die bei der Anonymisierung von Gesundheitsdaten entfernt bzw. zumindest generalisiert werden müssen. Diese zweite Variante ist damit sehr viel konkreter und leichter verständlich, insbesondere für Laien auf dem Gebiet der Anonymisierung. Wesentlich hilfreicher erscheint es aber, entsprechend der ersten Variante nicht ein bestimmtes Verfahren, sondern einen bestimmten Erfolg der Anonymisierung zu fordern.

4.6 Sanktionierung der Re-Identifikation

Ein grundsätzlich anderer Ansatz ist das explizite gesetzliche Verbot der Re-Identifizierung von personenbezogenen Daten, wie dies in Großbritannien bereits der Fall ist (Sect. 171 *UK Data Protection Act 2018*), wenn auch mit vielen Ausnahmen. Auch Japan hat ein solches Verbot der Re-Identifikation, siehe Abschn. 4.8. In Australien dagegen war ein ähnliches Verbot mit der *Privacy Amendment (Re-identification Offence) Bill 2016 (Cth)* geplant, wurde aber letzten Endes nicht verabschiedet.

Implizit ist die Re-Identifizierung zwar meist auch durch die DSGVO verboten, weil es keine Rechtsgrundlage für diese Verarbeitung personenbezogener Daten gibt. Ein explizites strafbewehrtes Verbot der Re-Identifizierung würde diesen Aspekt verstärken und damit eine Lösung des Problems unterstützen, wenn auch das Problem nicht vollständig lösen. Insbesondere kann ein gesetzliches Verbot nicht verhindern, dass Besitzer der Daten außerhalb des Geltungsbereiches des jeweiligen Gesetzes die Daten re-identifizieren, und auch innerhalb des Geltungsbereiches ist es beispielsweise schwierig zu erkennen, wenn ein Besitzer eine Entscheidung auf Grund einer verbotenen Re-Identifizierung getroffen hat. Ohm schrieb daher schon 2010 „A reidentification ban is sure to fail, however, because it is impossible to enforce. How do you detect an act of reidentification?“ [10, S. 1758].

Darüber hinaus ist es eine Herausforderung, in einem solchen Gesetz zwischen legitimen Gründen für eine Re-Identifikation und den zu verbietenden nicht legitimen Gründen zu unterscheiden, wie schon an den vielen Ausnahmeregelungen in den genannten Gesetzen erkennbar ist.

Insgesamt kann ein solches gesetzliches Verbot der Re-Identifikation als Ergänzung weiterer Maßnahmen helfen, wird aber die beschriebenen Probleme nicht alleine lösen können.

4.7 Bewertung der Anonymisierung als wenig oder nicht geeignete Datenschutzmaßnahme

Im Gegensatz zu den bisher beschriebenen Lösungsansätzen argumentieren Zibuschka et al. in [18], dass eine sichere Anonymisierung in der Praxis kaum erreichbar sei, eine misslungene Anonymisierung aber immer noch dazu führt, dass die definierten Rechte der Betroffenen (auf Auskunft, Löschung etc.) nicht mehr erfüllt werden können. Im Ergebnis führe das dazu, dass Anonymisierung unter den Rahmenbedingungen von Data Science etc. als Maßnahme zum Datenschutz nicht mehr geeignet ist, sondern im Gegenteil mehr schadet als nützt.

Die in der DSGVO wiederholt als Datenschutzmaßnahme genannte Anonymisierung sollte aus dieser Sicht nicht mehr genutzt werden, sondern stattdessen der Fokus auf die sonstigen technischen und organisatorischen Maßnahmen sowie die Rechenschaftspflicht des Verantwortlichen gelegt werden sollte.

Anders als bislang bewertet ist aus dieser Sicht eine Pseudonymisierung der Anonymisierung vorzuziehen: Die Schutzwirkung nach außen ist annähernd gleich hoch, aber bei der Pseudonymisierung ist eindeutig, dass die resultierenden Daten immer noch personenbezogen sind und daher dem Datenschutz und den damit verbundenen Einschränkungen unterliegen. Dazu kommt, dass – anders als bei einer Anonymisierung – die Betroffenenrechte nach einer Pseudonymisierung weiterhin erfüllbar sind.

4.8 Beispiel: Japan

Im japanischen Datenschutzrecht gibt es, anders als in fast allen anderen Ländern, auch einige Vorgaben zum Umgang mit anonymisierten Daten, hier als „Anonymously Processed Information" bezeichnet, siehe [13, S. 166 f.].[3] Gefordert ist hier u. a., dass die Anonymisierung gemäß den in weiterführenden Regelungen genannten Mindestanforderungen der Aufsichtsbehörde durchgeführt wird und Maßnahmen zur Sicherheit der anonymisierten Daten ergriffen werden. Bei einer Anonymisierung bzw. bei einer Weitergabe anonymisierter Daten müssen darüber hinaus die Kategorien der Daten und einige weitere Informationen veröffentlicht werden (Art. 36, 37, 39 APPI). Schließlich, wie bereits in Abschn. 4.6 angesprochen, gibt es ein explizites Verbot der Re-Identifikation anonymisierter Daten (Art. 38 APPI).

Zwar weicht die Abgrenzung zwischen Anonymisierung und Pseudonymisierung in Japan etwas von der Abgrenzung gemäß der DSGVO ab, was dazu führt, dass manche in Japan als anonymisiert betrachteten Daten in der EU nur als pseudonymisiert betrachtet werden, siehe [3, Abs. 30 f.]. Da die beschriebenen Regelungen damit aber insbesondere für anonymisierte Daten gelten, ist diese Abweichung für die hier betrachtete Fragestellung nicht relevant.

[3] Eine englische Übersetzung des japanischen *Act on the Protection of Personal Information* (APPI) findet man auf der Web-Präsenz der japanischen Datenschutzaufsicht unter https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf. Die im Folgenden genannten weiteren Regelungen der Aufsichtsbehörde sind unter https://www.ppc.go.jp/files/pdf/PPC_rules.pdf verfügbar.

5 Ergänzender Lösungsansatz: Ausdehnung des Datenschutzes auf „im erweiterten Sinne personenbezogene Daten"

Als Ergänzung der bisher betrachteten Lösungsansätze wird ein wie folgt erweiterter Begriff des Personenbezugs vorgeschlagen:

Definition 1 *Daten sind im erweiterten Sinn personenbezogen, wenn sie sich auf eine oder mehrere (natürliche) Personen beziehen, unabhängig davon, ob die konkreten Personen identifizierbar sind oder nicht.*

Diese Definition schließt anonymisierte oder auch aggregierte Daten über Personen ein und adressiert damit auch die mit diesen Fällen verbundenen Risiken für die Betroffenen, die vom aktuellen Datenschutzrecht nicht berücksichtigt werden. Ähnlich erhält man durch diese Definition auch einen Hebel, um die oben eingeführten Gefährdungen der Aufdeckung einer Gruppenzugehörigkeit oder von Attributen bei anonymisierten Daten zu adressieren, da auch diese Gefährdungen sich auf im erweiterten Sinn personenbezogenen Daten beziehen.

Auf die Definition von anonymen Daten als Gegensatz zu personenbezogenen Daten lässt sich dies allerdings nicht übertragen, denn unter anonym versteht man ja im allgemeinen Sprachgebrauch gerade, dass Daten sich auf eine bestimmte, aber nicht identifizierbare Person beziehen, (z. B. ist „anonym" im Duden definiert als „ungenannt, ohne Namensnennung"), also gemäß unserer Definition im erweiterten Sinn personenbezogen sind.

Aufbauend auf der Definition des erweiterten Personenbezugs können nun Anforderungen an den Schutz von im erweiterten Sinn personenbezogenen Daten definiert werden. Dieser Ansatz geht noch einen Schritt weiter als die beispielsweise in Japan geforderte Anwendung des Datenschutzes auf anonymisierte Daten, da darunter auch Daten fallen, die von vornherein anonym waren oder die sich auf Gruppen von Personen beziehen.

Die Datenschutzanforderungen können nicht vollständig die gleichen Forderungen wie für personenbezogene Daten sein, da beispielsweise die Betroffenenrechte für im erweiterten Sinn personenbezogene Daten nur sehr eingeschränkt erfüllbar sind. Insofern ist zuerst zu prüfen, welche Anforderungen anwendbar sind, und darüber hinaus, inwieweit eine Anwendung der potentiell anwendbaren Forderungen auch wünschenswert ist.

Die in Art. 5 DSGVO gelisteten Grundsätze für die Verarbeitung personenbezogener Daten (Rechtmäßigkeit, Zweckbindung, Datenminimierung etc.) sind auch für im erweiterten Sinn personenbezogene Daten anwendbar. Das gilt entsprechend

auch für die in Art. 6 DSGVO aufgeführten möglichen Rechtsgrundlagen, mit einer leichten Einschränkung bei der Nutzung einer Einwilligung als Rechtsgrundlage, denn – wie auch jetzt schon nach einer Anonymisierung von personenbezogenen Daten – die Rücknahme einer Einwilligung führt nicht dazu, dass die betroffenen Daten von der Verarbeitung ausgeschlossen werden können. Bei den Rechten der Betroffenen gemäß Art. 12–23 DSGVO können nur die Informationspflichten (Art. 13, 14 DSGVO) umgesetzt werden, im Zweifel durch Veröffentlichung der entsprechenden Informationen, ähnlich wie das in Japan bei der Anonymisierung bereits gefordert ist (siehe Abschn. 4.8). Die anderen Betroffenenrechte dagegen sind nicht mehr anwendbar, da sie sich auf Einzelpersonen beziehen, die bei im erweiterten Sinn personenbezogene Daten möglicherweise nicht mehr zugeordnet werden können.

Mit diesem Ansatz würde Anonymisierung rechtlich als ein Ansatz zum Schutz der Daten gesehen, ähnlich wie bereits jetzt die Pseudonymisierung, würde aber nicht mehr dazu führen, dass die Daten nicht mehr dem Datenschutz unterliegen.

Um die weitere Nutzung anonymisierter Daten für legitime Zwecke zu erleichtern, könnten dann entsprechende Erleichterungen definiert werden für die Verarbeitung von Daten, die nur im erweiterten Sinn personenbezogen sind, beispielsweise durch eine Festlegung, dass eine Veröffentlichung dieser Daten nur erlaubt ist, wenn ein bestimmter Grad der Anonymität erreicht ist und eine DSFA gemäß Art. 35 Abs. 4 DSGVO durchgeführt wurde.

6 Zusammenfassung und Ausblick

Der vorliegende Beitrag zeigt, dass auch anonymisierte Daten in vielen Fällen noch dem Datenschutz unterliegen sollten. Diese Erkenntnis ist in vielen Veröffentlichungen aus den letzten etwa zehn Jahren zu finden, spiegelt sich aber nicht in aktuellen gesetzlichen Regelungen wie der DSGVO wider. Es wurden einige unterschiedliche Lösungsansätze für diese Herausforderung vorgeschlagen, und punktuell werden diese auch bereits umgesetzt, aber nicht als allgemeingültige gesetzliche Regelung.

Im Kern lassen sich die Lösungsansätze in drei Gruppen unterteilen: Die erste Gruppe besteht im Wesentlichen aus einer gesetzlichen Festlegung, dass auch anonymisierte Daten schutzbedürftig im Sinne des Datenschutzes sind. Daraus ergibt sich die Forderung nach einer Regelung, dass ausgehend von einer Bewertung der verbleibenden Risiken (inkl. der Risiken, die über die reine Re-Identifikation der Daten hinausgehen) eine Umsetzung geeigneter Schutzmaßnahmen auch für anonymisierte Daten erforderlich ist. Eine zweite Gruppe geht das Problem auf juristischem

Weg durch ein Verbot der Re-Identifikation an, was die anderen Ansätze unterstützen kann, alleine aber wohl nicht ausreicht.

Die dritte Gruppe geht einen völlig anderen Weg und lehnt Anonymisierung als Maßnahme zum Datenschutz grundsätzlich ab. Stattdessen wird eine verschärfte Rechenschaftspflicht gefordert, um den mit einer Anonymisierung verbundenen Verlust der Betroffenenrechte zu verhindern.

Allerdings beschreibt keiner dieser Lösungsansätze eine vollständige Lösung der betrachteten Probleme, sondern es handelt sich jeweils nur um Teillösungen. Der vorliegende Beitrag soll daher als Grundlage für eine Diskussion dienen, wie man – wahrscheinlich mit einer Kombination verschiedener Teillösungen – die beschriebene Herausforderung am besten adressieren kann, um eine praktisch wie juristisch angemessene Lösung zu finden, beispielsweise auf Basis des hier eingeführten Begriffs der im erweiterten Sinne personenbezogenen Daten.

Literatur

1. Boehme-Neßler, V.: Das Ende der Anonymität. Wie Big Data das Datenschutzrecht verändert. DuD Datenschutz und Datensicherheit **40**(7), 419–423 (2016)
2. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI): Konsultationsverfahren zur Anonymisierung erfolgreich. https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2020/16_Konsultationsverfahren_erfolgreich.html (2020)
3. EU-Kommission: Durchführungsbeschluss (EU) 2019/419 der Kommission vom 23. Januar 2019 nach der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Japan im Rahmen des Gesetzes über den Schutz personenbezogener Informationen. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L:2019:076:FULL (2019)
4. Federal Trade Commission: Protecting consumer privacy in an era of rapid change. recommendations for businesses and policymakers. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (Mar 2012)
5. Kneuper, R., Steiner, M., Voßbein, B.: Stellungnahme: Anonymisierung unter der DSGVO. https://fb-sicherheit.gi.de/fileadmin/FB/SICHERHEIT/Stellungnahmen/Stellungnahme_FB-Sicherheit_BfDI-Konsultationsverfahren_Anonymisierung2020.pdf (2020)
6. Marnau, N.: Anonymisierung, Pseudonymisierung und Transparenz für Big Data. DuD Datenschutz und Datensicherheit **40**(7), 428–433 (2016)
7. Meyermann, A., Porzelt, M.: Hinweise zur Anonymisierung von qualitativen Daten. forschungsdaten bildung informiert 1, Forschungsdatenzentrum (FDZ) Bildung am DIPF (2014), https://www.forschungsdaten-bildung.de/get_files.php?action=get_file&file=fdb-informiert-nr-1.pdf
8. Narayanan, A., Shmatikov, V.: Robust de-anonymization of large sparse datasets. In: 2008 IEEE Symposium on Security and Privacy. S. 111–125 (2008)

9. Office for Civil Rights (OCR): Guidance regarding methods for de-identification of protected health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) privacy rule. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (Nov 2012)
10. Ohm, P.: Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Rev. **57**, 1701–1777 (Aug 2010), https://www.uclalawreview.org/broken-promises-of-privacy-responding-to-the-surprising-failure-of-anonymization-2/
11. Petrlic, R., Sorge, C.: Datenschutz: Einführung in technischen Datenschutz. Datenschutzrecht und angewandte Kryptographie, Springer Vieweg (2017)
12. Pohle, J., Hölzel, J.: Anonymisierung aus Sicht des Datenschutzes und des Datenschutzrechts. https://www.bfdi.bund.de/DE/Infothek/Transparenz/Konsultationsverfahren/01_Konsulation-Anonymisierung-TK/Stellungnahmen/Alexander-von-Humboldt-Institut.pdf?__blob=publicationFile&v=1 (2020)
13. Roßnagel, A., Geminn, C.: Datenschutz-Grundverordnung verbessern, Der Elektronische Rechtsverkehr, Bd. 43. Nomos Verlagsgesellschaft mbH & Co. KG (2020). 10.5771/9783748920991, https://www.nomos-elibrary.de/10.5771/9783748920991.pdf?download_full_pdf=1
14. Rubinstein, I., Hartzog, W.: Anonymization and Risk. SSRN Scholarly Paper ID 2646185, Social Science Research Network, Rochester, NY (Aug 2015), https://papers.ssrn.com/abstract=2646185
15. Sarunski, M.: Big Data - Ende der Anonymität. DuD Datenschutz und Datensicherheit **40**(7), 424–427 (2016)
16. Schmidt, W.: Die bedrohte Entscheidungsfreiheit. JuristenZeitung **29**(8), 241–250 (1974)
17. Sweeney, L.: *k*-Anonymity: a model for protecting privacy. Int. J. Uncertainty, Fuzzyness Knowl.-Based Syst. **10**(5), 557–570 (2002)
18. Zibuschka, J., Kurowski, S., Roßnagel, H., Schunck, C.H., Zimmermann, C.: Anonymization is dead – long live privacy. In: Roßnagel, H., Wagner, S., Hühnlein, D. (Hrsg.) Open Identity Summit 2019, S. 71–82. Gesellschaft für Informatik, Bonn (2019)

Digitales Lernen – Welche Rolle spielt die Privatheit der Daten von Schüler:innen bei der Nutzung von Lernsoftware?

Judith Meinert und Nicole C. Krämer

Zusammenfassung

Die Nutzung von Smartphones und Tablets ermöglicht auch den Zugang zu Applikationen zum Lernen und Vertiefen von Schulinhalten. Allerdings werden dabei zwangsläufig eine große Anzahl persönlicher Daten gesammelt. Hierbei kann es sich um demografische Daten, administrative Informationen, Daten aus Interaktionen und individuelle Daten wie das Vorwissen oder Testergebnisse handeln. Da die Funktionsweise solcher Lernsysteme oftmals intransparent ist, stellt sich die Frage, inwiefern Kinder und Jugendliche die Bedrohung ihrer Privatheit in horizontaler (durch die Einblicke von Lehr:innen, Eltern und Mitschüler:innen in sensible Leistungsdaten) und vertikaler (durch die kommerzielle Nutzung und Weitergabe an Unternehmen) Hinsicht wahrnehmen. Im Rahmen einer empirischen Befragung von Schüler:innen sowie von Lehrkräften und Eltern wird deshalb untersucht, in welchem Umfang Lernsoftware in den Schulen und Zuhause genutzt wird, und, ob Kenntnisse über potenzielle Bedrohungen der persönlichen Daten durch die Speicherung und Weitergabe bei der Nutzung von Lernsoftware existieren und welche Schutzmaßnahmen im Zuge dessen ergriffen werden, um die eigenen Daten zu schützen.

J. Meinert (✉) · N. C. Krämer
Universität Duisburg-Essen, Duisburg, Deutschland
E-Mail: judith.meinert@uni-due.de

N. C. Krämer
E-Mail: nicole.kraemer@uni-due.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_10

Schlüsselwörter

Lernsoftware • Privatheit • Schutzmaßnahmen • Datensicherheit • Wissen

1 Einführung

Die Nutzung von Smartphones und Tablets beginnt heutzutage bereits im Kindesalter und ermöglicht auch den Zugang zu Applikationen zum Lernen und Vertiefen von Schulinhalten. Seit ein paar Jahren bevölkern unzählige Anbieter verschiedener Software zum Lernen den Markt und werden vermehrt auch im Schulunterricht eingesetzt [9]. Allerdings existiert weder ein Überblick noch eine Systematisierung, welche Software zur Lernunterstützung in den Schulen zum Einsatz kommt, beziehungsweise wofür es Lizenzen gibt und inwieweit übergreifend gehostete Plattformen wie Moodle oder Logineo verwendet werden [11]. Darüber hinaus gibt es zahlreiche private Anbieter wie beispielsweise Sofatutor, die eher ergänzend zur Nachhilfe oder zusätzlichen Unterstützung Zuhause angeboten werden.

Generell bietet Lernsoftware verschiedenartige Lernunterstützung zu spezifischen Themen, Unterrichtsfächern, Aufgaben und Wissensständen, die auch die wechselseitige Kommunikation mit anderen Lernenden (z. B. im Klassenverband) ermöglicht [12]. Weiterhin werden die Lernprozesse und -fortschritte der Nutzenden analysiert, um personalisierte Hilfestellungen darbieten zu können [7]. Das geht zwangsläufig auch mit einer enormen Sammlung von Daten einher. So werden bei der Nutzung von Lernsoftware nicht nur demografische Daten der Nutzenden (wie z. B. Geschlecht und Alter), sondern auch administrative Informationen wie die Schule, Klasse und Ortsangaben als auch Daten aus Interaktionen mit anderen Nutzenden oder dem System wie beispielsweise das Navigationsverhalten, Eingaben in Texte und Quizze, Beiträge in Foren und individuelle Daten wie das Vorwissen, Testergebnisse und teilweise sogar Motivationen oder Stimmungszustände gespeichert [7], [13].

Aufgrund der Tatsache, dass nicht nur das generelle Verständnis der Datenverarbeitungsmechanismen von Software limitiert ist, sondern auch die Funktionsweise von Lernsoftware zumeist intransparent für die Nutzenden ist [5], ist unklar, inwiefern Kinder und Jugendliche Risiken, die mit der Speicherung ihrer Daten einhergehen (und der dadurch möglichen Erstellung, Interpretation und Weitergabe von Datenprofilen) überhaupt wahrnehmen und inwiefern Aufklärung,

Sensibilisierung und Unterstützung dahingehend durch Eltern und Lehrkräfte im privaten und schulischen Umfeld stattfindet.

Obwohl die Thematisierung von Datenschutzrisiken im Bereich der sozialen Medien teilweise schon Einzug in den Schulunterricht erhalten hat, wird der Umgang mit den Daten im Rahmen von Lernapplikationen bislang gar nicht oder nur wenig thematisiert [3]. Dabei existieren in diesem Kontext nicht nur Datenschutzrisiken in Bezug auf die kommerzielle Nutzung und Weitergabe an Unternehmen und Werbetreibende (vertikale Privatheit), sondern auch die Möglichkeit, dass Lehrkräfte, Eltern und Mitschüler:innen Einblicke in die sensiblen Leistungs- und Lernfortschrittsdaten der Schüler:innen bekommen können (horizontale Privatheit). Dementsprechend liegt die Kontrolle über die eigenen Daten nicht bei den jungen Nutzer:innen selbst. Oftmals muss bereits zur Anmeldung die (Email-) Adresse angegeben werden und die individuellen Leistungsdaten werden im Klassenverband miteinander verknüpft und/oder an die Eltern und Lehrer:innen gesendet [12]. Dadurch entstehen neben den Vorteilen einer innovativen Nutzung kreativer und zugeschnittener Lernmethoden [1] durch die damit verbundene Sammlung personenbezogener und lernbezogener Daten auch erhebliche Risiken für die Privatheit und den Schutz der Daten der Schüler:innen. Insbesondere Kinder und Jugendliche sind als vulnerable Nutzergruppe zu verstehen, die die Risiken, die sich für ihre persönlichen Daten ergeben, nicht vollumfänglich erfassen und ihren Handlungsspielraum bezüglich der Kontrolle ihrer Daten nicht kennen [5].

Studienergebnisse aus Großbritannien zeigten bereits, dass Schüler:innen sich mehr Unterstützung wünschen, um effektive Strategien zu erlernen, mit denen sie ihre Daten bei der Nutzung von Medien und Software schützen können [10]. In Deutschland ist bislang noch nicht ausgiebig untersucht worden, wie der Wissensstand der Schüler:innen zum Thema Datenschutz und Kontrolle über die eigenen Daten ist, und, ob Aufklärung darüber Zuhause oder in der Schule stattfindet. Unklar ist zudem, wer sich in der Rolle des Verantwortlichen für die Aufklärung über mögliche privatheitsbedrohende Einstellungen und datenschutzkonforme Nutzungsstrategien sieht, beziehungsweise, ob Lehrer:innen und Eltern selbst ausreichend Wissen und Medienkompetenz besitzen, um diese Rolle einnehmen zu können. Damit einhergehend stellt sich auch die Frage, ob der soziale Hintergrund eine Rolle spielt bei der Aufklärung von Kindern und Jugendlichen bezüglich ihrer Mediennutzung und dem Schutz ihrer Daten [8].

2 Empirische Befragung

Um detailliertere Einsichten sowohl in die Nutzung von Lernsoftware-Angeboten in der Schule als auch zur Unterstützung der Lernleistung Zuhause zu erhalten, wurde eine empirische Befragung von Schüler:innen sowie Lehrkräften und Eltern durchgeführt. Dabei wurden jedoch Eltern und Lehrkräfte unabhängig von den Schüler:innen rekrutiert, sodass keine relationalen Beziehungen zwischen den drei Stichproben bestehen. An der Befragung nahmen bislang 80 Schüler:innen (36 w, 41 m, 3 divers, Alter: $MW = 16.4$; $SD = 0.51$; Range 15–18) der Schulformen Gesamtschule und Gymnasium ebenso wie 69 Lehrkräfte (43 w, 25 m, 1 divers, Alter: $MW = 43.49$; $SD = 11.16$; Range: 24–65) und 55 Elternteile (36 w, 17 m, 2 divers, Alter: $MW = 42.6$; $SD = 8.7$; Range: 24–60) teil. Durschnittlich hatten die befragten Elternteile 1.76 ($SD = 0.43$) Kinder mit dem Durchschnittsalter 12.35 ($SD = 5.25$).

Es wurde untersucht, in welchem Umfang Lernsoftware in den Schulen und Zuhause genutzt wird, und, ob eine Bedrohung (vertikal und horizontal) der persönlichen Daten durch die Speicherung und Weitergabe bei der Nutzung von Lernsoftware empfunden wird. Weiterführend wurde erhoben, wie die generelle Einstellung zur Online-Privatheit ist und welche Schutzmaßnahmen ergriffen werden, um die eigenen Daten zu schützen. Darüber hinaus waren auch die wahrgenommene Selbstwirksamkeit zum Schutz der horizontalen und vertikalen Privatheit und der Zugang zu Informationen über den Schutz der eigenen Daten (Privacy Literacy) Bestandteil der Befragung.

Aufgrund der Schulschließungen im Zuge der Covid-19 Pandemie musste die Befragung unterbrochen werden, sodass die Stichprobengröße bislang noch nicht die geplante Zieldimension erreicht hat und die Befragung aktuell noch fortgesetzt wird. Dementsprechend beziehen sich die nachfolgenden Ergebnisdarstellungen auf die Auswertung der vorläufigen Stichprobe.

3 Nutzung von Lernsoftware

Um ein einheitliches Verständnis der Begrifflichkeiten Lernsoftware und Lernapplikationen zu erlangen, wurde zu Beginn der Befragungen erklärt, dass damit Apps, Programme und Software jeglicher Art gemeint sind, die zum Lernen am Smartphone, Tablet oder PC genutzt werden können. Als Beispiele wurden Antolin, Apps von Schulbuchverlagen (z. B. Klett) oder Sofatutor genannt.

In Bezug auf die generelle Nutzung von Lernsoftware gaben 35 der befragten Schüler:innen ($N = 80$) an Lernapplikationen zu nutzen, wohingegen die

anderen 45 nicht mit Lernsoftware arbeiten. Überraschenderweise gaben jedoch weitaus mehr Schüler:innen an, dass sie gerne mit Lernsoftware arbeiten würden (64). Durchschnittlich wird 15.79 min ($SD = 31.46$) am Tag mit Internetanwendungen gearbeitet, bei einer durchschnittlichen Gesamtinternetnutzungsdauer von 2.42 Stunden am PC ($SD = 4.69$) und 4.56 Stunden am Smartphone ($SD = 4.23$). Überwiegend scheint die Nutzung von Lernsoftware dabei den Schüler:innen Spaß zu machen ($MW = 3.38$; $SD = 1.33$; Skala von 1 = Trifft nicht zu bis 5 = Trifft zu). Die Schüler:innen gaben an, mehr Zuhause ($MW = 3.13$; $SD = 1.16$) als in der Schule ($MW = 2.73$; $SD = 1.19$) mit Lernsoftware zu arbeiten. Allerdings scheint dies nicht mit einer Aufforderung der Eltern in Zusammenhang zu stehen, da die Schüler:innen berichteten, dass ihre Eltern sie eher nicht auffordern, mit Lernsoftware zu üben ($MW = 1.66$; $SD = 0.88$; Skala von 1 = Trifft nicht zu bis 5 = Trifft zu). Am häufigsten wird offenbar den Lernapplikationen der Zugriff auf die Kamera (36 = Ja; 38 = Nein; 6 = Weiß nicht), gefolgt von der Kontaktliste (27 = ja, 42 = Nein, 11 = Weiß nicht) und dem Standort gewährt (20 = Ja; 56 = Nein; 4 = Weiß nicht), wobei anzumerken ist, dass die Mehrheit der Schüler:innen generell Lernapps keinerlei Zugriffe zu gewähren scheint.

Von den befragten Lehrkräften gab die Mehrheit an, Internetanwendungen im Unterricht zu verwenden (51 = Ja; 18 = Nein). Allerdings wurden dabei die AGBs der jeweiligen Lernapplikationen eher nicht gelesen (18 = Ja; 43 = Nein; 8 = Weiß nicht). Interessanterweise schätzen die Lehrkräfte, dass Internetanwendungen häufiger Zuhause ($MW = 2.93$; $SD = 1.05$; Skala 1 = Nie bis 5 = Sehr häufig) als in der Schule ($MW = 2.64$; $SD = 1.14$; Skala 1 = Nie bis 5 = Sehr häufig) genutzt werden, was in Einklang damit steht, dass im Durchschnitt nur gelegentlich zur Nutzung von Lernsoftware im Unterricht aufgefordert wird ($MW = 2.78$; $SD = 0.97$; Skala 1 = Trifft nicht zu bis 5 = Trifft zu). Insgesamt sprach sich die Mehrheit der befragten Lehrkräfte für eine Nutzung von Lernsoftware im Unterricht aus (52 = Ja; 9 = Nein; 8 = Weiß nicht).

Bezüglich der generellen Nutzung von Internetanwendungen gab die Mehrheit der Eltern an, dass ihre Kinder Internetanwendungen zum Lernen und Üben nutzen (49 = Ja; 6 = Nein), jedoch hat sich weniger als die Hälfte der Eltern im Zuge dessen mit den AGBs vertraut gemacht (23 = Ja; 28 = Nein; 4 = Weiß nicht). Als durchschnittliche tägliche Mediennutzungsfrequenz ihrer Kinder gaben die Eltern 174.04 Minuten an ($SD = 118.39$), wobei dies offenbar starken Unterschieden unterworfen ist (Range = 0 bis 600 Minuten), die sich nicht durch Altersunterschiede der Kinder erklären lassen. Dabei werden laut Einschätzung der Eltern offenbar täglich im Durchschnitt 69.09 Minuten ($SD = 64.70$; Range = 0 bis 300 Minuten) mit Internetanwendungen verbracht. Ebenso wie die Schüler:innen und Lehrer:innen

gaben auch die Eltern an, dass Lernsoftware häufiger Zuhause ($MW = 3.70$; $SD = 1.00$; Skala 1 = Nie bis 5 = Sehr häufig) als in der Schule genutzt wird ($MW = 2.96$; $SD = 1.21$; Skala 1 = Nie bis 5 = Sehr häufig). Weiterhin bitten die Eltern ihre Kinder gelegentlich mit Lernanwendungen zu arbeiten ($MW = 2.98$; $SD = 1.27$; Skala 1 = Nie bis 5 = Sehr häufig) ebenso wie sie ihren Kindern gelegentlich weitere, nicht in der Schule genutzte Lernapplikationen installiert haben ($MW = 3.33$; $SD = 1.44$; Skala 1 = Nie bis 5 = Sehr häufig). Dabei scheinen die Eltern davon auszugehen, dass ihren Kindern die Arbeit mit Lernsoftware (eher) Spaß macht ($MW = 3.67$; $SD = 1.11$; Skala 1 = Trifft nicht zu bis 5 = Trifft zu).

In Einklang mit vorherigen Untersuchungen [6] scheint generell eine positive Einschätzung von Lernsoftware und deren Effektivität in Hinblick auf Lernfortschritte zu herrschen. Es fällt jedoch auf, dass insbesondere die Eltern scheinbar die generelle Nutzungsdauer ihrer Kinder zu unterschätzen scheinen, vor allem in Hinblick auf die Smartphone-Nutzung. Allerdings muss man hierbei beachten, dass die befragte Stichprobe der Schüler:innen durchschnittlich älter war als die Kinder der befragten Elternteile. Im Umkehrschluss wird die Nutzungsdauer von Lernanwendungen innerhalb der Gesamtmediennutzung jedoch überschätzt im Vergleich zu den Angaben der Schüler:innen.

4 Einschätzung der Datensicherheit

Wie bereits eingangs erwähnt, wird bislang die Wahrnehmung und Bewertung der Datensicherheit bei der Nutzung von Lernsoftware in Befragungen zumeist weniger berücksichtigt [3], [6]. Bei der Befragung der Schüler:innen zur ihrer Einschätzung der Sicherheit ihrer Daten bei der Nutzung von Lernsoftware und möglichen Nachteilen für ihre Privatheit zeigte sich, dass die Schüler:innen die Datensicherheit auf einem mittleren Level einstuften ($MW = 2.77$; $SD = 0.88$; Skala 1 = Trifft nicht zu bis 5 = Trifft zu). Hinsichtlich spezifischer negativer Konsequenzen, die durch die Nutzung von Lernsoftware entstehen können, wurde die Veröffentlichung privater Fotos am wahrscheinlichsten bewertet ($MW = 3.75$; $SD = 1.31$; Skala 1 = sehr unwahrscheinlich bis 5 = sehr wahrscheinlich) gefolgt von Identitätsklau ($MW = 3.51$; $SD = 1.28$; Skala 1 = sehr unwahrscheinlich bis 5 = sehr wahrscheinlich), Mobbing ($MW = 3.40$; $SD = 1.37$; Skala 1 = sehr unwahrscheinlich bis 5 = sehr wahrscheinlich) und einem stärkeren Vergleich zwischen den Schüler:innen ($MW = 3.10$; $SD = 1.46$; Skala 1 = sehr unwahrscheinlich bis 5 = sehr wahrscheinlich).

Die Lehrkräfte bewerten die Datensicherheit bei der Nutzung von Lernsoftware auf einem ähnlichen Level wie die Schüler:innen im mittleren Bereich

($MW = 2.70$; $SD = 0.58$; Skala 1 = Trifft nicht zu bis 5 = Trifft zu). Allerdings bewerteten sie als mögliche, aus der Nutzung resultierende Konsequenz den stärkeren Vergleich unter den Schüler:innen am wahrscheinlichsten ($MW = 3.28$; $SD = 1.17$; Skala 1 = sehr unwahrscheinlich bis 5 = sehr wahrscheinlich), gefolgt von Mobbing ($MW = 2.91$; $SD = 1.19$; Skala 1 = sehr unwahrscheinlich bis 5 = sehr wahrscheinlich), der Veröffentlichung von Fotos ($MW = 2.84$; $SD = 1.26$; Skala 1 = sehr unwahrscheinlich bis 5 = sehr wahrscheinlich) und einem Identitätsdiebstahl ($MW = 2.77$; $SD = 1.10$; Skala 1 = sehr unwahrscheinlich bis 5 = sehr wahrscheinlich). Laut Aussage der Lehrer:innen haben ihre Schüler:innen bislang eher wenige negative Erfahrungen durch die Nutzung von Lernsoftware erfahren, wobei die Mehrzahl der Lehrer:innen angab, dies nicht zu wissen (10 = Ja; 28 = Nein; 31 = Weiß nicht).

Die Gruppe der Eltern bewertete die Sicherheit der Daten bei der Verwendung von Lernapplikationen am höchsten ($MW = 2.84$; $SD = 0.61$; Skala 1 = Trifft nicht zu bis 5 = Trifft zu). Bezüglich der Wahrscheinlichkeit möglicher auftretender negativer Konsequenzen stand wie bei den Lehrer:innen der stärkere Vergleich unter den Schüler:innen ($MW = 3.22$; $SD = 1.03$; Skala 1 = sehr unwahrscheinlich bis 5 = sehr wahrscheinlich) an erster Stelle, gefolgt von der Veröffentlichung von Fotos ($MW = 2.64$; $SD = 1.18$; Skala 1 = sehr unwahrscheinlich bis 5 = sehr wahrscheinlich), Mobbbing ($MW = 2.56$; $SD = 1.15$; Skala 1 = sehr unwahrscheinlich bis 5 = sehr wahrscheinlich) und Identitätsdiebstahl ($MW = 2.53$; $SD = 0.86$; Skala 1 = sehr unwahrscheinlich bis 5 = sehr wahrscheinlich).

Auf Basis der Ergebnisse lässt sich erkennen, dass es offenbar einen Unterschied in der Perspektive Erwachsener und Jugendlicher zu geben scheint bezüglich antizipierter Ängste und Nachteile bei der Verwendung von Lernsoftware und der durch die Datenweitergabe möglicherweise entstehenden Konsequenzen. Am stärksten unterschieden sich dabei die Eltern von den Schüler:innen und Lehrer:innen in der Bewertung der Datensicherheit bei der Verwendung von Lernsoftware, wobei diese am wenigsten besorgt um die Sicherheit der Daten waren. Allerdings ist hierbei anzumerken, dass die drei Gruppen sich nicht statistisch signifikant in ihrer Einschätzung der Datensicherheit bei der Nutzung von Lernsoftware unterschieden (F (2; 201) = 1.85; $p = .160$; $\eta^2 = .018$) und die berichteten Mittelwerte somit lediglich als Tendenz gedeutet werden können.

Des Weiteren wurden auch die möglichen negativen Konsequenzen unterschiedlich bewertet. So bewerteten die Schüler:innen die Veröffentlichung privater Fotos am wahrscheinlichsten, wohingegen Eltern und Lehrkräfte einen Leistungsvergleich zwischen den Schüler:innen am ehesten vermuteten.

5 Wahrgenommene Kontrolle durch Andere

Die Schüler:innen nehmen keine starke Kontrolle durch Eltern ($MW = 1.57$; $SD = 1.11$; Skala 1 = Trifft nicht zu bis 5 = Trifft zu) und Lehrer:innen ($MW = 1.46$; $SD = 0.80$; Skala 1 = Trifft nicht zu bis 5 = Trifft zu) bei der Nutzung von Lernsoftware wahr. Außerdem empfinden sie keinen stärkeren Vergleich zu anderen Mitschüler:innen ($MW = 1.53$; $SD = 0.66$; Skala 1 = Trifft nicht zu bis 5 = Trifft zu).

Die Lehrer:innen gaben an, die Leistungen der Schüler:innen größtenteils zu kontrollieren (32 = Ja; 25 = Nein; 5 = Weiß nicht), konnten jedoch kaum einschätzen, inwieweit die Eltern der Schüler:innen die Leistungen kontrollieren (12 = Ja; 17 = Nein; 40 = Weiß nicht). Die Lehrkräfte schätzen das wahrgenommene Gefühl von Kontrolle der Schüler:innen bei der Nutzung von Lernsoftware weitaus höher ein, als diese angaben ($MW = 3.05$; $SD = 0.87$; Skala 1 = Trifft nicht zu bis 5 = Trifft zu).

Die Eltern sind überwiegend der Auffassung, dass die Leistungen ihrer Kinder bei der Nutzung von Lernsoftware von den Lehrkräften kontrolliert werden (28 = Ja; 22 = Nein; 5 = Weiß nicht). Dementsprechend schätzten die Eltern auch das wahrgenommene Gefühl von Kontrolle ihrer Kinder bei der Nutzung von Lernapplikationen höher ein ($MW = 2.81$; $SD = 0.76$; Skala 1 = Trifft nicht zu bis 5 = Trifft zu) als die Schüler:innen selbst, jedoch nicht so hoch wie die Lehrer:innen.

6 Selbstwirksamkeit beim Schutz der eigenen Daten

Da bei der Nutzung von Lernsoftware nicht nur Datenschutzrisiken in Bezug auf die Einsichtnahme in persönliche Daten und Lernleistungen durch Lehrer:innen, Eltern und Mitschüler:innen bestehen, was eine Bedrohung der Privatheit in horizontaler Ebene beschreibt, sondern auch die Weitergabe persönlicher Daten an Werbeunternehmen als potenzielles Risiko der Privatheit auf vertikaler Ebene existiert, wurden die Schüler:innen, Lehrkräfte und Eltern zu der Einschätzung ihrer Selbstwirksamkeit beim Schutz der persönlichen Daten im Rahmen der Nutzung von Internetanwendungen wie beispielsweise Lernsoftware befragt. Die Selbstwirksamkeit lässt sich als die Überzeugung definieren, im Besitz der entsprechenden Fähigkeiten zu sein, um eine bestimmte Situation zu bewältigen [2]. Die Schüler:innen schätzten ihre eigene Selbstwirksamkeit in Bezug auf horizontale Privatheitsbedrohungen im mittleren Bereich ein ($MW = 2.85$; $SD = 0.81$; Skala 1 = Stimme nicht zu bis 5 = Stimme zu), allerdings höher als ihre Selbstwirksamkeit bezüglich vertikaler Risiken ($MW = 2.62$; $SD = 0.89$; Skala 1 = Stimme nicht zu bis 5 = Stimme zu).

Im Vergleich dazu bewerteten die Lehrer:innen ihre Selbstwirksamkeit geringer, jedoch auch hier wurde die Selbstwirksamkeit für den Schutz gegen horizontale Bedrohungen ($MW = 2.49$; $SD = 0.91$; Skala 1 = Stimme nicht zu bis 5 = Stimme zu) höher eingeschätzt, verglichen mit der Selbstwirksamkeit, vertikale Eingriffe zu verhindern ($MW = 2.28$; $SD = 0.98$; Skala 1 = Stimme nicht zu bis 5 = Stimme zu).

Auch die befragten Eltern schätzten ihre eigene Selbstwirksamkeit hinsichtlich horizontaler Bedrohungen ($MW = 2.95$; $SD = 0.77$; Skala 1 = Stimme nicht zu bis 5 = Stimme zu) höher ein als ihre Fähigkeiten, die eigenen Daten in Hinblick auf die vertikale Privatheit adäquat zu schützen ($MW = 2.70$; $SD = 0.94$; Skala 1 = Stimme nicht zu bis 5 = Stimme zu).

Insgesamt schätzten dabei die Eltern ihre Fähigkeiten für den horizontalen (F (2, 201) = 5.76; $p = .004$; $\eta^2 = .054$), als auch vertikalen (F (2, 201) = 3.73; $p = .026$; $\eta^2 = .036$) Schutz signifikant höher ein als die Schüler:innen und Lehrer:innen. Zudem schätzten die Eltern, die Fähigkeiten ihrer Kinder, sich und die eigenen Daten auf horizontaler Ebene zu schützen ($MW = 2.38$; $SD = 1.04$; Skala 1 = Stimme nicht zu bis 5 = Stimme zu) höher ein im Vergleich zu vertikalen Schutzfähigkeiten ($MW = 2.25$; $SD = 1.16$; Skala 1 = Stimme nicht zu bis 5 = Stimme zu). Auffallend dabei ist, dass die Eltern die eigenen Fähigkeiten in beiden Bereichen als ausgeprägter bewerten als die ihrer Kinder.

7 Einstellung zur Online-Privatheit

Weiterhin wurden die Stichproben der Schüler:innen, Eltern und Lehrkräfte zu ihrer generellen Einstellung zur Online-Privatheit befragt. Dabei kann nach Burgoon (1982) [4] die Privatheit in eine informationale, psychologische und soziale (sowie im Offline-Kontext eine physische) Dimension unterschieden werden.

Die informationale Privatheitsdimension bezieht sich auf die Preisgabe von Informationen, durch die die eigene Person identifiziert werden kann. Dementsprechend wurden die Studienteilnehmer:innen gebeten, auf einer Skala anzugeben, wie vorteil- bzw. nachteilhaft und wie gefährlich sie es empfinden, persönliche Informationen wie beispielsweise ihren Namen im Internet preiszugeben. Erstaunlicherweise empfanden die Schüler:innen die Preisgabe persönlicher Informationen als eher vorteilhaft ($MW = 3.62$; $SD = 1.08$; Skala 1 = sehr nachteilig bis 5 = sehr vorteilhaft) und eher ungefährlich ($MW = 3.55$; $SD = 1.01$; Skala 1 = total gefährlich bis 5 = total ungefährlich). Ein deutlich anderes Bild zeigte sich bei den Lehrer:innen, die die Preisgabe persönlicher Informationen als deutlich nachteiliger ($MW = 2.00$; $SD = 1.09$;

Skala 1 = sehr nachteilig bis 5 = sehr vorteilhaft) und gefährlicher (MW = 2.28; SD = 0.97; Skala 1 = total gefährlich bis 5 = total ungefährlich) bewerteten. Die Eltern hingegen schätzten die Informationsweitergabe zwar nachteiliger (MW = 2.42; SD = 0.91; Skala 1 = sehr nachteilig bis 5 = sehr vorteilhaft) und gefährlicher (MW = 2.40; SD = 0.92; Skala 1 = total gefährlich bis 5 = total ungefährlich) als die Schüler:innen ein, jedoch nicht in einem so starken Ausmaß wie die Lehrkräfte.

Die psychologische Privatheitsdimension repräsentiert die Offenbarung von Gefühlen, Werten und Einstellungen, sodass die Stichproben nach ihrer Einschätzung gefragt wurden, wie vorteilhaft und ungefährlich die Preisgabe persönlicher Gedanken, Gefühle und Einstellungen im Internet ist. Die Schüler:innen empfanden es als eher vorteilhaft (MW = 3.90; SD = 1.12; Skala 1 = sehr nachteilig bis 5 = sehr vorteilhaft) und ungefährlich (MW = 3.57; SD = 0.93; Skala 1 = total gefährlich bis 5 = total ungefährlich), im Internet Gedanken und Gefühle zu veröffentlichen. Im Kontrast dazu bewerteten die Lehrer:innen das Teilen von Gefühlen und Gedanken als eher nachteilig (MW = 1.99; SD = 1.01; Skala 1 = sehr nachteilig bis 5 = sehr vorteilhaft) und gefährlich (MW = 2.41; SD = 1.05; Skala 1 = total gefährlich bis 5 = total ungefährlich). Die Bewertungen der Eltern waren im mittleren Bereich angesiedelt, mit einer leichten Tendenz zur eher vorteilhaften (MW = 2.75; SD = 0.84; Skala 1 = sehr nachteilig bis 5 = sehr vorteilhaft) und ungefährlichen Einschätzung (MW = 2.91; SD = 1.04; Skala 1 = total gefährlich bis 5 = total ungefährlich).

Die soziale Privatheit reflektiert das erwünschte Verhältnis von Nähe und Distanz zu anderen Menschen, was im Online-Kontext beispielsweise durch die Regulation von Zugänglichkeit zum eigenen Profil definiert werden kann. In Folge dessen wurden die Teilnehmer:innen gefragt, wie vorteilhaft und ungefährlich sie es finden, zu bestimmen, wer Zugang zu ihren Kommentaren und Updates auf sozialen Netzwerkseiten (z. B. Facebook) hat. Die Schüler:innen bewerteten das Zugriffs-Management auf ihre persönlichen Profile als eher nachteilig (MW = 2.63; SD = 1.51; Skala 1 = sehr nachteilig bis 5 = sehr vorteilhaft) und den freien Zugang als eher ungefährlich (MW = 3.07; SD = 1.18; Skala 1 = total gefährlich bis 5 = total ungefährlich). Bei den Lehrer:innen fielen die Einschätzungen von Zugriffsregulation sehr viel vorteilhafter (MW = 4.09; SD = 1.40; Skala 1 = sehr nachteilig bis 5 = sehr vorteilhaft) aus. Auch die Eltern bewerteten die Regulation von Zugriffen anderer auf die eigenen Profilinhalte als vorteilhaft (MW = 3.67; SD = 1.20; Skala 1 = sehr nachteilig bis 5 = sehr vorteilhaft) und ungefährlich (MW = 3.95; SD = 1.24; Skala 1 = total gefährlich bis 5 = total ungefährlich). Insgesamt fällt deutlich auf, dass die Schüler:innen auf den verschiedenen Ebenen des informationalen (F (2; 201) = 47.96; p <.001; η^2 = .326), psychologischen (F (2; 201) = 62.86; p <.001; η^2 = .388)

und sozialen (F (2; 201) = 22.89; p <.001; η^2 = .188) Privatheitsverhaltens am sorglosesten sind.

8 Zugang zu Privatheitswissen (Privacy Literacy)

Eine entscheidende Vorrausetzung zum Schutz der Privatheit und eigenen Daten im Internet besteht darin, zu verstehen, wie Informationen erfasst und weiterverwendet werden können und welchen Handlungsspielraum zum Schutz der Nutzende hat [15].

Die Stichproben aus Schüler:innen, Lehrer:innen und Eltern sind deshalb nach ihrem Zugang zu Wissen über den Schutz der eigenen Privatheit im Internet befragt worden. Der verwendete Fragebogen enthielt dabei zum Beispiel Fragen danach, ob im privaten und schulischen Umfeld darüber gesprochen wird, wie man im Internet seine Daten schützen kann und, ob man selbst aktiv nach Informationen sucht oder durch die Medien mitbekommt. Dabei berichteten die Schüler:innen (MW = 2.28; SD = 0.68; Skala 1 = Nie bis 5 = Immer), deutlich weniger Zugang zu Informationen über den Schutz der eigenen Daten und Privatheit zu erhalten als die Lehrer:innen (MW = 2.71; SD = 0.64; Skala 1 = Nie bis 5 = Immer) und Eltern (MW = 3.06; SD = 0.67; Skala 1 = Nie bis 5 = Immer). Die drei Gruppen der Schüler:innen, Lehrer:innen und Eltern unterscheiden sich dabei in ihrem jeweiligen Zugang zu Privatheitswissen, statistisch signifikant voneinander (F (2; 201) = 23.16; p <.001; η^2 = .187).

Bezüglich der spezifischen Wege, über die Informationen und Wissen über Privatheit und Privatheitsschutz erlangt werden, zeigte sich, dass die Schüler:innen am häufigsten im privaten Umfeld Informationen erhalten, wohingegen die Lehrkräfte und Eltern häufiger im beruflichen Umfeld sowie durch die aktive Suche und im Internet mit Privatheitswissen in Berührung kommen. Eine detaillierte Übersicht findet sich in Tab. 1.

Damit stehen die Ergebnisse der aktuellen Befragung hinsichtlich der Einschätzung des eigenen Zugangs zu Wissen über Privatheitsschutz im Gegensatz zu Autoren, die postulieren, dass Kinder und Jugendliche heutzutage als sogenannte *digital natives* über ausreichend Wissen und Kompetenzen verfügen, um verantwortungsbewusst mit Internetanwendungen und Lernapplikationen umzugehen – sofern es in ihrem Handlungsspielraum liegt [14].

Tab. 1 Gegenüberstellung der Wege, über die die Schüler:innen, Lehrkräfte und Eltern Zugang zu Privatsheitswissen erhalten (Skala 1 = Nie bis 5 = Immer)

	Schüler:innen	Lehrer:innen	Eltern
Im privaten Umfeld	2,42 (1,08)	2,80 (0,82)	2,53 (0,99)
Im Internet	2,41 (1,10)	2,77 (0,96)	3,35 (0,96)
Aktive Suche	2,38 (1,05)	2,87 (1,06)	3,13 (0,96)
Im schulischen/ beruflichen Umfeld	2,35 (1,01)	3,14 (0,97)	3,35 (1,09)
Durch Medienkampagnen	2,20 (1,17)	2,28 (0,95)	3,13 (1,11)
Per Mail	1,95 (1,20)	2,58 (1,09)	2,98 (1,13)

9 Schutzmaßnahmen

Um zu erfahren, wie praktisch mit dem Schutz der eigenen Daten im Internet umgegangen wird, wurden die Teilnehmer:innen gefragt, welche Schutzmaßnahmen sie in den letzten sechs Monaten im Internet ergriffen haben. Dabei waren Mehrfachnennungen möglich (Übersicht in Tab. 2).

Die am häufigsten von den Schüler:innen genannte Maßnahme war dabei die Nutzung einer Verschlüsselungssoftware, um im Internet zu surfen (91,1 %). Darauf folgten die Optionen ‚Ich habe Online-Dienstbetreibende darum gebeten, persönliche Daten von mir zu löschen' (88,6 %) und ‚Ich habe andere Internet-Nutzende darum gebeten, persönliche Daten von mir zu löschen' (87,3 %).

Bei den Lehrer:innen war die am häufigsten ausgewählte Maßnahme ‚Ich habe andere Internet-Nutzende darum gebeten, persönliche Daten von mir zu löschen' (92,8 %), direkt gefolgt von der Option ‚Ich habe keine dieser Maßnahmen ergriffen' (91,3 %). Am dritthäufigsten wurde die Nutzung von Browsern mit der Tor- oder Wrapper-Software genannt (88,4 %).

Die Gruppe der Eltern gab am häufigsten an, keine der genannten Maßnahmen ergriffen zu haben (98,2 %). Darüber hinaus wurden am zweithäufigsten Schutzmaßnahmen wie das Nutzen von Browsern mit Tor- oder Wrapper-Software (92,7 %) und Anonymisierungstools (87,3 %) angegeben.

In der Gesamtbetrachtung fällt auf, dass die Schüler:innen wesentlich mehr unterschiedliche Maßnahmen anwenden, um ihre Privatheit im Internet zu schützen. Im Unterschied dazu verwendeten die Lehrer:innen insbesondere Maßnahmen, die im eigenen Kontrollspektrum liegen (z. B. die Nutzung von Verschlüssungssoftware oder speziellen Browsern) oder gar keine Maßnahmen, was eventuell auf große individuelle Unterschiede in der Handhabung der eigenen Privatheit im Internet basierend auf Erfahrungshorizont und Erfahrungen

Tab. 2 Gegenüberstellung der von Schüler:innen, Lehrer:innen und Eltern genutzten Schutzmaßnahmen in Prozent und Anzahl der Nennungen (Mehrfachnennungen waren möglich)

Schutzmaßnahmen	Schüler:innen (80)	Lehrer:innen (69)	Eltern (55)
Ich habe eine Verschlüsselungssoftware genutzt, um im Internet zu surfen.	91,1% (72)	87,0% (60)	81,8% (45)
Ich habe Online-Dienstbetreibende darum gebeten, persönliche Daten von mir zu löschen.	88,6% (70)	85,5% (59)	81,8% (45)
Ich habe andere Internet-Nutzende darum gebeten, persönliche Daten von mir zu löschen.	87,3% (69)	92,8% (64)	85,5% (47)
Ich nutzte extra Browser mit der Tor- oder Wrapper-Software.	84,8% (67)	88,4% (61)	92,7% (51)
Ich habe Anti-Tracking-Software genutzt (z. B. uBlock Origin, Adblock Plus, Better Privacy).	79,7% (63)	56,5% (39)	67,3% (37)
Ich habe keine dieser Maßnahmen ergriffen.	79,7% (63)	91,3% (63)	98,2% (54)
Ich nutzte Anonymisierungstools, wenn ich online bin (z. B. Ghostery, welches die Übermittlung von privaten Daten).	69,6% (55)	78,3% (54)	87,3% (48)
Ich habe die Cookies oder den Cache (d.h. Zwischenspeicher) meines Internet-Browsers gelöscht.	62,0% (49)	30,4% (21)	20,0% (11)
Auf Online-Plattformen habe ich mich mit einem Pseudo-/Kosenamen angemeldet.	57,0% (45)	52,2% (36)	45,5% (25)
Ich habe eine nicht echte E-Mail-Adresse bei der Anmeldung auf bestimmten Internet-Seiten genutzt.	55,7% (44)	68,1% (47)	56,4% (31)
Ich habe auf die Nutzung bestimmter Online-Dienste verzichtet, um meine persönlichen Daten nicht dafür herzugeben.	54,4% (43)	36,2% (25)	47,3% (26)
Ich beschränkte mich in dem, was ich im Internet tue und sage, um meine Privatsphäre zu schützen.	50,6% (40)	43,5% (30)	47,3% (26)
Ich habe den Verlauf meines Internet-Browsers (z. B. Chrome, Mozilla Firefox, Safari) gelöscht.	39,2% (31)	43,5% (30)	36,4% (20)

rückschließen lässt. Ein Großteil der Eltern scheint überwiegend keine Maßnahmen zu verwenden. Insgesamt sprechen die Ergebnisse dafür, einen reziproken Wissens- und Kompetenzaustausch zwischen Schüler:innen und Lehrer:innen sowie Eltern zu etablieren und vertiefen, sodass die Erwachsenen auch von einem Wissensvorsprung der Kinder und Jugendlichen profitieren könnten.

10 Fazit

Die Ergebnisse der Befragung der Schüler:innen, Eltern und Lehrkräfte liefern nicht nur Evidenz über den Einsatz von Lernsoftware, sondern ebenso über den Wissensstand von Schüler:innen, Lehrer:innen und Eltern in Hinblick auf die Relevanz und Erreichung eines effektiven Datenschutzes bei der Nutzung von Lernsoftware. Auffallend ist dabei insbesondere, dass generell von nur einer geringen Anzahl Schüler:innen Lernsoftware genutzt wird, wobei ein Großteil jedoch gerne mit Software-Lösungen zum Lernen arbeiten würde. Demzufolge sollte zukünftig insbesondere systematisch untersucht werden, welche Lernapplikationen in den Schulen genutzt werden.

Weiterhin zeigte sich, dass die Eltern der befragten Stichprobe die geringsten Bedenken bezüglich der Sicherheit der persönlichen Daten bei der Nutzung von Lernsoftware hatten, was insbesondere in Hinblick darauf problematisch sein kann, dass Eltern ihre Kinder zur Nutzung von Lernapplikationen ermutigen (z. B. um Lerninhalte zu vertiefen oder Wissensdefizite aufzuarbeiten) ohne vollumfänglich die damit einhergehenden Risiken zu beachten oder sich dementsprechend zu informieren, beispielsweise durch das Lesen der AGBs. Entsprechend schätzten sowohl Lehrer:innen als auch Eltern ihre eigenen Fähigkeiten gegenüber vertikalen Privatheitsbedrohungen (u. a. die Weitergabe von Daten an Unternehmen zu Werbezwecken) gering ein, woraus sich schlussfolgern lässt, dass ihnen demnach auch die Kompetenz fehlt, ihre Schüler:innen und Kinder adäquat im Umgang mit derartigen Risiken zu schulen und unterstützen. In diesem Sinne berichteten die Schüler:innen auch über sehr wenig Zugangsmöglichkeiten zu Wissen über Privatheitsrisiken (z. B. über Gespräche im privaten Umfeld, in der Schule oder in den Medien).

Darauf basierend ergeben sich Implikationen, um nicht nur die Aufmerksamkeit des Themas Datenschutz im Bildungsbereich zu forcieren, sondern auch auf Basis der Erkenntnisse über den Wissensstand und die Verantwortungsverortung Maßnahmen für den gezielten Kompetenzerwerb der Schüler:innen abzuleiten. Hierbei sollte in erster Linie der Zugang zu Wissen über Privatheitsschutz fokussiert werden, da vor allem die Schüler:innen kaum Zugang zu Wissen über den Schutz der eigenen Daten und den Umgang mit Privatheit zu haben schienen. Dies könnte beispielsweise als fester Bestandteil in Lehrpläne integriert werden, um den Schüler:innen nicht nur im schulischen Kontext, sondern auch in privaten Nutzungskontexten die reflektierte Auswahl von Software und Applikationen unter (stärkerer) Berücksichtigung datenschutzrelevanter Einstellungen zu ermöglichen.

Bei der Interpretation der Ergebnisse der Befragung müssen allerdings einige Limitationen berücksichtigt werden. Bislang ist nur eine Altersgruppe von Schüler:innen befragt worden, sodass noch unbeantwortet ist, wie jüngere Schüler:innen den Schutz ihrer Daten und Privatheit bewerten. Weiterhin bestanden zwischen den drei Stichproben der Schüler:innen, Lehrkräfte und Eltern keine relationalen Beziehungen, was die Generalisierbarkeit der Ergebnisse einschränkt, insbesondere da die befragten Eltern sehr viel jüngere Kinder hatten. Ein weiterer Aspekt bezieht sich auf die Erhebungszeitpunkte, die vor und während der Covid-19 Pandemie lagen, wodurch digitales Lernen durch Homeschooling und Online-Unterricht unterschiedlich salient wahrgenommen und dementsprechend bewertet worden sein kann.

Literatur

1. Avella, J.T., Kebritchi, M., Nunn, S.G., Kanai, T.: Learning analytics methods, benefits, and challenges in higher education: A systematic literature review. Online Learning, **20**(2), 13–29 (2016)
2. Bandura, A.: Self-efficacy: toward a unifying theory of behavioral change. Psychol. Rev. **84**(2), 191 (1977)
3. Biehl, C.J., Hug, A.: Entwicklung einer Unterrichtsreihe zu dem Thema Datenschutz mit Fokus auf den mathematischen Relationen in Sozialen Netzwerken (Doctoral dissertation, Universität Koblenz-Landau) (2019)
4. Burgoon, J.K.: Privacy and communication. Annals. Int. Commun. Associat., **6**(1), 206–249 (1982)
5. Drachsler, H., Greller, W.: Privacy and analytics: it's a DELICATE issue a checklist for trusted learning analytics. In: Proceedings of the sixth international conference on learning analytics & knowledge, 89–98 (2016)
6. Fokides, E.: Digital educational games and mathematics. Results of a case study in primary school settings. Educat. Inform. Tech., **23**(2), 851–867 (2018)
7. Ifenthaler, D., Schumacher, C.: Learning analytics im Hochschulkontext. WiSt–Wirtschaftswissenschaftliches Studium, **45**(4), 176–181 (2016)
8. Kutscher, N., Bouillon, R.: Kinder. Bilder. Rechte, Persönlichkeitsrechte von Kindern im Kontext der digitalen Mediennutzung in der Familie. ISO 690. (2018) https://doi.org/10.13140/RG.2.2.17887.71845
9. Link, T., Schwarz, E.J., Huber, S., Fischer, U., Nuerk, H.C., Cress, U., Moeller, K.: Mathe mit der Matte – Verkörperlichtes Training basisnumerischer Kompetenzen. Zeitschrift für Erziehungswissenschaft, **17**(2), 257–277 (2014)
10. Livingstone, S., Stoilova, M., Nandagiri, R.: Talking to children about data and privacy online: research methodology. (2019)
11. Niegemann, H., Weinberger, A.:Was ist Bildungstechnologie?. In: Handbuch Bildungstechnologie, (S. 3–16). Springer, Berlin, Heidelberg (2020)

12. Pardo, A., Siemens, G.: Ethical and privacy principles for learning analytics. British J. Edu. Tech. **45**(3), 438–450 (2014)
13. Romero, C., Ventura, S.: Educational data mining and learning analytics: An updated survey. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, **10**(3), e1355 (2020)
14. Wai, I.S.H., Ng, SS.Y., Chiu, D.K., Ho, K.K., Lo, P.: Exploring undergraduate students' usage pattern of mobile apps for education. J. Librarian. Inform. Sci. **50**(1), 34–47 (2018)
15. Zhao, J., Wang, G., Dally, C., Slovak, P., Edbrooke-Childs, J., Van Kleek, M., Shadbolt, N.: I make up a silly name' Understanding Children's Perception of Privacy Risks Online. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 1–13 (2019)

Datenschutz- und Sicherheitsanalyse von Mobilen Learning Apps

Sunny Dass, Michael Kreutzer, Linda Schreiber und Hervais Simo Fhom

Zusammenfassung

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 der der Präsenz-Schulbetrieb mehrfach stark eingeschränkt werden musste. Im Rahmen dieses Beitrags untersuchen wir, inwieweit Android Learning Apps vor dem Hintergrund der DSGVO die Privatheit ihrer Nutzenden (i. d. R. Minderjährige) gewährleisten bzw. Anforderungen an Datensicherheit erfüllen. Die Datengrundlage für die Untersuchung besteht aus 199 Learning Apps aus dem Google Play Store. Die Analyse unterteilt sich in zwei Schritte: die grobgranulare und die feingranulare Analyse. Die grob-

Diese Forschungsarbeit wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

M. Kreutzer · L. Schreiber · H. Simo Fhom (✉)
Fraunhofer SIT, Darmstadt, Deutschland
E-mail: Hervais.SimoFhom@sit.fraunhofer.de

M. Kreutzer
E-mail: Michael.Kreutzer@sit.fraunhofer.de

L. Schreiber
E-mail: Linda.Schreiber@sit.fraunhofer.de

S. Dass
Technische Universität Darmstadt, Darmstadt, Deutschland
E-mail: sunny.dass@stud.tu-darmstadt.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_11

granulare Analyse befasst sich mit Beobachtungen und statistischen Erkenntnissen, welche direkt aus den bereits gesammelten Metadaten der Apps ersichtlich sind. Weiterhin werden die Ergebnisse hinsichtlich Datenschutz und Datensicherheit kritisch hinterfragt, indem Metadaten bezüglich Datenschutzerklärung und Berechtigungen eingestuft werden. Die feingranulare Analyse baut auf der grobgranularen Analyse auf. Hierbei wird das Android Package (APK) mittels Tools zur statischen und dynamischen Analyse genauer betrachtet. Des Weiteren werden das Vorhandensein und die Qualität von Maßnahmen zur Absicherung des Datenverkehrs der ausgewählten Apps untersucht und bewertet. Wir stellen fest, dass viele Learning Apps Datenschutzrichtlinien oder sichere Datenübertragung bieten, die Apps auf unsichere Weise implementiert sind und oft eine zum Teil niedrige Codequalität vorweisen, was auf zusätzliche Cybersicherheits- und Datenschutzrisiken schließen lässt.

Schlüsselwörter

Learning Apps • Privatheit • Datenschutz

1 Einführung

In der aktuellen Corona-Pandemie scheinen Learning Apps, welche von Kindern und Jugendlichen jederzeit und von überall benutzt werden können, eine besonders attraktive Alternative zu sein, um ihre schulischen Fertigkeiten weiterzuentwickeln Tengler et al. (2020) [12]. Die Vorteile solcher Learning Apps zeichnen sich vor allem durch die Bereitstellung eines vielfältigen digitalen Lernangebots aus. Trotz steigender Attraktivität bleibt jedoch die Frage offen, wie es mit Daten- und Privatheitschutz in Mobile Learning Apps steht. Dabei ist insbesondere die Frage zu beantworten, ob und wie privatheitsinvasiv und anfällig für Cyberangriffe Mobile Learning Apps sind.

Das Hauptziel dieser Arbeit ist es, eine umfassende Untersuchung der Datenschutz- und Sicherheitsproblematik im Zusammenhang mit Learning Apps aus dem Google Play Store durchzuführen. Die vorliegende Arbeit behandelt diese Frage auch vor dem Hintergrund der DSGVO, die beispielsweise mit Erwägungsgrund 38 einen besonderen Schutz für Kinder und Minderjährige vorschreibt (siehe Abschn. 2). Dies wirft weitere Fragen auf, denen wir im Rahmen unserer Studie nachgegangen sind, u. a.: Wie hoch ist der Anteil von Learning Apps ohne eine Datenschutzerklärung? In welchem Land sitzt der Anbieter? Welche Zusatzbibliotheken für Tracking und Werbung (die sog. Third-Party Libraries) sind im App-

Code eingebettet? Welche Berechtigungen werden i. d. R. angefordert? Welche/wie viele Sicherheitslücken und Fehlkonfigurationen im Quellcode gibt es? Um eben erwähnte Fragen beantworten zu können, wurde im Rahmen der Studie eine Vorgehensweise konzipiert, die aus zwei aufeinanderfolgenden und abgestimmten Schritten besteht: 1) Aufbauen eine Datengrundlage und 2) Durchführung der Analyse.

Als Datengrundlage, siehe Abschn. 3, werden 199 Android Learning Apps aus dem Google Play Store Germany in unsere Analyse einbezogen, 167 kostenlose Apps und 32 kostenpflichtige Apps. Pro App werden die sog. Android Package (APK-Datei) und entsprechenden Metadaten gesammelt, 33 Metadaten insgesamt. Zu den Metadaten gehören u. a. die Datenschutzerklärungs-URL, die Adresse des Entwicklers und die Gesamtanzahl der Bewertungen der App auf Google Play. Um festzustellen, inwieweit diese Learning Apps eine Bedrohung für die Privatheit und den Datenschutz ihrer Nutzenden darstellen, konzipieren wir eine Analyse bestehend aus zwei Stufen: eine grobgranulare Analyse (Abschn. 4) und eine feingranulare Analyse (Abschn. 5). Die grobgranulare Auswertung zielt auf eine Beurteilung der Privatheitsbedrohung einer Learning App ausschließlich auf Grundlage einer statistischen Interpretation ihrer Metadaten ab. Darunter fallen Statistiken zu einzelnen Metadaten, wie die Entwickleradresse bei der Ursprungslandsanalyse oder die durchschnittliche Bewertung, Anzahl an Installationen oder Kommentaren, welche bei der Popularitätsanalyse erstellt worden sind. Weiterhin werden die Ergebnisse hinsichtlich Datenschutz und Datensicherheit kritisch hinterfragt. Somit folgt eine Datenschutzerklärungsanalyse bei der die Verteilung zwischen Apps mit bzw. ohne Datenschutzerklärung zusammen mit anderen Metadaten in Verbindung gebracht wird. Zuletzt folgt eine Berechtigungsanalyse, wobei Berechtigungen hinsichtlich normaler und gefährlicher Berechtigungen statistisch dargestellt und analysiert werden. Die feingranularen Analysen konzentrieren sich dagegen darauf, die APK-Datei der gegebenen Learning App auf mögliche Schwachstellen und Fehlkonfigurationen zu überprüfen. Dabei werden zur Charakterisierung ihres Laufzeitverhaltens und ihrer Datensammlungspraktiken sowohl statische als auch dynamische Analysemethoden und Tools verwendet.

2 Learning Apps im DSGVO-Kontext

Für die vielfältigen Risiken der digitalisierten Welt sind insbesondere Kinder und Jugendliche in ihrer Entwicklungsphase anfällig. Zudem sind sich Kinder den Folgen der Verarbeitung von personenbezogenen Daten oftmals weniger bewusst oder

sie können diese schlechter kontrollieren.[1] Diese besondere Schutzbedürftigkeit wird auch von der Datenschutz-Grundverordnung (DSGVO) anerkannt.

Gemäß Erwägungsgrund 38 sollte ein besonderer Schutz „insbesondere die Verwendung personenbezogener Daten von Kindern für Werbezwecke oder für die Erstellung von Persönlichkeits- oder Nutzerprofilen und die Erhebung von personenbezogenen Daten von Kindern bei der Nutzung von Diensten, die Kindern direkt angeboten werden, betreffen". Da das Merkmal „direkt angeboten" nicht weiter eingeschränkt wird, ist davon auszugehen, dass hiervon nicht nur Angebote erfasst sind, die sich ausschließlich an Kinder richten, sondern auch Angebote, die sich sowohl an Kinder als auch an Erwachsene richten.[2]

Unter der DSGVO besteht eine grundsätzliche Verpflichtung zur Information betroffener Personen zum Zeitpunkt der Datenerhebung durch den Verantwortlichen. Gemäß Art. 13 Abs. 1 DSGVO umfasst dies unter anderem den Kontakt der verantwortlichen Stelle, die Zwecke der Verarbeitung sowie Informationen über die Rechte Betroffener. Die Vorschriften zur Ausgestaltung dieser Datenschutzinformationen ergeben sich aus Art. 12 Abs. 1 DSGVO. Demnach hat der Verantwortliche alle Informationen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten." Die Artikel-29-Datenschutzgruppe präzisiert die Anforderung der „klaren und deutlichen Sprache", indem Informationen so einfach wie möglich und unter Vermeidung komplexer Satz- und Sprachstrukturen zu formulieren sind. Darüber hinaus sollte eine übermäßig juristische, technische oder fachspezifische Terminologie vermieden werden. Zur Voraussetzung der Verständlichkeit gehört, dass der Verantwortliche den jeweiligen Kenntnisstand des Zielpublikums berücksichtigt und die Informationen so gestaltet, dass sie von einem durchschnittlichen Mitglied dieses Publikums verstanden werden. Wenn ein App-Anbieter also Kinder als Zielgruppe hat oder sich bewusst ist oder sein sollte, dass das Angebot insbesondere von Kindern genutzt wird, sollte er sicherstellen, dass Vokabular, Tonfall und Stil der verwendeten Sprache für Kinder geeignet sind.[3] Ein Beispiel für eine auf Kinder ausgerichtete Sprache nennt die Artikel-29-Datenschutzgruppe der „UN Convention on the Rights of the Child in Child Friendly Language".[4] Die Datenschutzinformation kann durch andere Maß-

[1] Ausführlich hierzu Roßnagel (2020) [8].

[2] Vgl. Heckmann/Paschke, Art. 8, in: Ehmann/Selmayr [5], Rn. 21/22; Buchner/Kühling, Art. 8, in: Kühling/Buchner [6], Rn. 16.

[3] Article 29 Working Party (2016) [1], S. 8–10.

[4] https://sites.unicef.org/rightsite/files/uncrcchilldfriendlylanguage.pdf. Stand: 06.07.2020.

nahmen wie Comics, Animationen und Piktogramme ergänzt werden.[5] Die sprachlichen Voraussetzungen implizieren auch, dass die Datenschutzinformation in der Sprache des Landes zur Verfügung gestellt werden, in dem die betroffenen Personen sind, an die sich die App richtet.[6]

3 Datengrundlage

Für die Erfassung der relevanten Learning Apps beschränken wir uns in dieser Arbeit auf den Google Play Store Germany als Datenquelle. Die Wahl von Google Play Germany lässt sich durch dessen hohen Marktanteil unter den globalen App Stores begründen.

Vorgehensweise bei der Datensammlung Anhand von passenden Sucheinstellungen und Suchbegriffen werden Apps aus dem Google Play Store selektiert und tabellarisch aufgeführt. Hierdurch ergibt sich zunächst eine Zwischenliste, welche anschließend aufgrund von Inkonsistenzen in einem Cleaning-Prozess aussortiert werden muss. Dies führt zu mehreren Iterationen im Suchprozess der Apps, wobei die Suchbegriffe konstant bleiben und lediglich die Sucheinstellungen variiert werden.

Sucheinstellungen Da wir mit Google Play Store Germany im deutschsprachigen Bereich nach unseren Apps suchen möchten, wählen wir als Sucheinstellung auf der Google Play Store-Webseite im Browser die Header-Sprache Deutsch. Weiterhin wollen wir in der Sektion Apps auf Google Play nach unseren Learning Apps suchen, sodass sich folgende URL als unsere Grundlage zum Datensammeln ergibt: https://play.google.com/store/search?q&c=apps&hl=de. Da wir außerdem nutzerbezogene Ergebnisse, welche durch Anmeldungen mithilfe eines Google-Kontos oder IP-bezogene Präferenzen auftreten können, vermeiden möchten, nutzen wir den Play Store ohne Anmeldung als Google Nutzer. Anders als beim Google Play Store in Smartphones werden im Browser keine Apps als Anzeige von Google geworben, sodass diese nicht in die Datenerfassung einbezogen werden. Alle Apps in unserem Datensatz wurden durch die Einstellung „Alle Preise“ in der Sektion „Apps“ ausgewählt, sodass sowohl kostenfreie als auch kostenpflichtige Anwendungen berücksichtigt worden sind.

[5] Article 29 Working Party (2016) [1], S. 12.

[6] Dix, Art. 12, in: Simitis/Hornung/Spiecker gen. Döhmann (2018) [10], Rn. 15.

Verwendete Suchbegriffe & Suchergebnisse Für unsere Suche werden 12 Suchbegriffe verwendet, welche semantische Verbindungen mit Learning Apps haben. Dazu zählen vor allem Begriffe mit Bezug zu Schulfächern und allgemeines Lernen. Da hierbei verschiedene Bereiche in Betracht gezogen worden sind, gelten die Ergebnisse der einzelnen Suchbegriffe als repräsentativ für die Gesamtheit von Learning Apps. Die verwendeten Suchbegriffe sind: *Learning, Education, School, M Learning, Mobile Learning, Language Learning, Sprachen lernen, Mathe, Deutsch, Hausaufgaben, Übungsaufgaben und Lernen*. Abgesehen vom Suchbegriff „Übungsaufgaben" wurden bei allen Suchbegriffen exakt 250 Apps gefunden, weil Google Play Store Germany je Suchbegriff nicht mehr Ergebnisse im Browser anzeigt. Fasst man alle Apps aus diesen 12 Zwischenergebnissen zusammen, so ergibt sich eine Gesamtheit von 2997 Apps.

Cleaning Aus den gesammelten 2997 Apps ergeben sich die folgenden drei Herausforderungen, welche bewältigt werden müssen, um einen konsistenten Datensatz für die Analyse zu sichern: 1) Duplikate (Eine App kann in mehreren Suchbegriff-Ergebnislisten vorkommen); 2) Große Ergebnismenge – (Weil die Analyse einer solche Menge an Apps den Rahmen unserer Studie sprengen würde, sind lediglich die Top 30-Apps pro Suchbegriff in den Datensatz eingeflossen); 3) Falsch zugeordnete Learning Apps (Apps, die keine Learning features vorweisen und lediglich das Etikett des Suchbegriffs tragen, sind irrelevant für die Analyse). Nach den Cleaning-Schritten erhalten wir eine Liste von 167 Apps.

Zusätzliche Betrachtung kostenpflichtiger Apps Auffällig bei dieser Datenmenge aus 167 Apps ist jedoch, dass bei keinem der zugrundeliegenden Suchbegriffe kostenpflichtige Apps in den Top 30 Ergebnissen aufgelistet sind. Bei den zuvor betrachteten Suchergebnissen traten kostenpflichtige Apps erst jenseits der Top 30 Grenze auf, da sie von Nutzern anscheinend seltener benutzt werden. Für unsere Analyse sollen aber auch kostenpflichtige Anwendungen explizit betrachtet werden. Hierfür wird lediglich die Einstellung „Alle Preise" zu „kostenpflichtig" in der Suche bei Google Play Store Germany umgewandelt. Die restlichen Einstellungen verbleiben unverändert. Der Vorgang der Datenerhebung wird hier genauso mit denselben Suchbegriffen vorgenommen. Jedoch definieren wir die Top 10 je Suchbegriff als angemessenen Umfang für die Datenerfassung kostenpflichtiger Apps. Somit erhalten wir mit einem identischen Vorgehen wie bei der ersten Suche eine Gesamtheit von 120 Apps. Nach einer Bereinigung der so erhobenen Datenmenge (analog zum Cleaning-Prozess für die Datenmenge der kostenlosen Apps) erhalten wir 32 kostenpflichtige Learning Apps. Unser Datensatz ist nach erfolgreicher Aussortierung der irrelevanten Datenelemente nun vollständig und enthält 199 Learning

Apps für Kinder und Jugendliche – 167 kostenlose Apps und 32 kostenpflichtige Apps.

Erfasste Metadaten Für eine ausgewogene Analyse reichen die zunächst gesammelten Angaben zu den Apps wie etwa App-Namen und App-URLs nicht aus, sodass weitere Informationen, sog. Metadaten, gesammelt werden müssen. 33 potenziell nützliche Metadaten (33 werden in dieser Studie verwendet), welche aus dem Google Play Store Germany frei verfügbar sind, werden berücksichtigt.

Datenerfassungsinstrumente Für die Datengrundlage werden pro App die APK-Datei und die entsprechenden Metadaten gesammelt. Für die Datenerfassung im Rahmen unserer Studie sind entsprechend zwei Instrumente entwickelt und eingesetzt worden: ein Metadaten-Crawler und ein APK-Crawler. Mittels beider Instrumente erhalten wir folglich eine Liste von 167 kostenlosen und 32 kostenpflichtigen Apps zusammen mit ihren gecrawlten Metadaten als Datengrundlage unserer Analyse.

4 Grobgranulare Analyse

Nachfolgend stellen wir unsere Ergebnisse der Ursprungslands-, Popularitäts- und Datenschutzerklärungsanalyse vor.

4.1 Ursprungslandsanalyse

Wir definieren das Ursprungsland als das Land, welches den Standort des Entwicklers laut Google Play Store bezeichnet. Somit wird das Ursprungsland einer App aus dem gesammelten Metadatenattribut „Entwickler-Adresse“ gewonnen. Es wird ein zusätzliches Attribut für die Apps aufgegriffen, um diese Ursprungsländer einer Ursprungsregion zuzuteilen. Wir wählen hierbei Regionen bzw. Länder als Ursprungsregionen aus, welche wir für diese Analyse hinsichtlich Datenschutz und Cybersicherheit als relevant erachten. Somit ergeben sich folgende 6 Ursprungsregionen: Europäische Union (EU), Vereinigte Staaten von Amerika, Kanada, Russland, China und Sonstige. Bei der EU sind auch Länder wie die UK (United Kingdom/Vereinigtes Königreich) enthalten, welche zwar nicht mehr in der EU-Mitglied sind, jedoch immer noch ein Datenschutzabkommen mit der EU einhalten (Stand: 2020).

Die Werte aus Abb. 1 zeigen deutlich, dass die meisten Apps sowohl bei den kostenlosen als auch kostenpflichtigen als Ursprungsland Deutschland oder die Vereinigten Staaten aufweisen. Bei den kostenlosen Apps fällt allerdings noch auf, dass 8 Apps aus Indien und 10 Apps aus Spanien stammen. Leider geben 33 der kostenlosen Apps keine Information zur Adresse des Entwicklers in Google Play Store an, sodass ihre Ursprungsländer für diese Analyse nicht verfügbar sind. Nachdem die einzelnen Länder den entsprechenden Ursprungsregionen zugeordnet worden sind, erhalten wir eine Verteilung der Ursprungsregionen wie folgt: Etwa 46 % der kostenlosen und 59 % der kostenpflichtigen stammen aus der Ursprungsregion EU. Interessant für die weitere Analyse ist hierbei, inwiefern die Apps die strengen Datenschutzrichtlinien der EU einhalten. Abgesehen von den sonstigen Ursprungsländern sind die Vereinigten Staaten von Amerika am zweithäufigsten vertreten. Auffällig bei den kostenlosen Apps ist vor allem, dass 25 bzw. 33 der Apps zu den sonstigen Ursprungsregionen bzw. keinem Ursprungsland zugeordnet worden sind, wobei die kostenpflichtigen lediglich ein bis zwei Apps dieser Eigenschaft enthalten.

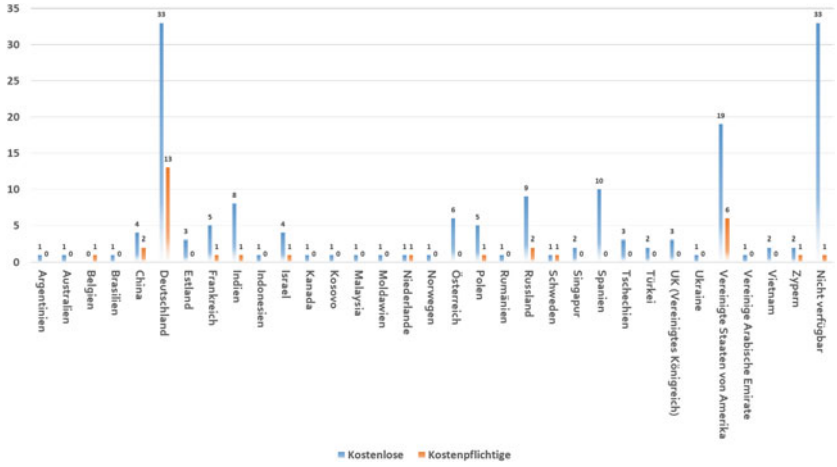


Abb. 1 Anzahl der Apps pro Ursprungsland

4.2 Popularitätsanalyse

Unter Popularität ist der Bekanntheitsgrad einer Learning App gemeint. Dies ist nicht zu verwechseln mit der Beliebtheit einer App, da eine App auch durch negative Erfahrungen bekannt und folglich nicht als beliebt bezeichnet werden kann. In unserer Popularitätsanalyse werden Metadaten betrachtet, welche vor allem die Bekanntheit einer App implizieren. Hierzu zählen wir die Metadaten: Installationen (minimale Anzahl an Installationen auf Endgeräten durch Nutzer), Bewertungen (die exakte Anzahl der Nutzerbewertungen, wobei eine Bewertung durch das Verteilen von Sternen in Google Play Store abgegeben wird), Kommentare (die Anzahl der vom Nutzer verfassten Kommentare unter einer App in Google Play Store), durchschnittliche Bewertung und Android-Versionen.

In Tab. 1 werden einige wichtige Durchschnittswerte zu entsprechenden Metadaten dargestellt. Hierbei zeigen die Werte deutlich, dass die kostenpflichtigen Apps im Durchschnitt weitaus weniger Kommentare, Installationen und Bewertungen aufweisen als die kostenlosen Apps. Dies ist nicht überraschend, da die meisten App-Store-Nutzer kostenfreie Apps vorziehen und daher diese Diskrepanz in den Metadaten entsteht. Überraschend ist jedoch, dass die Nutzerzufriedenheit bei kostenpflichtigen Apps bei einer durchschnittlichen Bewertung von 3,6 nicht besonders gut ist, obwohl die Entwickler Geld für den Erwerb dieser Apps fordern. Die Werte aus der Tabelle implizieren, dass die kostenlosen Apps populärer sind als die kostenpflichtigen, da sie weitaus mehr Kommentare, Installationen und Bewertungen im Durchschnitt ausweisen. Je höher diese Werte sind, desto höher ist auch der Bekanntheitsgrad einer App. Aus Abb. 2 geht hervor, dass vor allem Learning Apps, welche die Vereinigten Staaten als Ursprungsregion bzw. -land haben, eine relativ hohe Anzahl an Installationen aufweisen im Vergleich zu den übrigen Ursprungsregionen. Zwar scheint auch die Ursprungsregion Kanada eine beträchtliche Anzahl an Installationen aufzuweisen, jedoch zeigte die Ursprungslandsanalyse, dass Kanada

Tab. 1 Durchschnittliche Werte für Metadaten aus unserem Datensatz

–	Kostenlose Apps	Kostenpflichtige Apps
Ø Anzahl an Installationen	3.155.822	14.850
Ø Anzahl an Bewertungen	90.070	835
Ø Anzahl an Kommentaren	35.970	343
Ø Anzahl an Berechtigungen	7,37	4,5
Ø Bewertung	4,01	3,6

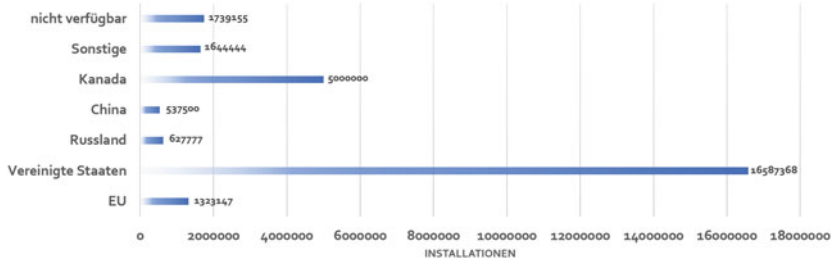


Abb. 2 Relation zwischen Ursprungsregion und zugehöriger durchschnittlicher Anzahl an Installationen bei den kostenlosen Apps

als Region lediglich eine App als Datenelement beinhaltet und somit kein ausgewogener Vergleich zu den Regionen Europa und Vereinigten Staaten durchgeführt werden kann. Die Europäische Union weist in dieser Grafik keine besonderen Merkmale auf, jedoch beträgt die Anzahl der durchschnittlichen Installationen für Apps aus dieser Region weniger als die Hälfte des Mittelwerts aller kostenlosen Apps, wie ein Vergleich mit Tab. 1 zeigt. Überraschend zu diesem Ergebnis ist der Vergleich mit den kostenpflichtigen Apps in Abb. 3. Hier liegt der Peak an Installationen bei der Region China, wobei auch hier erwähnt werden muss, dass diese Region nur 2 Apps als Elemente aufweist. In dieser Grafik belegen die Apps mit der Ursprungsregion Vereinigten Staaten den vorletzten Platz vor den sonstigen Regionen. Im Vergleich zu den kostenlosen Apps liegt die durchschnittliche Anzahl an Installationen bei den europäischen, kostenpflichtigen Apps viel näher bei dem Mittelwert aus Tab. 1.

4.3 Bewertungen

Abb. 4 zeigt, dass der Großteil der Apps eine durchschnittliche Bewertung von 4 Sternen enthält. Unter 167 kostenlosen Apps existieren jedoch auch 7 Apps, welche keine Bewertung zum Zeitpunkt der Datenerfassung hatten (z. B. die *OLLIS:Mathe 3* App). Besonders auffällig hierbei ist, dass keine der Apps eine Bewertung oder Nutzerkommentare aufweist, obwohl die Anwendungen teilweise seit 2017 in Google Play Store veröffentlicht worden sind. Unter den kostenpflichtigen existieren 5 Apps, welche ebenfalls keine Bewertungen von Nutzern im Google Play Store erhalten haben.

In Abb. 5 sind die durchschnittlichen Bewertungen pro Ursprungsregion für kostenlose und kostenpflichtige Apps abgebildet. Wir stellen fest, dass Europa als

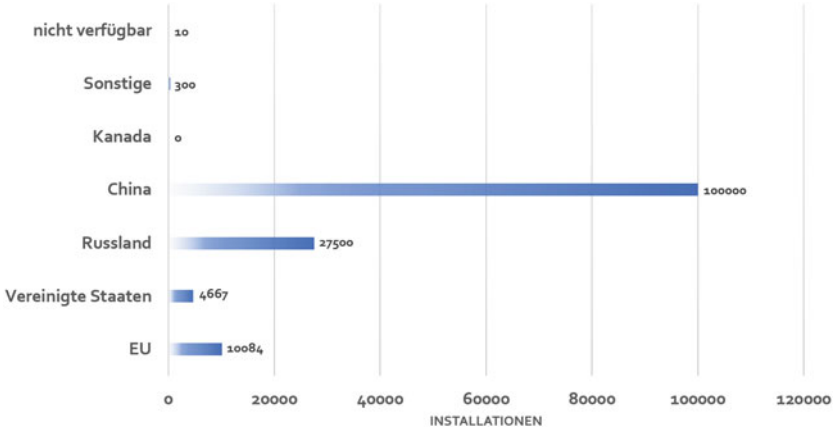


Abb. 3 Relation zwischen Ursprungsregion und zugehöriger durchschnittlicher Anzahl der Installationen bei den kostenpflichtigen Apps

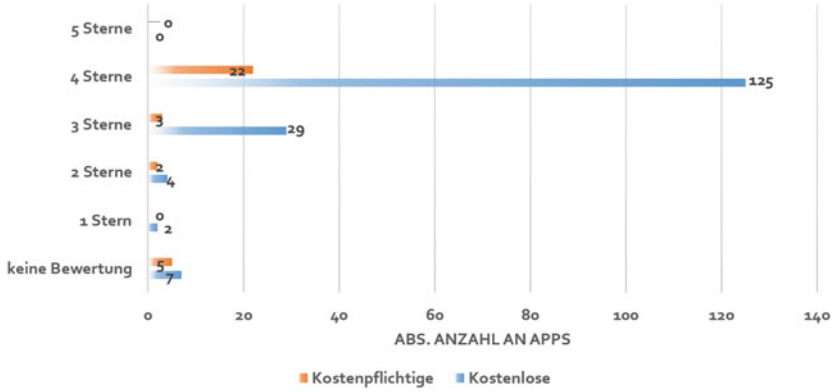


Abb. 4 Anzahl der Sternbewertung und zugehörige Anzahl an Apps; die Sternbewertung ist auf die nächste ganze Zahl abgerundet worden

Ursprungsregion für beide Datensätze eine wesentlich schlechtere Durchschnittsbewertung aufweist als die übrigen Regionen.

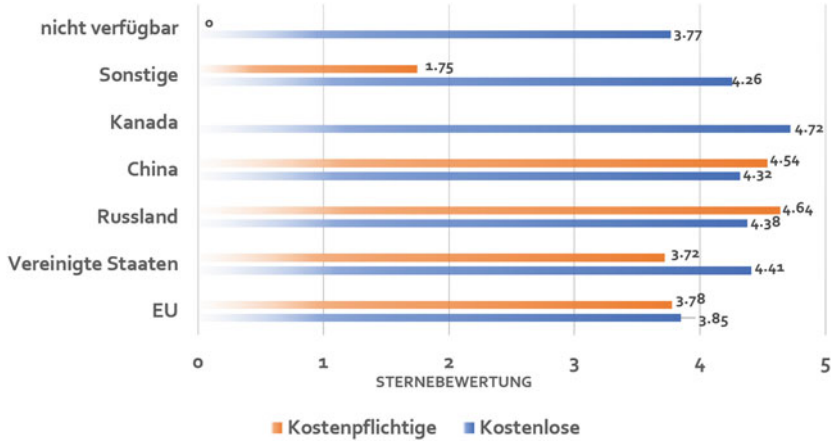


Abb. 5 Relation zwischen Ursprungsregion und zugehöriger durchschnittlicher Bewertung

4.4 Datenschutzerklärungsanalyse

Entwickler sind gesetzlich dazu verpflichtet eine Datenschutzerklärung zu erstellen und für ihre Nutzer im Google Play Store öffentlich verfügbar zu machen, falls sie personenbezogene Daten vom Nutzer verarbeiten (siehe Abschn. 2). Wenn also Learning Apps keine Datenschutzerklärung bereitstellen, so dürfen sie beispielsweise persönliche Informationen von ihren Nutzern weder anfordern noch speichern. Dies muss je nach Anwendungsfall auf Implementierungsebene überprüft werden. Wenn bestimmte sensitive Berechtigungen angefragt werden, welche auf persönliche Informationen vom Smartphone des Nutzers zugreifen können, so muss eine Datenschutzerklärung vorliegen.[7] Im Google Play Store ist die Datenschutzerklärung, sofern diese vom Entwickler veröffentlicht worden ist, bereits vor der Installation über einen Link verfügbar, welcher im Crawling-Prozess erfasst worden ist. Es gibt jedoch auch Apps wie etwa *Mathe-Formeln – Offline26,* welche einen Link zu einer Datenschutzerklärung in Google Play Store angeben[8], wobei dieser Link jedoch zu keiner gültigen Webseite oder Dokument führt. Solche Apps werden ebenfalls zu Apps ohne Datenschutzerklärung hinzugezählt, da dem Nutzer zur Zeit der Überprüfung keine Erklärung angeboten werden konnte. Von den 167 kostenlosen Apps besitzen 13 keine Datenschutzerklärung, welche auf Google Play

[7] Article 29 Working Party (2016) [1].

[8] http://thanhhangfood.com/elearning_privacy_policy.txt

Tab. 2 Vergleich zwischen Learning Apps mit und ohne Datenschutzerklärung

–	Mit Datenschutzerklärung	Ohne Datenschutzerklärung
Ø Anzahl an Installationen	3.407.930	169.315
Ø Anzahl an Bewertungen	97.500	2055
Ø Anzahl an Kommentaren	38 940	777
Ø Anzahl an Berechtigungen	7,44	6,54
Durchschnittliche Bewertung	4,00	4,06

Store öffentlich verfügbar ist. So hat beispielsweise die App *Mathe Arena – Mathematik für Abitur & Matura27* keine Datenschutzerklärung. Auffällig bei einigen dieser Anwendungen ist jedoch, dass sie im Durchschnitt 6,5 Berechtigungen und einige Elemente sogar bis zu 20 Berechtigungen fordern. Die Verteilung von Apps mit und ohne Datenschutzerklärungen ist bei den kostenpflichtigen Apps weiter kompakter als bei den kostenlosen. So geben nur 3 von 32 kostenpflichtigen Apps keine Datenschutzerklärung an. Nennenswert hierbei ist vor allem, dass nur eine davon Berechtigungen anfordert (Tab. 2).

Der Vergleich zwischen Apps mit und ohne Datenschutzerklärung in Tab. 5 zeigt, dass Anwendungen ohne eine Datenschutzerklärung deutlich weniger Installationen, Bewertungen und Nutzerkommentare aufweisen als die übrigen Anwendungen. Die Anzahl der angeforderten Berechtigungen ist im Durchschnitt bei Apps ohne Datenschutzerklärung nur leicht höher. Die Bewertungen der Apps sind bei beiden Vergleichsgruppen sehr nah beisammen.

Ursprungsregionen der Apps ohne Datenschutzerklärung 38 % (5 von 13) dieser Apps geben keine Entwickleradresse an, sodass wir keine Ursprungsregion für diese Elemente feststellen können. Besonders auffällig bei den Daten sind die 4 Apps ohne Datenschutzerklärung, welche der EU als Ursprungsregion angehören. Von diesen Apps fordern 2 Apps 20 Berechtigungen bzw. 7 gefährliche Berechtigungen[9] an, obwohl sie keine gültige Webseite für die Datenschutzerklärung anbieten. Gefährliche Berechtigungen indizieren meist den Gebrauch von sensitiven Informationen des Nutzers. Im Vergleich hierzu gehören 2 der 3 kostenpflichtigen Apps ohne Datenschutzerklärung der Ursprungsregion EU und das übrige Datenelement gehört der Region Russland an. Eine der europäischen Apps fordert hierbei 2 gefährliche Berechtigungen an.

[9] Android Developers: Protection levels: https://developer.android.com/guide/topics/permissions/. Stand: 06.07.2020.

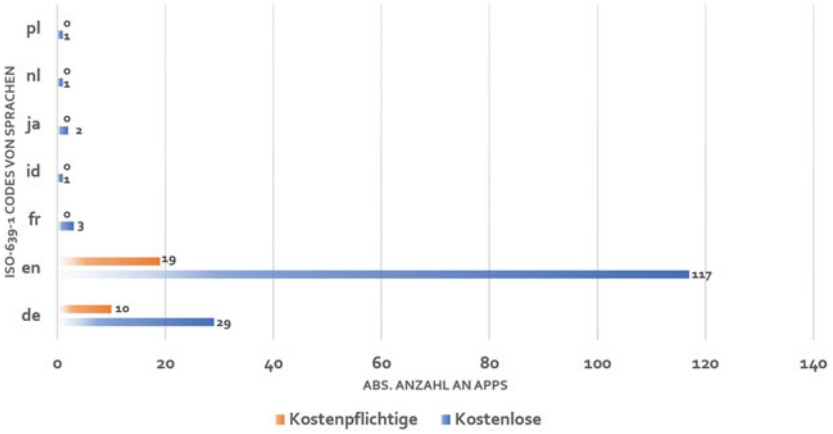


Abb. 6 Sprachen der Datenschutzerklärungen

Sprachen der Datenschutzerklärungen Datenschutzerklärungen auf Deutsch und Englisch sind mit großem Vorsprung am stärksten vertreten, siehe Abb. 5. In den Datenschutzerklärungen treten neben Deutsch (29 kostenlose und 10 kostenpflichtige), Englisch (117 kostenlose und 19 kostenpflichtige) die Sprachen Französisch (3 kostenlose und 0 kostenpflichtige), Indonesisch (1 kostenlose und 0 kostenpflichtige), Japanisch (2 kostenlose und 0 kostenpflichtige), Niederländisch (1 kostenlose und 0 kostenpflichtige) und Polnisch (1 kostenlose und 0 kostenpflichtige) auf (Abb. 6).

Die Ergebnisse in Abb. 7 zeigen, dass Learning Apps mit Datenschutzerklärungen in den Sprachen Deutsch und Französisch die höchste Anzahl an Berechtigungen im Schnitt aufweisen, wobei Französisch zusätzlich eine sehr schlechte durchschnittliche Bewertung mit 1,35 Sternen besitzt. Die Apps mit deutschen Datenschutzerklärungen besitzen lediglich eine Durchschnittsbewertung von 3,23 Sternen.

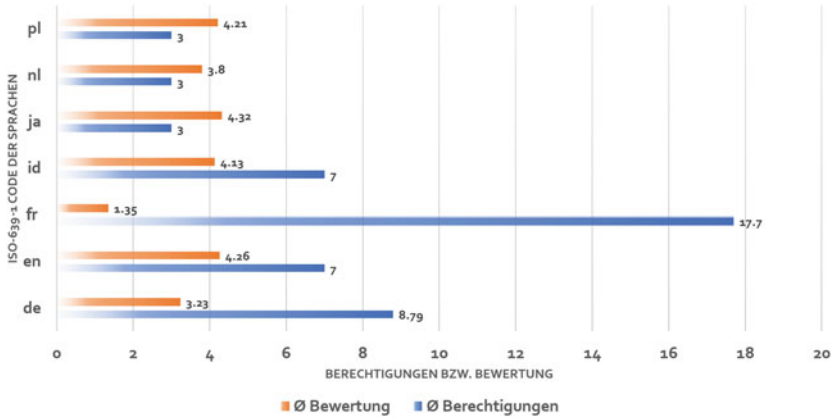


Abb. 7 Sprache der Datenschutzerklärung und zugehörige Statistik bezüglich durchschnittlicher Bewertung und angeforderte Berechtigungen bei den kostenlosen Apps

5 Feingranulare Analyse

5.1 Berechtigungsanalyse

Das Android-Betriebssystem bietet ein Berechtigungsmodell zur Steuerung des Zugangs zu persönlichen Daten (z. B. Standort) und sensiblen Systemressourcen (z. B. Mikrofon)[10]. Für die Berechtigungsanalyse stützen wir uns auf den **„Protection levels“** von Google, welche jede einzelne Berechtigung in **normale, gefährliche und Signatur Berechtigungen** unterteilt.[11] Hierbei wird zusätzlich zwischen den sogenannten Laufzeit-Berechtigungen und Berechtigungen, welche zur Installationszeit angefordert werden, unterschieden. Bei letzteren fordert die App vor der Installation die Zustimmung des Nutzers für alle in Google Play Store aufgelisteten Berechtigungen an. Als **normale Berechtigungen** definiert Google Berechtigungen, welche benötigt werden, um auf Daten außerhalb der Sandbox einer App zuzugreifen. Hierbei besteht, verglichen mit gefährliche Berechtigungen, jedoch nur ein geringfügiges Risiko für die Privatsphäre des Nutzers oder Operationen anderer Apps. Diese Berechtigungen werden der App zur Installationszeit gewährt, sofern diese im Android-Manifest der App deklariert worden

[10] https://developer.android.com/guide/topics/permissions/overview. Stand: 06.07.2020.

[11] Android Developers: Protection levels: https://developer.android.com/guide/topics/permissions/. Stand: 06.07.2020.

sind, und können vom Nutzer nicht widerrufen werden. Ein Beispiel für eine normale Berechtigung wäre *android.permissions.BLUETOOTH*, welche einer App die Möglichkeit gewährt, sich mittels Bluetooth mit anderen Bluetooth-Geräten zu verbinden. ***Signatur-Berechtigungen*** werden einer App ebenfalls zur Installationszeit gestattet, jedoch nur, falls die angeforderte Berechtigung mit demselben Zertifikat signiert ist wie die App, welche die Berechtigung definiert. So kann beispielsweise eine App mittels der Signatur-Berechtigung *android.permission.BATTERY_STATS* Informationen zum Status der internen Batterie sammeln. ***Gefährliche Berechtigungen*** hingegen ermöglichen es einer App, auf private Daten und Informationen des Nutzers zuzugreifen oder die Operation von anderen Apps zu beeinträchtigen. Außerdem können Apps Kontrolle über das Gerät erhalten und sich somit negativ auf den Nutzer auswirken. Der Nutzer muss jedoch explizit den aufgelisteten, gefährlichen Berechtigungen zustimmen, damit die App Zugriff auf die betreffenden Funktionen erhält. Ohne dessen Zustimmung kann die App die Funktionen, welche die gefährliche Berechtigung benötigt, nicht ausüben. So wird beispielsweise die gefährliche Berechtigung *android.permission.CAMERA* benötigt, falls eine App Zugriff auf die Kamera des Gerätes fordert.

Angeforderte Berechtigungen per Apps Die Anzahl der angeforderten Berechtigungen für alle Apps variiert sehr stark – zwischen 0 und 28 Berechtigungen pro App. Abb. 8 stellt eine Übersicht über die Verteilung der Berechtigungen über alle untersuchten Learning Apps unseres Datensatzes dar. Der Graph weist 3 Peaks bei 3, 8 und 15–20 Berechtigungen bei den kostenlosen Apps auf. Bei den kostenfreien hingegen sind die Balken relativ ausgeglichen, jedoch liegen die größeren Balken hier bei vergleichsmäßig niedrigeren Berechtigungszahlen als bei den kostenlosen. Diese Erkenntnis spiegelt sich auch in den Durchschnittswerten aus der Übersicht in Tab. 1 wieder.

Angeforderte Berechtigung per Protection Level Insgesamt fordern die 199 Apps 1412 normale, 267 gefährliche und 79 Signatur-Berechtigungen in den Android-Manifesten an. Die daraus resultierenden Durchschnittswerte sind in Abb. 9 dargestellt.

Berechtigungen & Sprache der Datenschutzerklärung Bereits mit Abb. 7 wurden die hohen Berechtigungswerte bei den Apps mit französischer Datenschutzerklärung festgestellt. Dieser Befund spiegelt sich auch in Abb. 10 wider: Da die gefährlichen Berechtigungswerte mit den Berechtigungen allgemein in Relation zu stehen scheinen, ist die Feststellung nicht überraschend, dass die Apps mit französi-

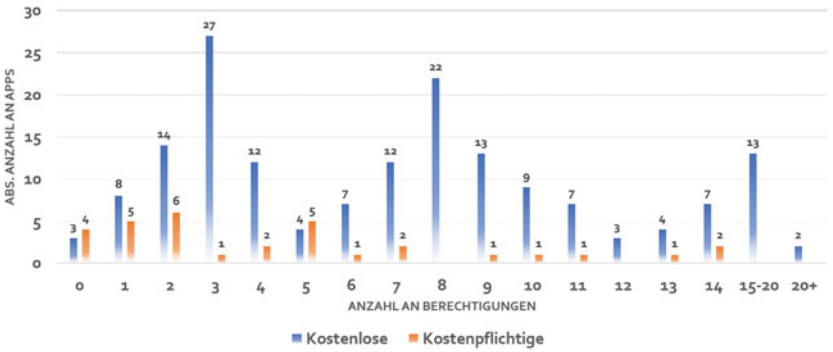


Abb. 8 Relation zwischen Apps und Berechtigungen

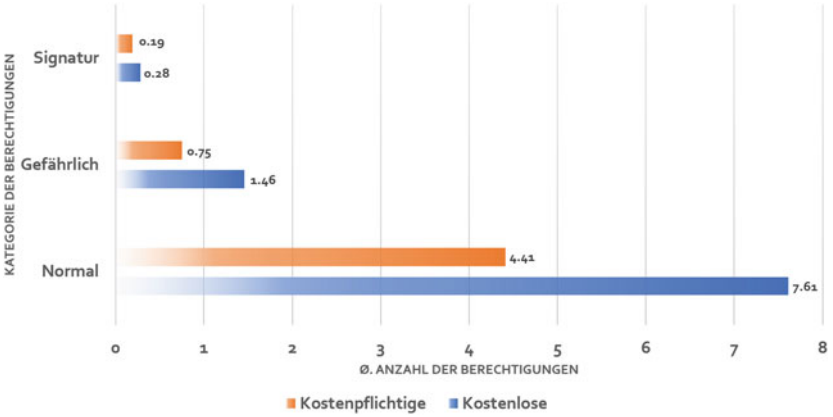


Abb. 9 Verteilung der Berechtigungen in ihre Kategorien und ihr durchschnittlicher Wert unter allen Apps

scher Datenschutzerklärung auch sehr viele gefährliche Berechtigungen anfordern. Bei den übrigen Sprachen sind keine besonderen Merkmale erkennbar.

Verteilung gefährlicher Berechtigungen Aus einer genauen Untersuchung geht hervor, dass 12 einzigartige, gefährliche Berechtigungen im Datensatz der kostenlosen Apps bzw. 5 im Datensatz der kostenpflichtigen auftreten. Wir führen hierbei eine Häufigkeitsanalyse durch, um festzustellen, für welche Funktionen Learning

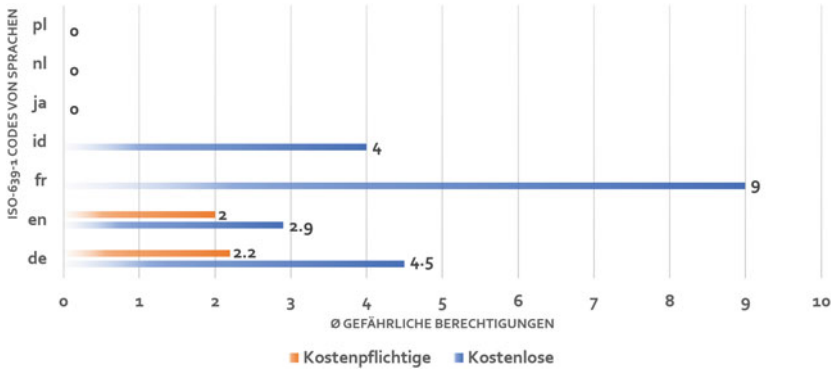


Abb. 10 Durchschnittliche Anzahl an gefährlichen Berechtigungen für Apps mit bestimmter Sprache in der Datenschutzerklärung

Apps gefährliche Berechtigungen im Allgemeinen anfordern. Die Ergebnisse dieser Analyse, in Abb. 11 zusammengefasst, zeigen deutlich, dass die meisten Apps in beiden Datensätzen überwiegend Zugriff auf Speicherdaten durch Berechtigungen wie *WRITE_EXTERNAL_STORAGE* oder *READ_EXTERNAL_STORAGE* erhalten. Berechtigungen wie etwa

RECORD_AUDIO oder *CAMERA,* welche für Gerätefunktionen wie das Mikrofon oder die Kamera benötigt werden, nehmen untere Plätze in der Häufigkeitsanalyse ein. *ACCESS_FINE_LOCATION* und *ACCESS_COURSE_LOCATION* wer-

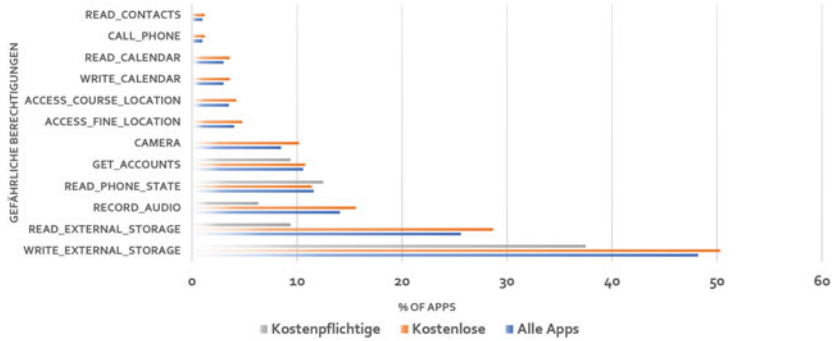


Abb. 11 Häufigkeit der angeforderten gefährlichen Berechtigungen

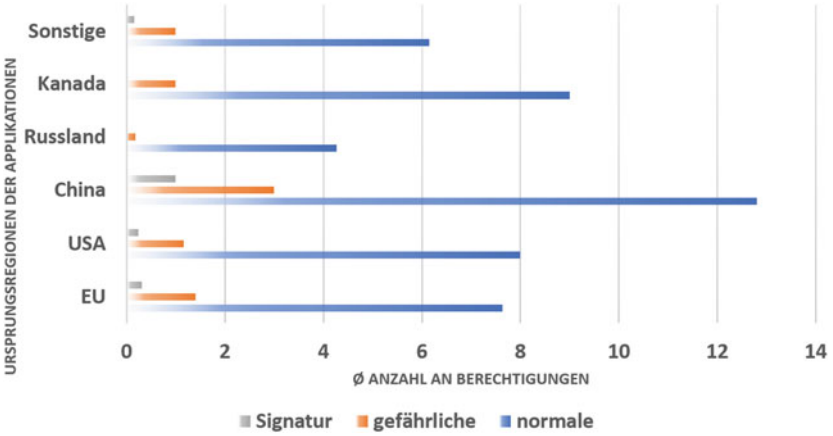


Abb. 12 Verteilung der durchschnittlichen Berechtigungen je Kategorie nach dem Google Berechtigungsmodell unter den Ursprungsregionen aller Apps

den für die Standortermittlung des Gerätes benötigt, sind jedoch nur von weniger als 5 % aller Learning Apps angefordert worden. Auffällig hierbei ist vor allem, dass Berechtigungen für die Nutzung der Standort-Funktion, Kamera- oder Kalenderinhalte von keiner der kostenpflichtigen Apps genutzt wird.

Berechtigungen & Ursprungsregionen Ein weiterer Teil unserer Analyse zielte auf den Vergleich zwischen einzelnen Ursprungsregionen aller Apps in Bezug auf die durchschnittlichen Berechtigungen in jeder Kategorie des Google Berechtigungsmodells für die 165 der 199 Apps, welche einer Ursprungsregion durch eine Angabe des Entwickler-Standorts zugeordnet werden konnten. Die Ergebnisse sind in Abb. 12 zusammengefasst. Hierbei wird deutlich, dass vor allem Apps aus den Regionen EU, Vereinigte Staaten und China mehr gefährliche und Signatur-Berechtigungen anfordern als die übrigen Ursprungsregionen. Sehr auffällig ist jedoch der Peak für alle drei Berechtigungskategorien in der Ursprungsregion China. Dieses Muster ist auch in den Top 10-Apps nach gefährlichen Berechtigungen erkennbar: zwei dieser Top 10-Apps weisen die Ursprungsregion China auf und 2 weitere liefern keinerlei Informationen zum Entwickler-Standort. Außerdem sind darunter 2 Apps enthalten, welche eine Datenschutzerklärung in der Sprache Französisch darlegen, obwohl im gesamten Datensatz der 199 Apps nur 3 Apps eine französische Datenschutzerklärung besitzen. In Abb. 13 sind nicht die Sprachen, sondern die Ursprungsregionen mit den gefährlichen Berechtigungen in Relation

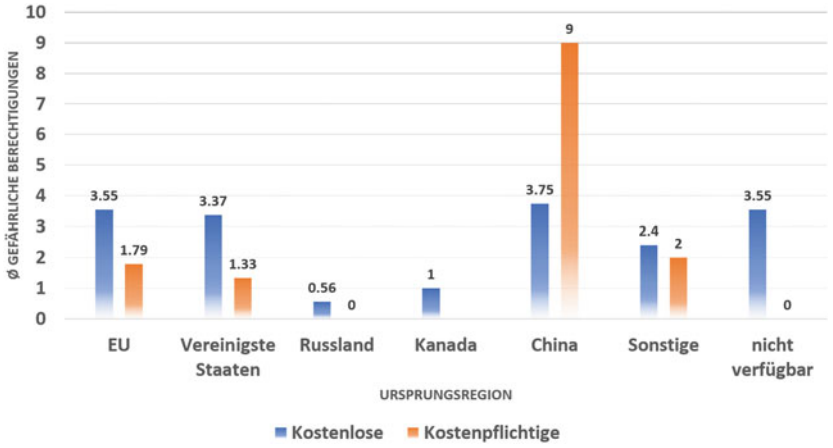


Abb. 13 Relation zwischen Ursprungsregion und zugehöriger Anzahl an gefährlichen Berechtigungen

gebracht worden. Hierbei stellen wir einen Peak bei der Ursprungsregion sowohl für die kostenlosen als auch kostenpflichtigen Apps fest. Learning Apps, deren Entwickler ihren Standort in China haben, scheinen mehr gefährliche Berechtigungen anzufordern als die übrigen Apps.

5.2 Third-party Library Analyse

Um Entwicklungs- und Wartungskosten für Apps gering zu halten, greifen Entwickler häufig auf Bibliotheken von Drittanbietern, die sog. Third-party Libraries, zurück. Mittels der Third-party Libraries ist es nicht nur möglich neue Funktionen in der App zu integrieren, sondern auch mit Werbung die Kosten aus Entwicklung und Wartung wieder einzunehmen. Eingeteilt werden können die Third-party Libraries in drei verschiedene Kategorien: Werbenetzwerke, soziale Netzwerken und Entwicklungswerkzeuge. Dies entspricht der Kategorisierung durch die Statistik-Webseite appbrain[12] Unsere Analyse baut ebenfalls auf Exodus Pri-

[12] AppBrain: Android library statistics. https://www.appbrain.com/stats/libraries. Stand: 06.07.2020.

vacy[13] auf. Dabei findet ein Abgleich zwischen der Library-Liste von Exodus mit ihren Code-Signaturen und einer Liste von eingebetteten Java-Klassennamen aus der untersuchten App statt, sodass ein positiver Vergleich die Existenz der Libraries in der Anwendung beweist. Folglich erhalten wir eine Liste aller Libraries, welche im Datensatz der 199 Apps verwendet worden sind, und wie oft die Information darüber, darin vorkommen. Die durchschnittliche Anzahl an Third-party Libraries in Learning Apps beträgt bei den kostenlosen etwa 4 und 1,6 bei den kostenpflichtigen. Die in den Apps verwendeten Libraries sollen nun genauer untersucht werden. Hierfür werden die von Exodus Privacy ausgegebenen Libraries aufgelistet und hinsichtlich ihrer Verteilung über alle Apps alysiert.

Top 25-Libraries unter allen kostenlosen und kostenpflichtigen Apps Da der Durchschnittswert für die Libraries bei etwa 4 liegt, ist es nicht verwunderlich, dass 60 % aller Apps 3 oder weniger Libraries verwenden. Circa 23 % der Learning Apps verwenden mehr als 5 Libraries. Das Auftreten der Top 25-Libraries in allen Apps wird in Abb. 13 prozentual untereinander verglichen. Wir gehen hierbei separat auf die kostenlosen und kostenpflichtigen ein. Besonders auffällig zeigen sich die Libraries von Google, welche mit 6 namenhaften Libraries wie Google Firebase Analytics oder Google Analytics in den Top 10 Libraries aufgelistet sind. Dies ist jedoch nicht verwunderlich, da Libraries von Google wie beispielsweise Firebase Analytics in etwa 61,4 % aller Android Apps enthalten sind. Die überwiegende Mehrheit der weites verbreitetsten Libraries werden von Internet Giganten angeboten. Erst die Libraries ab Platz Nummer 12 in Abb. 14 weisen einen anderen Namen als Google oder Facebook auf. Diese als nächsthäufigste verwendeten Libraries *Unity3dAds, Moat* und *AppLovin* werden genauso, wie Google Ads und Facebook Ads hauptsächlich für Werbeanzeigen benutzt. Aus unserer Analyse ist zu entnehmen, dass etwa 14 % aller Apps in unserem Datensatz Libraries für soziale Netzwerke benutzen. 38 % bzw. 48 % der Apps beinhalten Libraries für Werbeanzeigen bzw. Libraries für Entwicklungstools. Der hohe Anteil von Libraries der Kategorie Werbeanzeigen (etwa 38 %) deutet darauf hin, dass ein Großteil von Learning Apps dazu verwendet werden, um gezielt Werbung auf dem Gerät des Nutzers anzuzeigen. Die am häufigsten vertretene Kategorie sind jedoch die Entwicklungstools, welche in circa 48 % aller Apps in unserem Datensatz auftreten.

[13] Exodus Privacy: Trackers. https://reports.exodus-privacy.eu.org/en/info/trackers/. Stand: 06.07.2020.

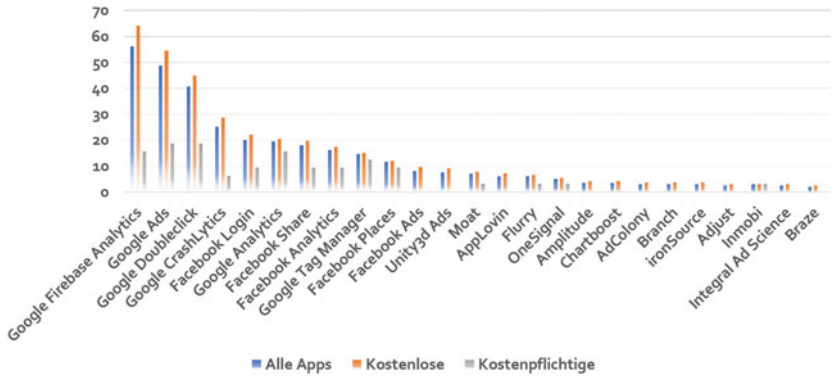


Abb. 14 Aufkommen der Top 25-Libraries unter allen kostenlosen und kostenpflichtigen Apps

Eingebettete Top 25-Libraries unter den Top 10-Apps nach Anzahl der Installationen Betrachten wir nun die Ergebnisse für die Top 10-Apps nach Installationen hinsichtlich ihrer eingebetteten Libraries, zusammengefasst in Tab. 3, so stellen wir fest, dass Libraries für Werbeanzeigen und Libraries für Entwicklungstools etwa gleichermaßen vertreten sind.

Der Schwerpunkt der am häufigsten benutzten Third-party Libraries liegt hauptsächlich bei den Top 4-Libraries von Google *(Google Firebase Analytics, Google Ads, Google Doubleclick* und *Google CrashLytics).*

Top 10-Apps nach meisten Third-party Libraries Zum Vergleich werden die Top 10-Apps nach Anzahl der eingebetteten Libraries in Tab. 3 dargestellt. Hierbei sind vor allem die Top 9-Libraries, welche den Unternehmen Google und Facebook zuzuschreiben sind, am häufigsten verwendet worden.

Top 10-Apps nach Anzahl der eingebetteten Libraries und korrespondierende Informationen bezüglich Datenschutzerklärung und Ursprungsregion Vergleichen wir die Apps mit und ohne Datenschutzerklärung hinsichtlich der durchschnittlichen Anzahl an eingebetteten Libraries, siehe Tab. 5, so stellen wir fest, dass Apps ohne Datenschutzerklärung weniger Libraries im Code enthalten als diejenigen mit einer Datenschutzerklärung. Diese in Abb. 15 illustrierten Ergebnisse lassen darauf schließen, dass Entwickler von Apps ohne Datenschutzerklärung dazu neigen, weniger Libraries zu verwenden. Wie bereits erläutert, können Libraries dazu eingesetzt werden, um nutzerbezogene Daten von der App zu erheben und abzuspei-

Tab. 3 Eingebettete Top 25-Libraries unter den Top 10-Apps nach Installationen. A1 – Duolingo; A2 – Photo-math; A3 – Google Classroom; A4 – Neuro Nation; A5 – Mathe Einmal-ein; A6 – Quizlet; A7 – Coursera: online courses; A8 – ABC Spiele; A9 – Class-Dojo; A10 – Mathe-Spiele

–	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10
Google Firebase Analytics	✓	✓		✓		✓	✓	✓	✓	✓
Google Ads	✓			✓	✓	✓		✓	✓	✓
Google Double-click				✓	✓			✓		✓
Google CrashLytics	✓	✓		✓		✓	✓		✓	
Facebook Login	✓	✓		✓		✓	✓			
Google Analytics				✓		✓				
Facebook Share	✓	✓		✓		✓	✓			
Facebook Analytics	✓			✓			✓			
Google Tag Manager				✓		✓				
Facebook Places	✓						✓			
Facebook Ads	✓									✓
Unity3d Ads						✓				
Moat						✓				
AppLovin						✓				
Flurry						✓				
OneSignal						✓				
Amplitude						✓				
Chartboost						✓				
AdColony						✓				
Branch						✓				
ironSource								✓		
Adjust	✓			✓						
Inmobi										
Integral Ad Science										
Braze						✓				

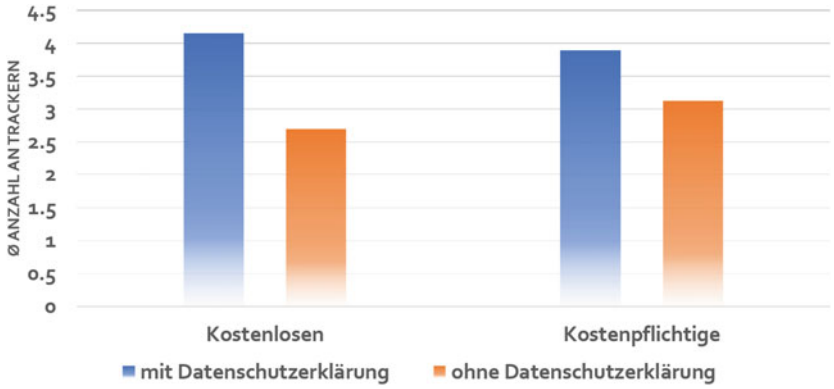


Abb. 15 Relation zwischen App mit und ohne Datenschutzerklärung bezüglich durchschnittlicher Anzahl an Trackern

chern, was gegen die Datenschutzrichtlinien verstoßen würde, falls die Entwickler dies nicht in einer Datenschutzerklärung dargelegt haben.

Auch bei den Top 10-Apps nach Libraries untersuchen wir, ob sie eine Datenschutzerklärung haben und welcher Ursprungsregion sie zugewiesen werden können. Die Ergebnisse hierzu sind in Tab. 4 abgebildet. Auch hier besitzen alle Apps eine Datenschutzerklärung, und diese sind bis auf eine französische Datenschutzerklärung in Deutsch bzw. Englisch verfasst. Bei den Ursprungsregionen sind jedoch einige Besonderheiten anzumerken: 3 Apps gehören der Ursprungsregionskategorie Sonstige an, wobei zwei davon dem Ursprungsland Indien und die übrige Apps Moldawien zuzuschreiben ist. Eine App gibt sogar keinerlei Informationen zum Entwickler-Standort an, sodass eine Ursprungsregion nicht abgeleitet werden kann. Die übrigen Apps stammen aus den Ursprungsregionen EU oder Vereinigte Staaten. Die Ursprungsregion der App scheint kaum Einfluss auf die Anzahl an eingesetzten Libraries zu haben.

5.3 Dynamische Code Analyse

In diesem Abschnitt sollen ausgewählte Learning Apps aus unserem Datensatz mittels einer werkzeugunterstützten dynamischen Codeanalyse unter die Lupe genommen werden. Die Vorgehensweise ergänzt die oben beschriebene statische Codeanalyse und zielt primär auf die Qualität des Quellcode, das Netzwerkverhalten und potenzielle Datenlecks in dem von einer App initiierten Datenaustausch über das Internet (Tab. 5).

Tab. 4 Eingebettete Top 25-Libraries unter den Top 10-Apps nach Anzahl der Libraries. A21 – Kinderzimmer Rätsel und Spiel; A22 – Neuro Nation; A23 – Kinder lernen zu schreiben; A24 – Einmaleins lernen & üben; A25 – Mathematik Logik spiele; A26 – Kostenlos Deutsch lernen mit FunEasy Learn; A27 – Skillshare Online Kurse; A28 – Homework Helper & Solver; A29 – M-Learningo; A210 – Kinderspiele f. Kinder

-	A21	A22	A23	A24	A25	A26	A27	A28	A29	A210
Google Firebase Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Google Ads	✓	✓	✓	✓	✓	✓		✓		✓
Google Double-click	✓	✓	✓	✓	✓			✓		✓
Google CrashLytics		✓		✓	✓	✓	✓	✓	✓	
Facebook Login	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Google Analytics		✓			✓	✓	✓	✓	✓	
Facebook Share	✓	✓	✓	✓	✓	✓	✓	✓		
Facebook Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Google Tag Manager		✓				✓	✓	✓	✓	
Facebook Places	✓	✓	✓				✓			
Facebook Ads				✓	✓	✓				
Unity3d Ads	✓		✓	✓	✓					✓
Moat	✓			✓						✓
AppLovin						✓				
Flurry	✓		✓			✓		✓		
OneSignal					✓	✓				
Amplitude						✓				
Chartboost				✓		✓				
AdColony	✓					✓				
Branch						✓				
ironSource					✓					✓
Adjust	✓									
Inmobi										✓
Integral Ad Science										✓
Braze						✓	✓			

Tab. 5 Top 10-Apps nach Anzahl der eingebetteten Libraries und korrespondierende Informationen bezüglich Datenschutzerklärung und Ursprungsregion

App-Name	Datenschutz-erklärung	Sprache	Ursprungsregion
Kinderzimmer Rätsel und Spiel	✓	Englisch	Sonstige (Indien)
NeuroNation	✓	Deutsch	EU
Kinder lernen zu schreiben	✓	Englisch	Sonstige (Indien)
Einmalleins lernen & üben	✓	Englisch	EU
Mathematik – Logikspiele	✓	Englisch	EU
Kostenlos Deutsch lernen mit FunEasyLearn	✓	Englisch	Sonstige (z. B. Moldawien)
Skillshare Online-Kurse	✓	Englisch	Vereinigte Staaten
Homework Helper & Solver	✓	Englisch	Nicht verfügbar
M-Learning	✓	Französisch	EU
Kinderspiele für Kinder ab 3	✓	Deutsch	Vereinigte Staaten

Hierbei soll eine typische Interaktion des Nutzenden mit der App mittels eines Emulators simuliert und der daraus resultierende Datenverkehr untersucht werden. Der von der App initiierte Datenaustausch über das Internet wird dabei abgefangen und hinsichtlich Datenschutz- und Datensicherheitsaspekten analysiert. Die gesammelten Datenpakete sollen Aufschluss darüber geben, wie personenbezogene und personenbeziehbare Daten durch die App verwendet bzw. an wen weitergeleitet werden. Das Hauptaugenmerk liegt dabei bei dem Einsatz von Third-party Libraries, Datenlecks in initiiertem Datenverkehr und (un)sichere Kommunikation. Aufgrund der Größe unseres Datensatzes ist eine solche feingranulare Analyse für alle 199 Apps nur mit enormen Zeitaufwand möglich. Wir beschränken daher den Umfang der zu analysierenden Apps auf 10 Kandidaten. Die Untersuchungsgegenstände für die werkzeugunterstützte dynamische Codeanalyse und korrespondierende Informationen bezüglich Datenschutzerklärung, Ursprungsregion und Installationen sind in Tab. 6 zusammengefasst.

5.3.1 Datenleaks

Bei dieser feingranularen Analyse soll die Vertraulichkeit der übermittelten Daten, welche potenziell auch persönliche Daten des Nutzers sein können, überprüft werden. Ob ein Datenpaket explizit eine persönliche Information enthält, kann nur eindeutig bestätigt werden, falls die Informationen als Klartext verschickt worden sind oder ein verschlüsseltes Datenpaket zuerst entschlüsselt und anschließend auf persönliche Daten untersucht wird. Um die verschlüsselte Übertragung von Daten

Tab. 6 Untersuchungsgegenstand für die dynamische Analyse

App-Name	Datenschutz-erklärung	Sprache	Ursprungsregion	Installationen (Mio.)
Duolingo	✓	Englisch	Vereinigte Staaten	100
Google Classroom	✓	Deutsch	Vereinigte Staaten	50
NeuroNation	✓	Deutsch	EU	10
Mathe-Einmaleins	✓	Englisch	Nicht verfügbar	10
Coursera: Online courses	✓	Englisch	Nicht verfügbar	10
Quizlet	✓	Deutsch	Vereinigte Staaten	10
Jitsi Meet	✓	Englisch	Nicht verfügbar	5
Mathematik-Logikspiele, Übungen für das Gehirn	✓	Englisch	EU	5
SoloLearn	✓	Englisch	Vereinigte Staaten	5
GeoGebra	✓	Englisch	Nicht verfügbar	5

zu verifizieren, untersuchen wir alle Datenpakete auf die benutzten Protokolle der Datenübertragung. Anhand des verwendeten Protokolls kann beurteilt werden, ob die Daten im Paket verschlüsselt oder als Klartext verschickt worden sind. Falls wir anhand der benutzten Protokolle verifizieren können, dass Daten sicher verschlüsselt übertragen werden, werden insofern Datenlecks nicht berücksichtigt. Daher stützen wir die Argumentation über Datenlecks im App-Datenverkehr auf eine Kombination zwischen dem von Razaghpanah et al. (2015) [7] vorgestellten App Lumen Privacy Monitor und den im Rahmen des Forum Privatheit entwickelten Tools, u. a. PISA Conrad/Simo (2018) [3]. Beide Tools ermöglichen es, Datenpakete lokal auf dem Nutzergerät zu untersuchen und Datenlecks aufdecken. Wir nutzen die Ergebnisse der Analyse durch Lumen Privacy Monitor und PISA, um potenzielle Datenlecks der untersuchten Apps in 3 Risikostufen zu unterteilen: niedriges, mittleres und hohes.

Niedriges Sicherheitsrisiko Unter den gefundenen Sicherheitslücken, welche ein niedriges Risiko für die persönlichen Informationen des Nutzers darstellen, fallen unter anderem Informationen zum Gerät des Nutzers oder etwa Verbindungseinstel-

lungen. Für die vorliegende Studie übernehmen wir die in Lumen Privacy Monitor vordefinierte Spezifikation von niedrigen Sicherheitsrisiken. Diese umfassen zum einen die Marke *(Brand),* das Modell und den Hersteller *(Device Model),* das Betriebssystem und die Android Version *(Build Fingerprint)* des verwendeten Gerätes. Außerdem stellt eine App ein geringfügiges Sicherheitsrisiko für die Daten des Nutzers dar, wenn sie Verbindungseinstellungen *(Connectivity)* einlesen kann. Alle untersuchten Apps weisen bei fast allen niedrigen Risiken einen positiven Befund durch Lumen Privacy Monitor auf.

Mittleres Sicherheitsrisiko Unter mittleren Sicherheitsrisiken werden Datenlecks wie *InstalledApps, Keyword:secret, UnprotectedLocationQueries* und *UntransparentCalenderAccess* zusammengefasst. Installed Apps definiert ein Risiko/ Bedrohung mittleren Grades, da die untersuchte Learning App Zugriff auf die übrigen auf dem Gerät installierten und aktuell ausgeführten Apps erhält und diese Informationen weiterleitet. Die so gewonnenen Informationen können von Entwicklern und Werbetreibenden genutzt werden, um u. a. Persönlichkeitsmerkmale zu inferieren Seneviratne et al. (2014) [9] und Personalisierung als Teil ihrer Marketing-Strategie umzusetzen. Zu den Apps mit dem Datenleck Installed Apps zählen *Duolingo* und *Mathematik – Logikspiele, Übungen für das Gehirn*. Die zweite Lücke *Keyword:secret* weißt auf das Vorhandensein des zuvor eingestellten Suchworts secret im Datenverkehr auf. Diese Tatsache wird als mittelschweres Datenleck ausgedrückt. Wir verwenden während der Simulation die Zeichenkette *„secret“* für Login-Daten bzw. Benutzernamen. Wenn also z. B. die Lumen App diese Zeichenkette im Datenfluss der untersuchten Learning-App ausfindig machen kann, so besteht die Gefahr, dass ein Angreifer ebenso eine solche sensitive Information aus dem Datenfluss ermitteln und ausnutzen kann. Daher stellt dies ein großes Risiko dar. Unter den zehn untersuchten Learning Apps könnte diese Problematik ausschließlich bei der App *JitsiMeet* festgestellt werden. Unter *UntransparentCalenderAccess* fassen wir Datenleaks zusammen, die dadurch entsteht, wenn die untersuchte App durch Query-Schnittstellen und ohne explizite Interaktion mit dem Nutzenden (z. B. Betätigung eines OK-Button) auf Kalendereinträge zugreifen kann. Bei einer der untersuchten Learning-Apps konnte dieses Datenleak festgestellt werden. *UnprotectedLocationQueries* weist auf das Risiko einer aus Sicht des Nutzenden unbeabsichtigen bzw. intransparenten Offenlegung von Standort- oder Web-Abfragedaten hin. Hier fokussieren wir insbesondere auf Leaks, die entweder durch unsichere Kommunikation mit (Dritt-)Dienstanbietern wie z. B. Google Maps oder einer Interpretation von WiFi- und Access-Point-Informationen wie z. B. die WiFi-MAC Adresse Cunche (2014) [4] entstanden sind. Unsere Befunde zeigen, dass 10 % der untersuchten Apps Google-Maps-Anfragen über unsichere Kanäle stellen.

Angreifer können dementsprechend Standort-Informationen aus den übermittelten Anfragen extrahieren. 30 % der Apps geben Details über WiFi- und Access-Point preis. Aggregiert betrachtet sind es 30 % der Apps die das *UnprotectedLocation-Queries* Risiko darstellen – d. h. die Möglichkeit bieten, unautorisiert auf Standorte zuzugreifen und Bewegungsprofile zu erstellen.

Hohes Sicherheitsrisiko Hohe Sicherheitsrisiken umfassen den Zugriff auf und die Weiterleitung von sensitiven Identifiers, welche Werbenetzwerken und Libraries die Möglichkeit gibt, den Nutzer über mehrere Anwendungen und Plattformen hinweg zu beobachten bzw. zu verfolgen. Dies stellt eine massive Beeinträchtigung der Privatsphäre dar, da der Nutzer dadurch zum Opfer von Tracking, Profilbildung und gezielter unerwünschter Werbeanzeigen werden kann. Die Hälfte der im Rahmen der dynamischen Analyse betrachteten Learning-Apps greifen und teilen mindesten einen eindeutigen Identifier (IMEI/MEID in 20 % der Fälle und MAC-Adresse in 30 % der Fälle). Darüber hinaus erfassen alle diese Apps zusätzlich die sog. *„Google advertising ID“,* eine Kennung für Werbetreibende, die es ihnen ermöglicht, die Werbeaktivitäten von Benutzern auf Android-Geräten anonym zu verfolgen. Ein Zugriff auf eindeutige Bezeichner, auch in Kombination mit der Advertising ID, stellt eine klare Verletzung der Google Play-Programmrichtlinien für Entwickler dar.[14]

5.3.2 Third-party Library-Analyse

Gemäß der EU-Gesetzgebung dürfen ohne elterliche Zustimmung keine Tracking-Aktivitäten bei Apps für Kinder stattfinden Stapf et al. (2021) [11]. In den USA werden ähnliche Anforderungen im Rahmen der COPPA (Children's Online Privacy Protection Act) US Congress (1998) [2] formuliert. Bei einigen der untersuchten Learning Apps, konnten keine Hinweise auf Google Play gefunden werden, die darauf abzielen, Eltern – oder den Nutzenden – über eine mögliche Tracking-Aktivität durch die App zu informieren. Im Durchschnitt beinhalten untersuchte Apps ca. 5,6 Third-party Libraries. Zu den am meisten angebundenen Drittparteien gehören *Google Firebase Analytics* (bei 90 % der Apps), *Google Tag Manager* (bei 90 % der Apps) und *Facebook* (bei 80 % der Apps). Unsere Ergebnisse bestätigen die zuvor im Rahmen der statischen Analyse gemachte Feststellung: in Learning Apps sind Third Party Libraries in hohen Maßen vorhanden, siehe Abschn. 5.2.

[14] https://support.google.com/googleplay/android-developer/answer/6048248?hl=de. Stand: 06.07.2020.

5.3.3 Sichere Kommunikation

Zielknoten Zunächst wollen wir die erfassten Zielknoten der einzelnen Verbindungen innerhalb des analysierten Datenflusses betrachten. Die meisten Zieladressen im Datenverkehr der untersuchten Apps liegen in den Vereinigten Staaten, wobei Deutschland am zweithäufigsten vertreten ist. Eine der untersuchten Learning Apps leitet Daten an einen sich in der Volksrepublik China befindlichen Server weiter. Ein Großteil der Apps in dieser Analyse leitet Daten zu IP-Adressen weiter, welche 6 oder weniger verschiedenen Organisationen zuzuordnen sind. Jedoch stechen die Apps *Mathe-Einmaleins, Quizlet* und *Coursera: online courses* besonders hervor, da sie IP-Verbindungen zu mehr als 9 verschiedenen Organisationen aufbauen. Nach unserer Analyse interagiert die App *Coursera* sogar mit mehr als 16 verschiedenen Organisationen.

Verwendete Sicherheitsprotokolle Wie die Ergebnisse der Untersuchung des Datenverkehrs durch Wireshark[15] zeigen, enthalten alle Apps Datenpakete in ihrem Datenfluss, welche das Verschlüsselungsprotokoll Transport Layer Security (TLS) verwenden. Lediglich eine App zeigt Anfälligkeiten und zwar in Bezug auf einen fehlerhaften benutzerdefinierten SSL/TLS-Vertrauensmanager. Hier wurde die Vertrauensverwaltung für Socket-Kommunikation auf unsichere Weise modifiziert. Durch die Anwendung des TLS-Protokolls wird sowohl die Verschlüsselung der übermittelten Daten als auch deren Integrität gewährleistet. Betrachtet man die Verteilung von TLS-Datenpaketen innerhalb des analysierten Datenverkehrs der Apps, so stellen wir fest, dass im Durchschnitt etwa 33 % des Datenflusses in den populärsten Apps mit TLS verschlüsselt ist. Die Abb. 16 stellt die Verteilung der TLS Datenpakete aller untersuchten Apps prozentual dar. Die Apps *Google Classroom* und *JitsiMeet* fallen hierbei besonders auf, da mehr als 50 % des Datenverkehrs mittels TLS verschlüsselt übertragen worden ist. Unter den übrigen Apps wie etwa *NeuroNation, Mathe–Einmaleins* oder *Coursera: online courses* weisen die Apps aber nur weniger als 20 % verschlüsselten TLS-Datenverkehr auf. Gehen wir näher auf die verwendeten TLS-Protokolle ein, so stellen wir fest, dass die Apps hauptsächlich TLS in der Version 1.2 (v1.2) bzw. Version 1.3 (v1.3) benutzen, wobei v1.3 eine neuere und damit fortschrittlichere Version darstellt. In TLS v1.3 wurden einige Sicherheitslücken, welche in der älteren Version 1.2 auftreten, behoben. Betrachten wir die Verbreitung der besser gesicherten TLS v1.3, so stellen wir fest, dass 6 der 10 untersuchten Apps weniger als 1 % des Datenflusses mit dieser TLS Version absichern. Die TLS Version 1.2 hingegen weist im Durchschnitt etwa 28 %

[15] Wireshark. https://www.wireshark.org/. Stand: 06.07.2020.

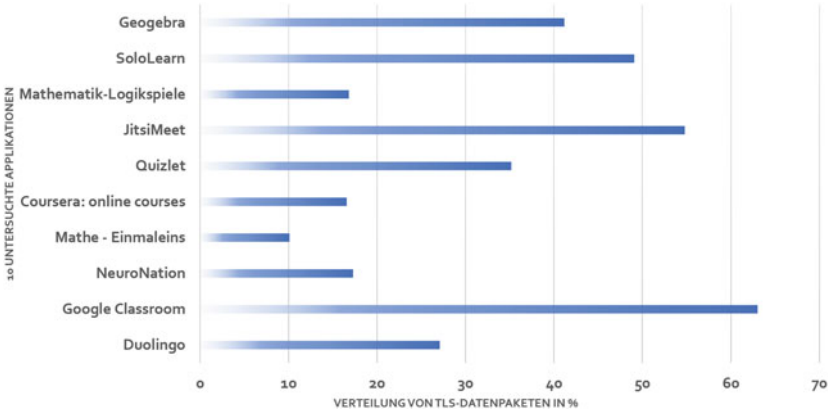


Abb. 16 Aufkommen von TLS-Datenpaketen im gesamten Datenfluss während der Datenverkehrsanalyse der untersuchten Apps

des gesamten Datenflusses auf und ist somit weitaus öfter vertreten als die neuere Version. Obwohl die untersuchten Apps zu den populärsten in unserem Datensatz gehören, so verwenden die Verbindungen dennoch nur selten die TLS v1.3, welche bereits seit 2018 veröffentlicht ist und dem Stand der Technik entspricht.

6 Fazit

Learning Apps gelten inzwischen als wichtige Instrumente zur Bereitstellung schulischer und außerschulischer Bildungsangebote und zur Vermittlung grundlegenden Wissens an Kinder und Jugendliche. Durch Learning Apps können Lernangebote personalisiert und interaktive Lernmethoden bereitgestellt werden. Diese können wiederum jederzeit und von überall konsumiert werden. Eine derartige Digitalisierung des Lern- und Wissensvermittlungsprozesses geht jedoch mit der Notwendigkeit einher, die damit verbundenen Risiken für die informationelle Selbstbestimmung und die Sicherheit der Daten der Minderjährigen zu erkennen und einzuordnen.

Die vorliegende Arbeit untersuchte, inwieweit Learning Apps privatheitinvasiv und anfällig für Cyber-Angriffe sind. Unsere umfassende Analyse von 199 Android Learning Apps belegt, dass ein signifikanter Anteil der untersuchten Apps zahlreiche Anfälligkeiten hinsichtlich Datenschutz und Cybersicherheit aufweisen. Mit den Ergebnissen unserer Studie zielen wir darauf ab, Pädagogen, Minderjährige,

Datenschutzbehörden, Verbraucherschutzorganisationen und App-Entwickler über Datenschutz- und Cybersicherheitsproblematiken im Zusammenhang mit Learning Apps zu sensibilisieren.

Literatur

1. Article 29 Working Party: Guidelines on transparency under Regulation 2016/679. WP260 rev.01. Brussels (2016). https://ec.europa.eu/newsroom/article29/redirection/document/51025
2. Commission, F.T., et al.: Children's online privacy protection rule ("coppa"). Retrieved on September **16** (2016)
3. Conrad, B., Simo, H.: Pisa - towards detecting tracking services via privacy-preserving mobile traffic analysis. Forum Privatheit Tech, Report (2018)
4. Cunche, M.: I know your mac address: targeted tracking of individual using wi-fi. J. Comput. Virol. Hack. Tech. **10**(4), 219–227 (2014)
5. Ehmann, E., Selmayr, M. (Hrsg): Datenschutz- Grundverordnung. Kommentar. 2. Aufl. C.H. Beck, München (2018)
6. Kühling, J., Buchner, B. (Hrsg): Datenschutz- Grundverordnung/BDSG. Kommentar. 2. Aufl. C.H. Beck, München (2018)
7. Razaghpanah, A., Vallina-Rodriguez, N., Sundaresan, S., Kreibich, C., Gill, P., Allman, M., Paxson, V.: Haystack: In situ mobile traffic analysis in user space. arXiv preprint arXiv:1510.01419 S. 1–13 (2015)
8. Roßnagel, A.: Der Datenschutz von Kindern in der Datenschutz-Grundverordnung - Vorschläge für die Evaluierung und Fortentwicklung. Zeitschrift für Datenschutz **9**(2), 88–92 (2020)
9. Seneviratne, S., Seneviratne, A., Mohapatra, P., Mahanti, A.: Predicting user traits from a snapshot of apps installed on a smartphone. ACM SIGMOBILE Mobile Comput. Commun. Rev. **18**(2), 1–8 (2014)
10. Simitis, S.; Hornung, G.; Spieker genannt Döhmann, I. (Hrsg.): Datenschutzrecht (DSGVO mit BDSG). Kommentar. Nomos, Baden-Baden (2019)
11. Stapf, I., Meinert, J., Heesen, J., Krämer, N., Ammicht Quinn, R., Bieker, F., Friedewald, M., Geminn, C., Martin, N., Nebel, M., Ochs, C.: Privatheit und kinderrechte. Schriftenreihe Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt, Karlsruhe S. 24 (2020)
12. Tengler, K., Schrammel, N., Brandhofer, G., Sabitzer, B.: Lernen auf distanz während der corona-krise. chancen und herausforderungen des distance learning für die primarstufe. In: Bildung und Digitalisierung, S. 195–216. Nomos Verlagsgesellschaft mbH & Co. KG (2020)

„das braucht die Technik nicht alles zu wissen“ – Digitale Datenerfassung im Spannungsfeld zwischen Privatheit, Datenschutz und gesellschaftlichem Auftrag

Diana Schneider

Zusammenfassung

Die Teilhabeplanung für Menschen mit Behinderung ist ein Instrument der Eingliederungshilfe, um soziale Partizipation und gleichberechtigte Teilhabe am Leben in der Gesellschaft zu fördern sowie die individuelle Selbstbestimmung zu ermöglichen. Im vorliegenden Beitrag wird auf Basis von 20 leitfadengestützten Interviews mit Personen aus dem Feld der Eingliederungshilfe dargelegt, wie die Praxis des Dokumentierens aussieht und unter welchen Umständen ggf. Informationen der Menschen mit Behinderungen zurückgehalten, d. h. nicht digital notiert werden. Dies soll Aufschluss darauf geben, welches Konzept von Privatheit die interviewten Personen vertreten. Zudem werden die Ergebnisse hinsichtlich der Datenschutzprinzipien diskutiert.

Schlüsselwörter

Privatheit • Digitale Dokumentationssysteme • Soziale Organisationen

D. Schneider (✉)
FH Bielefeld University of Applied Sciences, Bielefeld, Deutschland
E-Mail: Diana.Schneider@fh-bielefeld.de

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

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_12

1 Einleitung

Die Teilhabeplanung ist ein Instrument zur Feststellung des individuellen Bedarfs einer Person im Rahmen der Eingliederungshilfe für Menschen mit (drohender) Behinderung. Ziel der Eingliederungshilfe ist es, die leistungsberechtigten Personen mithilfe von Sozialleistungen so zu befähigen, dass diese „ihre Lebensplanung und -führung möglichst selbstbestimmt und eigenverantwortlich wahrnehmen" können [§ 90 Abs. 1 SGB IX n. F.]. Um geeignete Maßnahmen und Vorgehen für die potenziellen Leistungsberechtigten zu bestimmen, müssen daher zunächst innerhalb des Antragsverfahrens die individuellen, gesellschaftlichen Teilhabebeschränkungen umfänglich dargelegt werden. Häufig werden in diesem Zusammenhang nicht nur die „systematische[n] Arbeitsprozesse und standardisierte[n] Arbeitsmittel (Instrumente)" [§ 13 Abs. 1 SGB IX n. F.] zur Feststellung des individuellen Bedarfs der Person[1], sondern auch der zyklische Prozess als solcher als Teilhabeplanung bezeichnet. Die doppelte Bedeutung des Wortes ist in diesem Zusammenhang zu betonen, denn der individuelle Bedarf einer Person ist je nach ihren Fortschritten und Lebenszielen stetig neu zu ermitteln, um die jeweiligen Sozialleistungen anzupassen.

Im Rahmen des interdisziplinären Projekts MAEWIN[2] (2018–2021) wird u. a. analysiert, wie die aktuelle Praxis des Dokumentierens innerhalb sozialer Organisationen aussieht. Zwischen Januar und Juni 2020 wurden daher insgesamt 20 leitfadengestützte Interviews mit Personen aus dem Feld der Eingliederungshilfe geführt. Im Zuge der Erhebung wurde deutlich, dass die Problematik der Privatsphäre der Menschen mit (drohender) Behinderung eine entscheidende Rolle spielt. Denn die im Rahmen der Dokumentation erhobenen Daten gehören i. d. R. zu der Kategorie besonderer personenbezogener Daten, denen ein hohes Schutzniveau zugesprochen wird [19]. Gleichzeitig spielt der Datenschutz innerhalb der Praxis Sozialer Arbeit „eine ambivalente und somit wenig klare Rolle" [19, S. 414]. So ist nach Pudelko und Richter [19] zwar ein Bewusstsein für die Notwendigkeit der Umsetzung rechtlicher Rahmenbedingungen zum Schutz personenbezogener Daten vorhanden, die nicht zuletzt durch die europäische

[1] Es gibt kein bundeseinheitliches Instrument zur Ermittlung des individuellen Bedarfs einer Person. Stattdessen haben sich je nach Bundesland und Rehabilitationsträger verschiedene Praktiken, Verfahren und Instrumente etabliert haben.

[2] Das Projekt MAEWIN ist eines von sechs Tandem-Promotionsprojekten im Rahmen des Verbundprojekts NRW Digitale Gesellschaft und an der FH Bielefeld University of Applied Sciences (Fachbereich Sozialwesen, Prof. Dr. Seelmeyer) und der Universität Bielefeld (Technische Fakultät, Prof. Dr. Cimiano) angesiedelt.

Datenschutz-Grundverordnung (DSGVO) an Relevanz erhalten haben, doch verbindet sich damit auch die Herausforderung, wie genau diese Anforderungen in der Praxis umgesetzt werden können. Denn mit der Anwendung der DSGVO werden Personen adressiert, die zu einer informierten Einwilligung fähig sein sollen; eine Annahme, die im Tätigkeitsfeld Sozialer Arbeit nicht überall vorausgesetzt werden kann. Sozialarbeiterisches Handeln versucht daher, diese Diskrepanz mittels ihres Doppelmandates aufzufangen: indem sich die Fachkräfte nicht nur dem Staat als Geld- und Auftraggeber gegenüber verpflichtet sehen, sondern sich auch an den Bedürfnissen und Bedarfen ihrer Adressatinnen und Adressaten orientieren [vgl. 7, S. 47]. Beispielsweise, indem Privatheitsbedürfnisse vulnerabler Personen wie im Rahmen der Teilhabeplanung nicht nur gegenüber Dritten, sondern auch organisationsintern geschützt werden. So deuten die Ergebnisse aus den 20 Interviews darauf hin, dass die interviewten Personen ein differenzielles Verständnis von Privatheit vertreten, welches sich auch im Umgang mit der Dokumentation niederschlägt. Im vorliegenden Beitrag werden daher zunächst die Funktionen sowie Leerstellen von Dokumentation sozialer Organisationen herausgearbeitet. Gerade, weil die Nutzung von Daten sozialer Organisationen durch andere Berufsgruppen (bspw. IT-Entwicklerinnen und IT-Entwickler) innerhalb Deutschlands noch am Anfang steht, sollen die Ergebnisse auch dafür genutzt werden, um für das Verständnis von Privatheit in diesem Anwendungsfeld zu sensibilisieren.

2 Einblicke in die Daten und die Dokumentationspraxis

Zunehmend, wenn auch noch nicht umfassend und flächendeckend, erfolgt die Dokumentation innerhalb sozialer Organisationen Deutschlands in digitalen Dokumentationssystemen (oftmals auch Fachsoftware bzw. digitale Fachverfahren genannt). Diese IT-gestützten Verfahren beinhalten sowohl lokal-gebundene als auch webbasierte Lösungen der Dokumentation [vgl. 17]. Mit Blick auf IT-basierte Anwendungen für die Sozialwirtschaft[3] lässt sich feststellen, dass eine Vielzahl an Systemen und Verfahren existieren, welche teils durch eigenkonstruierte Softwarelösungen einzelner Organisationen ergänzt werden [11, 12]. Während das Für und Wider solcher digitalen Verfahren in der Literatur bereits stark diskutiert wird [vgl. 10, 12, 13, 15, 17, 18], fällt der Blick vergleichsweise selten auf die intendierten Leerstellen solcher Dokumentationen. Also auf das, was nicht dokumentiert wird, obwohl es bekannt und für den weiteren Verlauf relevant ist. Im Folgenden soll daher der Versuch unternommen werden, nach

[3] Siehe hierzu: https://social-software.de/.

vorhandenen und nicht-vorhandenen Daten der Dokumentation zu unterscheiden. Hierbei ist zu berücksichtigen, dass die Grenzen zwischen dem, was notiert wird, und dem, was fehlen könnte bzw. fehlt, durchaus fließend sind.

Basis der vorliegenden Ergebnisse stellen die zwischen Januar und Juni 2020 geführten, leitfadengestützten Interviews mit 20 Personen aus dem Feld der Eingliederungshilfe dar. Die interviewten Personen arbeite(te)n entweder bei einem Leistungserbringer oder einem Leistungsträger der Sozialhilfe oder Eingliederungshilfe[4] in Nordrhein-Westfalen oder Berlin und waren zum Zeitpunkt des Interviews zwischen 29 und 63 Jahren alt; einige Personen übernehmen Führungsaufgaben[5].

2.1 Vorhandene Daten

Zunächst wird auf diejenigen Daten eingegangen, die im Rahmen der Eingliederungshilfe in digitalen Dokumentationssystemen festgehalten werden und für mögliche Datenanalysen bspw. im Rahmen algorithmischer Verfahren zur Verfügung stehen würden. Insbesondere im zweiten Teil werden zudem Ergebnisse aus den Interviews thematisiert und mit vereinzelten Zitaten aus den Interviews unterlegt.

2.1.1 Daten (in) der Teilhabeplanung

Da die Teilhabeplanung als Verfahren und Instrument der Eingliederungshilfe den gesetzlichen Regelungen derselben unterliegt, lassen sich die notwendigen Kriterien für eine „individuelle und funktionsbezogene Bedarfsermittlung“ sowie deren Dokumentation und Nachprüfbarkeit dem dazugehörigen Gesetzestext entnehmen [§ 13 Abs. 2 SGB IX n. F.]; diese sollen insbesondere erfassen,

1. ob eine Behinderung vorliegt oder einzutreten droht,
2. welche Auswirkungen die Behinderung auf die Teilhabe der Leistungsberechtigten hat,
3. welche Ziele mit Leistungen zur Teilhabe erreicht werden sollen und

[4] In den Interviews wurde sich vornehmlich auf Leistungen zur Sozialen Teilhabe [vgl. § 90 Abs. 5 SGB IX n. F.] konzentriert. Dies beinhaltet bspw. Unterstützung im Wohn- und Sozialraum sowie Leistungen zur Mobilität.

[5] Aus Gründen der zugesicherten Anonymität gegenüber den interviewten Personen wird von einer detaillierteren Beschreibung der interviewten Personen und der Zuordnung der im Folgenden genannten Zitate zur jeweiligen Person bzw. Personengruppe abgesehen.

4. welche Leistungen im Rahmen einer Prognose zur Erreichung der Ziele voraussichtlich erfolgreich sind.

Ausgehend von dieser Bestimmung werden im Rahmen der Teilhabeplanung neben sozialrechtlich relevanten Daten einer Person zur Abwicklung des Antrags, auch besondere, personenbezogene Daten wie medizinische Diagnosen und (fach-) ärztliche Gutachten sowie Berichte (bspw. Arztbriefe, Krankenhausunterlagen) über die (drohende) Behinderung eines Menschen erfasst. Hierbei kommt es weniger auf die medizinische Diagnose gemäß der aktuellen *International Statistical Classification of Diseases and Related Health Problems* (ICD) an sich, sondern vielmehr auf die Wesentlichkeit der Einschränkung von Teilhabe aufgrund dieser medizinisch festgestellten Behinderung an. Häufig wird in diesem Zusammenhang daher von der „wesentlichen Behinderung“ gesprochen [2]. Eine wesentliche Behinderung liegt dann vor, wenn die körperliche, geistige oder seelische Behinderung so gravierend ist, dass die Menschen mit diesen Behinderungen „in *erheblichen* Umfange in ihrer Fähigkeit zur Teilhabe am Leben in der Gemeinschaft eingeschränkt sind“ [2, S. 5, Hervorhebung im Original]. Für die Bestimmung der wesentlichen Behinderung müssen daher neben den medizinischen Diagnosen auch die „resultierenden Beeinträchtigungen der funktionalen Gesundheit“ bekannt sein [2, S. 7]. Spätestens mit Inkrafttreten des Bundesteilhabegesetzes (BTHG, 2017–2023) soll sich hierfür an der *International Classification of Functioning, Disability and Health* (ICF) orientiert werden [§ 118 Abs. 1 SGB IX n. F.][6].

Zum Nachweis dieser Wesentlichkeit bedarf es je nach Art der Behinderung und Einschränkung der Teilhabe unterschiedlicher Dokumente. Im Rahmen der geführten Interviews wurde deutlich, dass dies trotz aller Individualität jedes Falls u. a. die folgenden Datensätze umfasst: detaillierte Beschreibung über die Fähigkeiten, Fertigkeiten, Ressourcen und Vorlieben eines Menschen sowie über (außer-)häusliche Probleme, Barrieren und Herausforderungen, welche die Person in ihrem Alltag beeinflussen. Darüber hinaus gibt es biografische Berichte zur Person, ihrer aktuellen Lebenssituation und ihrer (bisherigen) Lebensentwicklung. Diese liegen i. d. R. in Form von (Selbst-)Beschreibungen vor und werden durch fachliche Stellungnahmen bspw. der Bezugsbetreuungen ergänzt und eingeordnet. Diese fachlichen Stellungnahmen sind dann besonders wichtig, wenn die betreffenden Personen ihre Bedarfe nicht direkt formulieren (bspw.

[6] Auf die Überlegungen und auch Kritikpunkte, die sowohl mit dem Bundesteilhabegesetz als auch an der Orientierung der ICF einhergehen, wird in diesem Beitrag nicht eingegangen.

aus Schamgefühl) oder, wie im folgenden Interviewzitat, wenn die bezugsbetreuenden Personen bestimmte Wünsche und Ideen hinter getätigten Aussagen und Wünschen vermuten, jene jedoch unausgesprochen bleiben:

> „Wenn Klienten sagen: Ich will eine Familie gründen, aber nicht wirklich verstehen, was das eigentlich heißt, was damit verbunden ist. Aber sie verbinden damit ein Gefühl. […] Und dann […] zu entwickeln, was verbindet sich hinter diesem Gefühl?"

Mittels der Informationen und Interpretationen sowie weiteren Daten werden Förderungsschwerpunkte identifiziert und geplante Fern- und Nahziele mit den sie betreffenden Personen definiert. Diese werden mit sogenannten Maßnahmen bzw. Vorgehen hinterlegt und konkretisiert. Das sind bspw. inhaltliche Verabredungen darüber, was in Zukunft umgesetzt werden soll, welcher Zeitbedarf dafür veranschlagt wird und ggf., ob die Unterstützung in Form einer Fachleistungsstunde oder einer Assistenzleistung erbracht werden könnte. Auch diese Daten werden meist im Rahmen des Instruments zur individuellen Bedarfsermittlung erfragt, definiert und festgehalten. Sofern es sich bei dem Teilhabeplan nicht um einen Erstantrag handelt, kann zudem auf vergangene Maßnahmen, Vorgehen und Ziele sowie auf die zur Verfügung gestellten Ressourcen (d. h. Anzahl und Umfang der bewilligten Leistungen zur Teilhabe) Bezug genommen und diese hinsichtlich ihrer Angemessenheit zur Erreichung der definierten Ziele bewertet werden.

2.1.2 Die Frage nach Relevanz und Subjektivität

Neben dem Instrument zur Ermittlung des individuellen Bedarfs einer Person werden bei den Leistungserbringern und Leistungsträgern der Sozialhilfe und der Eingliederungshilfe weitere Daten und Informationen festgehalten. Das Dokumentieren innerhalb sozialer Organisationen ist dabei kein Selbstzweck, sondern dient bestimmten Funktionen [6, 16]. Merchel und Tenhaken [17, S. 171 f.] benennen sechs Intentionen, die mit Dokumentation einhergehen können:

- als Tätigkeitsbeleg – entweder als einfacher Nachweis für ein tatsächliches Handeln oder in Form eines legitimatorischen Nachweises korrekt erbrachter, im Sinne einer vorherigen Handlungsanweisung realisierten Leistung […];
- als Dokument zur Absicherung in Situationen, die künftig möglicherweise eine Rekonstruktion des Handelns in legitimatorischer Absicht erfordern […];
- zur Planung und Steuerung von Hilfen […];
- als Strukturierungs- und Bewertungshilfe für eine intensive fachliche Auseinandersetzung mit dem Verlauf und den Ergebnissen von Hilfen […];

- als Grundlage für (möglicherweise künftig erforderliche) gutachterliche Stellungnahmen gegenüber Gerichten […];
- oder als Grundlage für (qualitative) Evaluation […].

Auffallend ist, dass der Blick in die unsichere Zukunft und die Unwissenheit, ob dort bestimmte Informationen benötigt werden *könnten,* eine zentrale Leitfrage im Dokumentationsprozess einnimmt. Fehlen in den Einrichtungen und sozialen Organisationen klare Kriterien bzw. festgelegte Dokumentationsroutinen [20] oder werden diese als unzureichend wahrgenommen, liegt die Bestimmung der Relevanz bestimmter Informationen im individuellen Ermessen der dokumentierenden Personen [vgl. auch 1, 24]. Exemplarisch werden folgend drei Kriterien zur Beurteilung der Relevanz vorgestellt[7].

Zum einen kann die Relevanz einer Information mit Verweis auf einen *impliziten und/oder expliziten Handlungsauftrag* innerhalb der Betreuung begründet werden. Die neuen Informationen haben dann direkte Auswirkung auf die Gestaltung der fachlichen Arbeit und sind entsprechend als Nachweis oder zur Rekonstruktion des Falls zu notieren. In knapp der Hälfte aller Interviews wurde hierbei die Zweckgebundenheit der Dokumentation zum direkt vorliegenden Betreuungsauftrag betont. Das folgende Interviewzitat verdeutlicht jedoch, dass die Abwägung beileibe nicht immer eindeutig ist und der implizite Handlungsauftrag auch als ein zukünftiger verstanden werden kann:

> „Wenn sich ein Klient verliebt, ist das eine sehr, sehr persönliche Geschichte. Wenn der mir das anvertraut: Habe mich da verliebt. Dann ist das zu dokumentieren, wenn sich darauf ein Unterstützungsbedarf ergibt. Wenn das aber nicht relevant ist/ wobei, bei diesem Thema hat es an vielen Stellen Relevanz.“

Zum anderen können bestimmte *Hintergrundinformationen* (ggf. in Verbindung mit ihrem Neuheitswert) als relevant eingestuft werden. Dies betrifft neben allgemeinen Informationen des täglichen Arbeitens, bspw. Absprachen mit den Angehörigen oder Veränderungen der Wohnsituation, mitunter auch intime Informationen der betroffenen Personen, die diese unter Umständen nicht dokumentiert sehen möchten. Im Rahmen des Abwägens wird dann nicht nur entschieden, ob diese Informationen so wichtig sind, dass sie dennoch notiert werden (und dies gegenüber der betroffenen Person transparent gemacht wird), sondern auch, ob diese Informationen im Zweifelsfall sogar gegen den ausdrücklichen Willen der

[7] Die idealtypische Abgrenzung der Kriterien lässt sich in der Praxis nicht durchhalten, da das Festhalten bestimmter Aspekte auch pluralistisch motiviert sein kann.

Personen (und mitunter ohne deren Kenntnis) an Dritte weitervermittelt werden, wie das folgende Zitat zeigt:

> „Das hört sich jetzt ganz böse an, weil eigentlich ist das ein Vertrauensmissbrauch des Bezugsbetreuers gegenüber den Menschen mit Behinderung. Wenn er uns Dinge mitteilt, wo der Leistungsberechtigte nicht möchte, dass wir sie wissen. Aber diese Aussagen sind so wichtig, weil wir sonst bestimmte Dinge nicht verstehen. Weil das sind ja die unausgesprochenen Lücken."

Die letzten beiden Interviewzitate geben einen ersten Hinweis darauf, dass die Beurteilung der Relevanz unter Umständen eng mit der (gewährten) Privatheit gegenüber derjenigen Person verbunden ist, die diese Informationen betrifft. Wird eine Relevanz für den Fall festgestellt, kann die Wahrung der Privatheit von Menschen mit (drohender) Behinderung demnach zweitrangig werden. In extremen Fällen kommt es sogar zu einer Datenweitergabe, obgleich die betreffende Person dieser (ausdrücklich) nicht zugestimmt hat. Für den letzten Fall lassen sich dabei durchaus berechtigte Gründe anführen, bspw. bei Gefahr in Verzug oder geregelten Schweigepflichtentbindungen bei drohendem Schaden für die betroffene Person bzw. Dritte.

Zum dritten können Informationen Relevanz bekommen, wenn sich die dokumentierende Person im Sinne ihres *professionellen Verständnisses* dazu verpflichtet sieht, bestimmte Aspekte, Beobachtungen oder Interpretationen festzuhalten. Dies trifft dann zu, wenn die organisationsintern vereinbarten, IT-gestützten Dokumentationsroutinen als unvollständig, unpassend oder unklar wahrgenommen werden [8]. In diesen Fällen werden, wenn möglich, die vorhandenen Dokumentationsmöglichkeiten hinsichtlich eigener Ansprüche an Fachlichkeit angepasst oder umgangen, indem bspw. bestimmte Beobachtungen in anderen digitalen Eingabefeldern oder separat notiert werden.

> „Ja, wir haben dieses Standardprotokoll, was jeder […] ausfüllt. Die sehen auch alle gleich aus. Wenn es dazu ein Gespräch gab, dann gibt es dazu immer noch ein Blanko-Bogen. Weil dieses Protokoll, diese Möglichkeit, dass man da ein Gespräch aufnehmen kann oder Sachen festhalten kann, eben so nicht hergibt. Da muss man einfach erfinderisch sein."

Die Beurteilung der Relevanz kann also verschiedenen Gründen folgen und wird im Zweifelsfall subjektiv entschieden. Die Subjektivität wird auch in den Interviews mehrfach thematisiert; so nimmt bspw. das individuelle (Lebens- und Berufs-)Erfahrungswissen eine wichtige Rolle innerhalb der professionellen Arbeit ein. Eine Dokumentation gibt damit gleichsam „Auskunft […] über

die Sichtweise und die Interpretationen der dokumentierenden Person(en), über ihre (selektiven) Wahrnehmungen, über ihre Selbstdarstellungsbedürfnisse, ihre Interessen, ihre Kategorien und »theoretischen« Denkmuster“ [17, S. 172]. Ihre Betonung stellt damit an mancher Stelle auch eine Abgrenzung zur Objektivität und Standardisierung[8] dar, die dem professionellen Verständnis der Sozialen Arbeit, nämlich der ganzheitlichen Betrachtung des individuellen Falls [9] nicht gerecht zu werden scheinen und stattdessen mit der „Gefahr von Reduktion und Verfälschung komplexer Lebenswelten“ einhergingen [17, S. 184].

Gleichzeitig hat die Wertschätzung der Klientinnen und Klienten einen hohen Wert innerhalb des professionellen Verständnisses der Sozialen Arbeit. Diese Wertschätzung soll sich zwar nach Ansicht der interviewten Personen auch in der Dokumentation selbst niederschlagen, dies ist jedoch nicht überall gelebte Praxis, wie das folgende Zitat verdeutlicht:

> „Und, es sind immer menschliche Urteile. (…) Und die können auch einmal richtig gemein, falsch, unprofessionell, unflätig sein. Erlebe ich auch. (…) Also, die Anforderung ist: Die müssen professionell sein. Verantwortlich.“

Dieser Punkt ist in zweifacher Hinsicht interessant: Zum einen macht er deutlich, dass der Anspruch an und Praxis der Dokumentation nicht zwingend übereinstimmen. Folglich enthalten die nach Merchel und Tenhaken [17] in der Dokumentation dargestellten Sichtweisen und Wahrnehmungen einer Person eben auch deren Schattenseiten wie Vorurteile, einseitige Perspektiven oder versteckte Verzerrungen [3, 22]. Zum anderen verweist die Anforderung bei konsequenter Umsetzung nicht nur auf die angestrebte Wertneutralität (in) der Dokumentation, sondern auch auf eine bestimmte Sprachpraxis (bis hin zu einer ggf. „positiven Verzerrung“ der dokumentierten Inhalte). Diese können sowohl innerhalb eines eigenen Arbeitsbereiches als auch besonders durch professionsfremde Personen fehlinterpretiert werden. So wurde in zwei Interviews angemerkt, dass bestimmte Wörter (bspw. das Wort *„Begleitung“*) oder Perspektiven der Dokumentation durch das Gegenüber anders interpretiert werden (könnten) als beabsichtigt.

[8] Auf den Aspekt der Standardisierung soll an dieser Stelle nicht vertiefend eingegangen werden, da sich hieran eine eigene Diskussion innerhalb der Sozialen Arbeit anschließt. Für den vorliegenden Beitrag sei lediglich vermerkt, dass eine Standardisierung (in) der Dokumentation durch die interviewten Personen nicht einheitlich bewertet wurde.

2.2 Nicht-vorhandene Daten

Während die Frage, was alles dokumentiert wird, mit Blick auf die rechtlichen Anforderungen von Dokumentation und die Dokumentationsroutinen sozialer Einrichtungen recht umfassend beantwortet werden kann, ist dies für nicht-vorhandene Daten weitaus schwerer zu bestimmen. Zumal an dieser Stelle durchaus zwischen dem, was nicht an Daten in ein elektronisches System eingespeist wird, und tatsächlichem Nichtwissen um diese Informationen unterschieden werden sollte. Letzteres ist für das Verständnis von Privatheit und der Weiterverwendung vorhandener Daten entscheidend.

2.2.1 Fehlende und verborgene Daten

Wird mit einer IT-gestützten Form der Dokumentation gearbeitet, können zunächst technische Rahmenbedingen als Ursache für nicht-vorhandene Daten benannt werden. Dies beinhaltet beileibe nicht nur fehlende oder begrenzte Hardware (bspw. geringe PC-Dichte in den sozialen Einrichtungen, fehlende mobile Endgeräte zur Erfassung außerhalb der Büroräumlichkeiten), sondern vor allem auch Einschränkungen durch die IT-gestützten Verfahren bzw. Software selbst. Dies reicht von einer schlichten Begrenzung der Zeichenanzahl bis zu einer durch die Software intendierten Aufzeichnungspraktik, die nicht mit dem Praxishandeln der Fachkräfte kompatibel ist [5, 8, 13, 17, 23]. Das ist bspw. dann der Fall, wenn eine Systematik (bspw. bestimmte Items) durch das System vorgeben wird, mit dieser jedoch Querschnittsthemen, Wechselwirkungen oder komplexe Strukturen zwischen den Einzelfaktoren nicht (mehr) transparent gemacht werden können. Oder auch, wenn innerhalb IT-basierter Verfahren nicht die Möglichkeit besteht, jenseits festgelegter Items zu dokumentieren (d. h. zu enge Dokumentationsroutinen bestehen) und damit o. g. Umgehungsstrategien beim Dokumentieren verhindert werden. Zudem sind mit dem Medienbruch selbst, also dem Wechsel von Papier- auf elektronische Akten, unter Umständen irreversible Datenverluste einhergegangen.

Darüber hinaus gibt es personenbezogene Faktoren, die Auswirkungen auf die Qualität und den Umfang einer Dokumentation haben können. In den Interviews wurden hierfür bspw. das fehlende Verständnis für die Wichtigkeit der Dokumentation [vgl. auch 17], Unsicherheit im Umgang mit der Software, Lustlosigkeit, Vergesslichkeit sowie fehlende Sprach- und Schreibkompetenzen beim Personal (bspw. Rechtschreibprobleme oder eingeschränkte deutsche Sprachkenntnisse) genannt. Darüber hinaus werden oftmals auch konkrete Einschränkungen durch organisatorische Rahmenbedingungen (bspw. mangelnde zeitliche und/oder personale Ressourcen, hohes Arbeitsaufkommen) sowie Vorbehalte gegenüber der

Technik im Allgemeinen oder der mit der Dokumentation einhergehenden Verbindlichkeit und Exaktheit im Besonderen angeführt [13, 15, 17], um die herausfordernde Zusammenarbeit zwischen IT-Technik und dem Sozialsektor zu beschreiben. Dies kann dazu führen, dass die Dokumentation auf ein Minimum beschränkt wird. Zudem werden häufig diejenigen Informationen nicht (elektronisch) erfasst, denen entweder im Abwägungsprozess hinsichtlich der Relevanz ein geringerer Stellenwert zugesprochen wird oder aber, die schlichtweg zu kurzfristige Informationen enthalten, um sie in ein digitales System einzuspeisen. Gerade im letzteren Fall sind stattdessen bspw. handgeschriebene Zettel oder Telefonate das bevorzugtere Medium der Kommunikation:

> „… wenn jetzt jemand aufschreibt, dass irgendwelche Kompressionsstrümpfe abgeholt werden können, dann findet man das in der Regel nicht im digitalen Netz wieder. Dann wird das auf Papier irgendwo ein Zettel hinterlegt (lacht) oder man wird angerufen […]. Dann schreibt man das in der Regel nirgendwo auf.“

Nicht zuletzt kann schließlich auch die Perspektive der betroffenen Menschen mit Behinderung im Verborgenen bleiben, deren Möglichkeiten zur Darstellung ihrer eigenen Perspektive bspw. durch das Instrument der Bedarfsermittlung selbst, organisationsinterne Dokumentationsroutinen und/oder aufgrund ihrer eigenen kommunikativen Fähigkeiten limitiert sein können. Gerade in extremen Fällen kann sich so die Darstellung der eigenen Perspektive auf stellvertretende Aussagen[9] oder vereinzelte Wunschäußerungen bzgl. der eigenen Lebensplanung beschränken; eine interviewte Person betonte hierbei das *„Machtgefälle“,* das hinsichtlich der Dokumentationsmöglichkeiten besteht. Im Rahmen einzelner Interviews wurde zudem geäußert, dass die Partizipation der Klientinnen und Klienten gerade auch in der Dokumentation wünschenswert wäre:

> „… ich fände es optimaler/ das ist auch gerade im Gespräch bei uns […] [d]ass man sich kurz hinsetzt am Ende eines Kontakts und guckt: Okay, was war heute wichtig? Was wollen wir reinschreiben? Man kann die also involvieren.“

[9] Stellvertretende Aussagen sind Aussagen über die betroffene Person, die bspw. durch die Bezugsbetreuung, gesetzliche Betreuung und/oder Angehörige im Sinne der betroffenen Person getätigt werden. Solche Aussagen werden bspw. dann herangezogen, wenn der Mensch mit Behinderung nonverbal kommuniziert und ein Dolmetschen erforderlich ist, um die jeweilige Perspektive zu verbalisieren oder, wenn das oftmals dialogisch ausgerichtete Instrument der individuellen Bedarfsermittlung durch die betreffende Person nicht bedient werden kann.

Eine solche Partizipation hätte mehrere Funktionen: Zum einen würde sie zu einer Entmystifizierung der Dokumentation beitragen, weil zunächst Transparenz hinsichtlich der dokumentierten Inhalte hergestellt werden würde. Im Sinne einer Überprüfung könnte darüber hinaus bestimmt werden, ob alle Akteure mit den dokumentierten Inhalten übereinstimmen. Beides sind Aspekte, die auch mit der DSGVO gefordert werden. Die Klientinnen und Klienten wären zudem nicht mehr bloß „Objekte der Datenerhebung" [14, S. 87, auch 6, 16], sondern aktiver Part im Prozess des Dokumentierens selbst; bspw., weil fehlerhafte Inhalte (schneller) korrigiert oder eigene Perspektiven ergänzt werden könnten.

Diese genannten Einschränkungen führen dazu, dass der Aussagengehalt der vorhandenen Dokumentation in den Interviews als *„lückenhaft"* bezeichnet wird [siehe auch 9]. Da die vorhandene Dokumentation durch die dokumentierenden Personen mitunter nur als eine von vielen möglichen Interpretationen wahrgenommen wird, bleibt in der alltäglichen Arbeit der Professionellen eine permanente Unsicherheit bzgl. der *Korrektheit* dieser Interpretationen bestehen. Diese muss nicht nur ausgehalten werden, sondern nimmt eine prägnante Rolle im professionellen Verständnis ein. Das, was verschriftlicht werden kann – sei es, weil es externalisiert wurde oder, weil es die Dokumentationsroutinen hergeben – und demnach als explizites Wissen zur Verfügung steht, stellt trotz allem häufig nur einen Ausschnitt von Wirklichkeit dar. Diese Wahrnehmung drückt sich besonders prägnant im folgenden Zitat aus: *„Papier ist geduldig. Man kann sich viel vorstellen, aber eben auch viel Falsches."* Die Diskrepanz zwischen dem, was verschriftlicht wird, und dem, was die Personen im alltäglichen Umgang mit den Klientinnen und Klienten erleben, schließt damit an die bereits genannte Kritik von Verbindlichkeit und Exaktheit der Dokumentation an [13, 17]. Mehr noch: Der teils starke Fokus auf die Eindeutigkeit der Dokumentation und die Relevanz der Inhalte verhindert mancherorts den reflexiven Aspekt des Schreibens, um Inhalte zu ordnen, Verbindungen zu konstruieren und Interventionen zu entwickeln.

2.2.2 Persönliche Informationen und Technik

Trotz einer fehlenden arbeitsfeldübergreifenden oder auch arbeitsfeldinternen Vereinheitlichung von Dokumentationsanforderungen [17], sprechen sich nur zwei Personen explizit dafür aus, dass es nichts geben dürfe, was nicht auch dokumentiert werden solle. Eine der beiden Personen verweist dabei insbesondere auf die Notwendigkeit einer offenen Fehlerkultur innerhalb sozialer Organisationen:

> „… es wäre falsch, nicht festzuhalten, dass es auch einmal scheitert. Dass man auch vielleicht mit seiner Einschätzung verkehrt liegt, finde ich auch richtig, dass man es dokumentiert.“

In den meisten Interviews können jedoch Indizien für einen normativen Konsens gesammelt werden, dass bestimmte Informationen über die leistungsberechtigten Personen nicht erfasst werden sollten. Dies betrifft nicht nur die bereits thematisierten, persönlichen Wertungen der dokumentierenden Personen, sondern vor allem den Umgang mit Informationen im Rahmen der Dokumentation selbst. So sprechen sich neun Personen dafür aus, dass bestimmte Themen gar nicht oder zumindest nicht detailliert dokumentiert werden sollten. Genannt werden neben Traumata oder Gewalterfahrungen, in der Vergangenheit liegende Lebensereignisse ohne Auswirkung auf die aktuelle Situation (bspw. Haftaufenthalte), Partnerschaft inkl. Sexualität (bspw. Partnerschaftsprobleme, Geschlechtskrankheiten oder die Häufigkeit der Sexualkontakte) auch die eigene Weltanschauung sowie psychische Themen, die bspw. im Rahmen von Therapien durch die Klientinnen oder Klienten aufgearbeitet werden.

Begründet wird ein solch bewusstes Nicht-Dokumentieren bzw. sparsames Dokumentieren zum einen mit der Intimität der Informationen. So verweist bspw. eine Person auf ihr Wissen um das Schamgefühl bei Menschen mit Behinderung, wenn diese ihren eigenen Hilfebedarf gegenüber Dritten kommunizieren müssen. In zwei weiteren Interviews wird betont, dass eine fachliche Dokumentation nicht der eigenen psychischen Verarbeitung von belastenden Informationen dient. Stattdessen sollten nur diejenigen Informationen festgehalten werden, welche die o. g. Funktionen erfüllen, also bspw. Informationen, die zur Rekonstruktion des Falls notwendig sind. Alle drei Aspekte, nämlich der Ausschluss bestimmter Themen, die Thematisierung des Schamgefühls und die Betonung dieser auch verarbeitenden Funktion des Schreibens unterstreichen die wahrgenommene Intimität der nicht bzw. nur sparsam dokumentierten Inhalte durch die dokumentierende Person. Sie werden eben deswegen nicht bzw. nicht in dieser Detailtiefe notiert, weil um ihren sensiblen Inhalt für die betroffene Person gewusst wird. Prägnant wird dies durch eine Person wie folgt formuliert: nämlich, *„dass es durchaus Geschichten gibt, die nirgendwo zwingend dokumentiert werden müssen.“*

Zum anderen führt aber gerade auch das Wissen um die potenzielle Weiterverwendung der Informationen bspw. im Rahmen des Antrags auf Leistungen zur Teilhabe dazu, dass insbesondere bei sensiblen Themen äußerst vorsichtig und umsichtig dokumentiert wird. So wird in fünf Interviews explizit darauf verwiesen, dass die im IT-gestützten Verfahren dokumentierten Daten bspw. aufgrund

einer gemeinsam geteilten, digitalen Akte durch organisationsinterne Kolleginnen und Kollegen anderer Organisationseinheiten eingesehen werden könnten. In einigen Fällen wird deswegen von einer detaillierten Darstellung abgesehen:

> „Aber ich würde keine intimen oder sehr privaten Details einer Person dort festhalten, weil das natürlich tendenziell auch immer Daten sind, die auch, wenn sie geschützt sind, vielleicht irgendwo mal einzusehen werden und ja auch gespeichert werden und ja existieren."

In solchen Fällen wird gerade so viel notiert, dass mit dem Fall vertraute Personen eine hinreichende Arbeitsgrundlage haben. Die so resultierende sparsame Dokumentation wurde dann bspw. als Dokumentation *„auf einer Metaebene"* bezeichnet.

3 Ein Erklärungsversuch

Die Ergebnisse können durchaus überraschen: Nicht nur kann es in seltenen Fällen dazu kommen, dass sensible Informationen trotz fehlendem Einverständnis mit Verweis auf die Relevanz an Dritte übermittelt werden. Darüber hinaus werden manche intimen Informationen gar nicht erst (so detailliert) digital dokumentiert, um sie so vor dem Zugriff Dritter innerhalb der eigenen Organisation zu schützen. Dieser scheinbare Widerspruch lässt sich unter Hinzunahme der Relationstheorien zur Privatheit erklären, in denen die Privatheit als Bedingung für eine vertrauensvolle, personelle Beziehungen (im Folgenden: intime Beziehung[10]) unterstrichen wird [4, 21].

Rössler [21] erweitert diese Theorien, wenn sie diese mit informationeller Privatheit verbindet: Demnach wird mithilfe der Theorien relationaler Privatheit nicht nur „die Differenz zwischen öffentlichen und privaten Beziehungen präzise" bestimmt, in denen es „wesentlich um die Funktionsbestimmung des Privaten als Austausch bestimmter Informationen geht" [21, S. 235]. Vielmehr verortet sie im Setting intimer Beziehungen den Versuch einer Person, „zu erproben, was ein

[10] Intime Beziehungen entstehen nach Rössler „in einem *setting,* das durch freundschaftliche Zuneigung oder Liebe, durch Sorge und Rücksichtnahme und eine besondere Form von Interesse ausgezeichnet ist" [21, S. 237 f., Hervorhebung im Original]. Ferner findet sich dieses Setting „in einem bestimmten Kontext von affektiver Zuwendung, sympathischen Einstellungen und eingegangen Verpflichtungen zwischen den beteiligten Personen" [21, S. 238].

selbstbestimmtes und authentisches Verhalten, Leben sein könnte, welche Inszenierungen von Selbstdarstellung möglich, erwünscht, authentisch usf. wären“ [21, S. 235]. Wird diese Theorie mit der Sozialen Arbeit in Verbindung gebracht, die „wie kaum ein anderes Berufsfeld auf eine ungestörte, vertrauensvolle Beziehung zu den Ratsuchenden angewiesen“ ist [19, S. 415], so wird deutlich, dass Beziehungen im Kontext der Eingliederungshilfe stets potenziell intime Beziehungen sein *können.* Dies gilt besonders, wenn Menschen mit Behinderung im Rahmen der Teilhabeplanung "Fragen der eigenen praktischen Identität" und "Grundfragen ihres Lebens" thematisieren [21, S. 240].

Mit Blick auf ihre Ausführungen ist eine solche These mindestens gewagt; spricht Rössler doch davon, dass die Beziehung bspw. zu einer Psychoanalytikerin nicht allein deswegen intim ist, weil ihr Details über das eigene Leben mitgeteilt werden [vgl. 21, S. 237]. Wohl aber kann es zu einer intimen Beziehung werden, nämlich dann, wenn in dem „symbolischen Raum“ mit dem Gegenüber „Prozesse der intersubjektiven Auseinandersetzung statt[finden], die als konstitutiv für die Identität und Autonomie der Betroffenen begriffen werden müssen“ [21, S. 238–239]. Ein solch intimes Setting mag einseitig und temporär in einer ansonsten professionellen Beziehung sein; gleichwohl zeugen Aussagen wie „*[w]enn der mir das anvertraut*“ oder etwas wurde „*im Vertrauen*“ erzählt für ihre Existenz. Hier wird die rein professionelle Beziehung verlassen und Informationen ausgetauscht, die in anderer Konstellation unter Umständen nicht mitgeteilt worden wären.

Zugleich ist die Ausbildung der eigenen Identität „auf Beziehungen angewiesen […], in denen […] konstitutive Liebe und Wertschätzung vermittelt wird: nur in solchen Beziehungen kann nämlich das für gelingende Identitäten notwendige Selbstvertrauen überhaupt erlangt werden“ [21, S. 239]. Die o. g. Forderung an die Dokumentation, dass diese wertschätzend ausfallen solle, kann demnach als Indiz für eben jene vertrauensvermittelnde Beziehung herhalten. Noch deutlicher wird es bspw. im Setting besonderer Wohnformen (ehemals: stationäre Einrichtungen), wo die Unterscheidung in Wohn- und Arbeitsräume nicht mehr trennscharf zu ermitteln ist: Was der Wohnort des einen ist, ist der Arbeitsort des anderen. Werden in einem solchen Setting „selbstbestimmtes und authentisches Verhalten“ und die „Inszenierungen von Selbstdarstellung“ erprobt [21, S. 235], ist damit zugleich die Anforderung an das Gegenüber verbunden, solche Erprobungen und Versuche nicht öffentlich zu machen [21, S. 244 ff.]. Die Öffentlichkeit beginnt dabei nicht erst, wenn Informationen in die Hände Dritter *außerhalb* der eigenen Organisation gelangen, sondern bereits mit dem Niederschreiben in ein digitales, organisations*internes* Dokumentationssystem, wo „bestimmte andere“ [21] diese privaten Informationen über die betreffende Person einsehen können. Das in solch (semi-) intimen Settings gewonnene Wissen muss daher hinsichtlich der Relevanz für die

Tab. 1 Relationale Beziehungen und deren Auswirkung auf die fachliche Dokumentation (in Anlehnung an Rössler [21], eigene Darstellung)

Interpretation der dokumentierenden Person	Antizipiertes intimes Setting aus Sicht der Klientin/des Klienten	Antizipiertes berufliches Setting aus Sicht der Klientin/des Klienten
Intimes Setting aus Sicht der dokumentierenden Person	• Intime Beziehung • Privatheit-Konflikte unwahrscheinlich, aber möglich • Dokumentation unwahrscheinlich, aber möglich	• Privatheit-Konflikte unwahrscheinlich, aber möglich • Auswirkung auf Dokumentation unklar
Berufliches Setting aus Sicht der dokumentierenden Person	• Privatheit-Konflikte • Ggf. Transformation des Wissens: sparsame Dokumentation möglich	• Professionelle Beziehung • Privatheit-Konflikte unwahrscheinlich, aber möglich • „normale“ Dokumentation

fachliche Arbeit bewertet und anschließend ggf. in das Dokumentationssystem transformiert werden (siehe Tab. 1).

Wird der Informationserhalt durch die dokumentierende Person in einem (beidseitig) intimen Setting verortet, so ist die Dokumentation der Inhalte unwahrscheinlich, aber möglich. Zu vermuten ist, dass eine ggf. doch vorhandene Dokumentation dann durch Dritte bspw. als *„Hetze“* [Interview], „Gerede, Tratsch“ oder Kollusion wahrgenommen wird [21, S. 242]. Stellen sich die mitgeteilten Informationen jedoch als relevant für die weitere professionelle Arbeit heraus, so ist eine Dokumentation erforderlich. Für die dokumentierende Person kann dies eine Dilemma-Situation darstellen: Einerseits *muss* die Kontrolle über relevante, intime Informationen abgegeben werden, da im Rahmen des Antragsverfahrens eine gewisse *Pflicht zur Offenlegung* besteht, um eine plausible und nachvollziehbare Legitimation zur Bewilligung von Leistungen zur Teilhabe nachweisen zu können. Andererseits *können* die Informationen nicht mitgeteilt werden, ohne damit die vertrauensvolle Beziehung zur Klientin bzw. zum Klienten ggf. nachhaltig zu gefährden und sich der Kollusion schuldig zu machen.

Ein potenzieller Ausweg scheint im advokatorischen Handeln der dokumentierenden Person zu liegen, nämlich, indem sie stellvertretend für die betroffene Person von der Weitergabe der intimen Details absieht, d. h. eine sparsame Dokumentation vornimmt. Damit belegen die dokumentierenden Personen eine

Schlüsselposition im Setting der Eingliederungshilfe: Als Protektoren bzw. Gatekeeper sorgen sie für eine Informationsreduktion, um die Privatsphäre der Betroffenen zu schützen; gleichzeitig vermitteln sie als Advokaten zwischen den Bedürfnissen der Betroffenen und den Anforderungen des Staates innerhalb der Eingliederungshilfe, indem gerade so viele Informationen zur Verfügung gestellt werden, wie notwendig sind.

Ein solches Verhalten ist jedoch nur erfolgreich, wenn das Wissen um Nichtwissen ausgehalten wird: Denn Auslassungen von Details sind nur dann möglich, wenn das die Informationen empfangende Gegenüber diese offensichtlichen Leerstellen akzeptieren kann. Gerade, weil mithilfe der dokumentierten Inhalte auch die Wesentlichkeit der Einschränkung von Teilhabe im Rahmen des Antrags auf Leistungen zur Teilhabe nachvollziehbar und plausibel belegt wird, sind Leerstellen nur als fallspezifische Aushandlungsprozesse zwischen allen am Prozess beteiligten Akteuren zu verstehen und daher in aller Regel eher Ausnahmen. Dabei werden insbesondere die Mitarbeitenden der Leistungsträger herausgefordert: Reichen ihnen diejenigen Informationen aus, die in schriftlicher Form in den Antrag einfließen, um zu einem Urteil über den Bescheid von Leistungen zu kommen? Eine positive Antwort auf diese Frage erhöht die Wahrscheinlichkeit, dass die Privatheit der Menschen mit Behinderung geschützt und gewährleistet wird. Zugleich hat es einen stabilisierenden Charakter in der Vertrauensbeziehung aller beteiligten Akteure zur Folge.

4 Fazit

Obgleich Pudelko und Richter [19, S. 414] von einer „wenig klare[n] Rolle“ des Datenschutzes innerhalb der Praxis Sozialer Arbeit sprechen, verdeutlichen die Ergebnisse der Interviews, dass einige Datenschutzprinzipien wie die Rechtmäßigkeit der Verarbeitung, Zweckbindung und Richtigkeit der Daten sowie die Datenminimierung bereits implizit bedacht, teils sogar schon umgesetzt werden. Gleichwohl wird deutlich, dass vorhandene Daten stark von der dokumentierenden Person und ihrer subjektiven Perspektive auf eine Situation [5, 17, 22–24] sowie von organisationsintern festgelegten Dokumentationsroutinen und deren Umsetzung durch die dokumentierende Person [5, 8, 9, 17, 20, 24] abhängen; ein Umstand, der bspw. mit Blick auf die Anforderungen von Richtigkeit und Speicherbegrenzung der Daten gemäß DSGVO nur schwer zu rechtfertigen ist. Gerade, weil innerhalb der Teilhabeplanung besondere personenbezogene Daten über die betroffenen Personen erhoben werden, erscheint partizipative Dokumentation bzw. die Mitsprache der Klientinnen und Klienten, wenigstens jedoch

eine umfassende Transparenz hinsichtlich der Fragen, welche Daten vorhanden sind, ob diese auch aus Perspektive der Menschen mit Behinderung korrekt sind und wann welche Daten nicht mehr relevant sind und folglich nach Ablauf der Speicherfristen gelöscht werden müssten, als unabdingbar.

Zugleich zeigt der vorliegende Beitrag, dass die Frage, wo öffentlicher Raum beginnt und an welcher Stelle datenschutzrechtliche, technische und organisatorische Maßnahmen (TOM) getroffen werden (müssten), nicht zwangsläufig mit dem Zuweisen von Zugriffsrechten innerhalb digitaler Dokumentationssysteme abgetan werden kann. Stattdessen erscheint auch hier eine professionelle Auseinandersetzung notwendig; gerade, wenn es die Wahrung von Privatheitsbedürfnissen vulnerabler Personengruppen in der professionellen Praxis betrifft. Denn öffentlicher Raum kann mitunter schon dadurch entstehen, *weil* Informationen im digitalen Dokumentationssystem erfasst werden.

Danksagung Das Projekt „Maschinelle Entscheidungsunterstützung in wohlfahrtsstaatlichen Institutionen: Nutzungsoptionen, Implikationen und Regulierungsbedarfe (MAEWIN)“ wurde im Rahmen des Forschungsverbundes NRW Digitale Gesellschaft durch das Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen gefördert.

Literatur

1. Berg, M.: Practies of reading and writing. The constitutive role of the patient record in medical work. Sociol. Health Illn. **18**(4), 499–524 (1996)
2. Bundesarbeitsgemeinschaft der überörtlichen Träger der Sozialhilfe (BAGüS): Der Behinderungsbegriff nach SGB IX und SGB XII und die Umsetzung in der Sozialhilfe. Orientierungshilfe für die Feststellung der Träger der Sozialhilfe zur Ermittlung der Leistungsvoraussetzungen nach dem SGB XII i. V. m. der Eingliederungshilfe-Verordnung (EHVO). Bundesarbeitsgemeinschaft der überörtlichen Träger der Sozialhilfe BAGüS, Münster. https://www.bagues.de/spur-down-load/bag/orientierungshilfe_behinderungsbegriffendf_24112009.pdf (2009). Accessed 11 Okt. 2020
3. Crawford, K.: The hidden biases in big data. https://hbr.org/2013/04/the-hidden-biases-in-big-data (2013). Accessed 29 Mär 2019
4. Fried, C.: Privacy. Yale Law J. **77**(3), 475–493 (1968). https://doi.org/10.2307/794941
5. Gillingham, P., Graham, T.: Big data in social welfare: the development of a critical perspective on social work’s latest “electronic turn”. Aust. Soc. Work **70**(2), 135–147 (2016). https://doi.org/10.1080/0312407X.2015.1134606
6. Heiner, M.: Diagnostik in der Sozialen Arbeit. In: Otto, H.-U., Thiersch, H. (Hrsg.) Handbuch Soziale Arbeit. Grundlagen der Sozialarbeit und Sozialpädagogik, 4. Aufl., S. 237–250. Reinhardt, München (2011)
7. Hoffmann, B.: Medienpädagogik und Soziale Arbeit – kongruent, komplementär oder konträr im Umgang mit Digitalisierung und Mediatisierung. In: Kutscher, N., Ley, T.,

Seelmeyer, U., Siller, F., Tillmann, A., Zorn, I. (Hrsg.) Handbuch Soziale Arbeit und Digitalisierung, 1. Aufl., S. 42–57. Beltz Juventa, Weinheim (2020)
8. Huuskonen, S., Vakkari, P.: “I did it my way”: social workers as secondary designers of a client information system. Inf. Process. Manage. **49**(1), 380–391 (2013). https://doi.org/10.1016/j.ipm.2012.05.003
9. Huuskonen, S., Vakkari, P.: Selective clients’ trajectories in case files: filtering out information in the recording process in child protection. Br. J. Soc. Work **45**(3), 792–808 (2015). https://doi.org/10.1093/bjsw/bct160
10. Kreidenweis, H.: Digitalisierung der Sozialwirtschaft. Herausforderungen für das Management sozialer Organisationen. In: Kutscher, N., Ley, T., Seelmeyer, U., Siller, F., Tillmann, A., Zorn, I. (Hrsg.) Handbuch Soziale Arbeit und Digitalisierung, 1. Aufl., S. 390–401. Beltz Juventa, Weinheim (2020)
11. Kreidenweis, H., Wolff, D.: IT-Report für die Sozialwirtschaft 2016. IT-Report für die Sozialwirtschaft, Bd. 2016. Katholische Universität Eichstätt-Ingolstadt, Eichstätt (2016)
12. Ley, T., Reichmann, U.: Digitale Dokumentation in Organisationen Sozialer Arbeit. In: Kutscher, N., Ley, T., Seelmeyer, U., Siller, F., Tillmann, A., Zorn, I. (Hrsg.) Handbuch Soziale Arbeit und Digitalisierung, 1. Aufl., S. 241–254. Beltz Juventa, Weinheim (2020)
13. Ley, T., Seelmeyer, U.: Dokumentation zwischen Legitimation, Steuerung und professioneller Selbstvergewisserung. Soz. Extra **38**(4), 51–55 (2014). https://doi.org/10.1007/s12054-014-0090-1
14. Merchel, J.: Zwischen ‚Diagnose‘ und ‚Aushandlung‘. Zum Verständnis des Charakters von Hilfeplanung in der Erziehungshilfe. In: Peters, F. (Hrsg.) Diagnosen – Gutachten – hermeneutisches Fallverstehen. Rekonstruktive Verfahren zur Qualifizierung individueller Hilfeplanung, 1. Aufl., S. 73–96. IGFH, Frankfurt/Main (1999)
15. Merchel, J.: Pädagogische Dokumentation zwischen Etikettierung und Ausweis fachlichen Handelns. In: Henes, H., Trede, W. (Hrsg.) Dokumentation pädagogischer Arbeit. Grundlagen und Methoden für die Praxis der Erziehungshilfen. Grundsatzfragen, Bd. 42, 1. Aufl., S. 15–41. Internationale Gesellschaft für erzieherische Hilfen; Walhalla Fachverlag, Frankfurt/Main (2004)
16. Merchel, J.: „Diagnostik“ als Grundlage für eine fachlich begründete Hilfeplanung: inhaltliche Anforderungen und angemessene Semantik. In: Verein für Kommunalwissenschaften e. V. (Hrsg.) Diagnostik in der Kinder- und Jugendhilfe. Vom Fallverstehen zur richtigen Hilfe. Dokumentation der Fachtagung vom 21.–22. April 2005 in Berlin. Aktuelle Beiträge zur Kinder- und Jugendhilfe, Bd. 51, S. 13–29. Berlin (2005)
17. Merchel, J., Tenhaken, W.: Dokumentation pädagogischer Prozesse in der Sozialen Arbeit: Nutzen durch digitalisierte Verfahren. In: Kutscher, N., Ley, T., Seelmeyer, U. (Hrsg.) Mediatisierung (in) der sozialen Arbeit. Grundlagen der sozialen Arbeit, Bd. 38, S. 171–191. Schneider Verlag Hohengehren GmbH, Baltmannsweiler (2015)
18. Moch, M.: Wenn Daten für sich sprechen – Fallstricke des Dokumentierens in pädagogischen Einrichtungen. In: Henes, H., Trede, W. (Hrsg.) Dokumentation pädagogischer Arbeit. Grundlagen und Methoden für die Praxis der Erziehungshilfen. Grundsatzfragen, Bd. 42, 1. Aufl., S. 57–75. Internationale Gesellschaft für erzieherische Hilfen; Walhalla Fachverlag, Frankfurt/Main (2004)
19. Pudelko, T., Richter, C.: Informationelle Selbstbestimmung, Datenschutz und der institutionelle Auftrag der Sozialen Arbeit in Zeiten der Digitalisierung. In: Kutscher, N., Ley,

T., Seelmeyer, U., Siller, F., Tillmann, A., Zorn, I. (Hrsg.) Handbuch Soziale Arbeit und Digitalisierung, 1. Aufl., S. 414–426. Beltz Juventa, Weinheim (2020)
20. Reichmann, U.: Schreiben und Dokumentieren in der Sozialen Arbeit. Struktur, Orientierung und Reflexion für die berufliche Praxis. UTB Soziale Arbeit, Bd. 4579. Budrich, Opladen (2016)
21. Rössler, B.: Der Wert des Privaten. Suhrkamp Taschenbuch Wissenschaft, 1. Aufl., Bd. 1530. Suhrkamp, Frankfurt a. M. (2001)
22. Schneider, D.: Decision Support Systeme in der Sozialen Arbeit – Herausforderungen an die Rolle der TA in Innovationsprozessen. In: Nierling, L., Torgersen, H. (Hrsg.) Die neutrale Normativität der Technikfolgenabschätzung: Konzeptionelle Auseinandersetzung und praktischer Umgang, S. 117–138. Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden (2020)
23. Schneider, D., Seelmeyer, U.: Challenges in using big data to develop decision support systems for social work in Germany. J. Technol. Hum. Serv. **37**(2–3), 113–128 (2019). https://doi.org/10.1080/15228835.2019.1614513
24. Taylor, C.: Trafficking in facts. Writing practices in social work. Qual. Soc. Work **7**(1), 25–42 (2008). doi: https://doi.org/10.1177/1473325007086414

Zum Konflikt zwischen Accessibility und Privacy

Irmhild Rogalla und Tilla Reichert

Zusammenfassung

Zunächst wird an konkreten Beispielen gezeigt, dass die digitale Welt für Menschen mit Behinderungen nicht problemlos zugänglich ist (Accessibility) und darüber hinaus unterschiedliche Konflikte zwischen Accessibility und Privacy bestehen. Zu den Konflikten tragen verschiedene Aspekte nicht hinreichender oder nicht vorhandener Accessibility wie Privacy bei. Die Ursachen für diese Situation liegen teilweise sehr früh und sehr tief in den Entwicklungsprozessen moderner Software und IT-Systeme, in mangelndem Bewusstsein wie fehlendem Wissen um entsprechende Anforderungen bei Entwickler:innen und Verantwortlichen. Eine Lösung dafür bietet der Europäische Standard EN 16234-1:2019 „e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in all industry sectors“. In seiner neuesten Fassung werden unter anderem Accessibility und Privacy als „transversal aspects“ besonders hervorgehoben und alle IT-Fach- und Führungskräfte zu ihrer Berücksichtigung verpflichtet.

Schlüsselwörter

Accessibility • Privacy • Zugänglichkeit • Barrierefreiheit • Informationelle Selbstbestimmung • „by design“ • E-Competence Framework • EN 16234 • Software Entwicklung

I. Rogalla (✉) · T. Reichert
Institut PI , Berlin, Deutschland
E-Mail: irmhild.rogalla@institut-pi.de

T. Reichert
E-Mail: tilla.reichert@institut-pi.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_13

1 Vom Konflikt zwischen Accessibility und Privacy zu strukturellen Lösungen

Die digitale Welt ist für Menschen mit Behinderungen nicht problemlos zugänglich (Mangel an Accessibility). Dieser Beitrag möchte über diese Erkenntnis hinaus aufzeigen, dass es leicht zu Konflikten zwischen Accessibility und Privacy kommt. Am Anfang stehen daher konkrete Beispiele, die aus eigenen Erfahrungen der Autorinnen sowie aus Untersuchungen zur Nutzung digitaler Technologien im Alltag von Menschen mit Behinderungen stammen [1, 2]. Zu den Konflikten tragen verschiedene Aspekte nicht hinreichender oder nicht vorhandener Accessibility wie Privacy bei. Für diese missliche Situation gibt es vielfältige Gründe. Häufig liegen die Ursachen sehr früh und sehr tief in den Entwicklungsprozessen moderner Software und IT-Systemen. Prinzipiell lautet die Lösung dann „Accessibility by design“ und „Privacy by design“. Hierzu besteht auf konzeptioneller wie technischer Ebene noch viel Forschungs- und Entwicklungsbedarf. Hinzu kommt: Entwickler:innen wie Verantwortlichen mangelt es oft an Bewusstsein bezüglich entsprechender Anforderungen und an Wissen, wie solche Anforderungen in der Entwicklung und damit Gestaltung der Technik berücksichtigt werden können. In der neuesten Fassung des Europäischen Standards EN 16234-1:2019 „e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in all industry sectors“ gibt es daher eine neue normative Dimension: die „transversal aspects“. Mit ihnen werden unter anderem Accessibility und Privacy besonders hervorgehoben und alle IT-Fach- und Führungskräfte zu ihrer Berücksichtigung verpflichtet.

2 „Tarnmodus“ – ein erstes Beispiel für den Konflikt zwischen Privacy und Accessibility

„Tarnmodus“ ist die Bezeichnung der Autorinnen für den Versuch, als taube Person mit Hilfe von Gebärdensprachdolmetscher:innen so mit Hörenden zu kommunizieren, dass die Gehörlosigkeit nicht auffällt und dementsprechend auch nicht thematisiert werden muss. Dabei geht es häufig gar nicht um die Fragen der Selbstoffenbarung [3] oder die Angst vor Diskriminierung, sondern schlicht um die praktische Bewältigung des (beruflichen) Alltags. Denn Gehörlosigkeit bedeutet auch, beim Telefonieren nichts verstehen zu können. Trotz zunehmender Nutzung des Internets spielen Telefonate für Terminabsprachen, kurze Auskünfte, die Suche nach der richtigen Ansprechpartnerin und ähnliches immer noch eine große Rolle. Als „Tarnmodus“ bezeichnen die Autorinnen folgende Konstellation

für Telefonate: Die Gehörlose, hier: Frau Dr. Rogalla, und ihre Dolmetscherin eröffnen zunächst per PC/Laptop und Internet eine Videokonferenz, sodass eine Verständigung mittels Gebärdensprache möglich ist. Dann stellen sie per Smartphone eine Telefonverbindung untereinander her, um dann mittels der Funktion „Telefonkonferenz"/„Anrufe zusammenführen" die eigentliche Gesprächspartnerin anzuwählen. Sowohl die allgemeine Höflichkeit wie auch die Regeln für die Tätigkeit von Gebärdensprachdolmetscher:innen gebieten es, nun den Gesprächspartner über die Situation (3er-Konferenz, Gehörlose mit Dolmetscher:in, etc.) zu informieren. „Tarnmodus" bedeutet nun, dies nicht zu tun, sondern einfach zu erledigen, was zu erledigen ist. Denn die Erfahrung lehrt, dass der Aufwand für die Erläuterung der Situation, der Behinderung, des Umgangs damit, der Nutzung von Gebärdensprache usw. in der Regel in keinem Verhältnis zu dem steht, was mit dem Anruf erledigt werden soll. Sowohl im Hinblick auf Barrierefreiheit wie auf Privatheit (aller Beteiligten) handelt es sich um eine komplizierte Situation. Darauf kann hier nicht im Detail eingegangen werden. Aufmerksam machen wollen wir aber auf das Verhältnis von Accessibility und Privacy: Einerseits ermöglicht die kombinierte Nutzung von Gebärdensprachdolmetscher:innen und Videokonferenz den Gehörlosen, ihre Privatsphäre zu schützen und sich nicht als „behindert" offenbaren zu müssen. Andererseits erfüllen gängige[1] Videokonferenz-Dienste aber grundlegende Anforderungen an Datenschutz und -sicherheit nicht [4, 5].

Ein weiterer, sehr typischer Konflikt zwischen Accessibility und Privacy tritt bei der Nutzung von Videokonferenz-Diensten dann auf, wenn die Gehörlose und ihre Dolmetscher:innen tatsächlich mit mehreren Personen an einer Videokonferenz teilnehmen. Denn Videokonferenz-Systeme sind in aller Regel für hörende und sprechende Menschen konzipiert: So wird oft der/die Sprecher:in automatisch groß angezeigt und die Videofenster der passiven Teilnehmer:innen verkleinern sich mit der Zunahme der Zahl der Teilnehmer:innen automatisch immer weiter. Beides sorgt dafür, dass die Gebärdensprachdolmetscher:innen nicht oder nicht in hinreichender Größe sichtbar sind. Anders gesagt: Ein für die Verdolmetschung in Gebärdensprache nutzbarer Videokonferenz-Dienst muss die Möglichkeit bieten, die Gebärdensprachdolmetscher:innen dauerhaft gut sichtbar zu machen. Dafür sollten – auch mehrere – Videofenster jederzeit fixierbar und ihre Größe einstellbar sein. Diese Accessibility-spezifische Anforderung ist unumgänglich und

[1] Mit gängigen Videokonferenz-Diensten sind hier typische, kostenpflichtige Cloud-basierte Angebote meist US-amerikanischer Anbieter gemeint, wie sie im Business-Umfeld genutzt werden, z. B. Cisco WebEx, GoToMeeting, Zoom u. ä.

hat daher zwangsläufig höchste Priorität. Sie sorgt dafür, dass auch bekannte Verstöße entsprechender Anbieter gegen Datenschutz und -sicherheit bei der Auswahl möglicher, zu nutzender Dienste in Kauf genommen werden (müssen)[2].

Dieser Konflikt zwischen Accessibility und Privacy ist insofern typisch, als er sehr häufig und bei vielen verschiedenen Systemen und Anwendungen auftritt: Damit Menschen mit Behinderungen diese Programme oder Dienste nutzen zu können, sind sie auf Zugänglichkeit bzw. Barrierefreiheit und/oder spezifische Funktionen zwingend angewiesen. Die Auswahl ist allerdings sehr begrenzt, sodass Nutzer:innen oft gezwungen sind, bei datenschutzrechtlichen Aspekten Abstriche zu machen, um überhaupt teilnehmen zu können.

3 Weitere Beispiele für Konflikte zwischen Privacy und Accessibility

Bei Untersuchungen zur Nutzung digitaler Technologien durch Menschen mit Behinderungen in den Jahren 2017 und 2018 [1, 2] zeigte sich ebenfalls, dass Accessibility keineswegs selbstverständlich ist und Accessibility und Privacy in der Regel nicht miteinander vereinbar sind[3].

Sehr häufig tritt der bereits beschriebene Konflikt auf: Viele digitale Anwendungen und internetbasierte Dienste sind nicht barrierefrei. Für Menschen mit Behinderungen ist die Auswahl daher sehr eingeschränkt und Anforderungen an Privacy oder auch nur an grundlegenden Datenschutz spielen zwangsläufig eine sehr untergeordnete Rolle. So sind beispielsweise die Geräte und Systeme mit Apples (proprietären) Betriebssystemen MacOS und iOS derzeit im Hinblick auf Accessibility, insbesondere für Menschen mit Sehbehinderung/Blindheit, mit Abstand führend. Kein freies, nicht-proprietäres Betriebssystem (wie die verschiedenen Linux-Derivate) erreicht auch nur annähernd dasselbe Maß an Zugänglichkeit. Zwar bemüht Apple sich im Vergleich zu anderen um Datenschutz und versucht auch, europäischen Standards gerecht zu werden. Trotzdem haben beispielsweise die amerikanischen Geheimdienste wie NSA und FBI Zugriff auf Daten, die auf amerikanischen Servern liegen und nicht voll verschlüsselt sind [3, 7].

[2] Im Bereich der Videokonferenz-Dienste gibt es aktuell (Sommer 2020) erste Lösungen (z. B. Whereby und BigBlueButton), die sowohl barrierefrei/-arm als auch DSGVO-konform (bei entsprechender Installation und Infrastruktur) sind.

[3] Bestätigt wird dieser Befund auch durch eine aktuelle (2020) Studie zur „Digitale Teilhabe von Menschen mit Behinderung“ [6].

Menschen mit Behinderungen haben nur wenig Möglichkeiten, über das Maß ihrer Privatheit zu bestimmen. Insbesondere wenn es um spezifische assistive Technologien geht, sind sie den jeweiligen Anbietern meist ausgeliefert. Beispiele dafür sind die Steuerung von Hilfsmitteln wie Prothesen, Hörgeräten oder anderen vernetzen, auf Cloud-basierten Diensten beruhenden Geräten. Hier lautetet die Alternative meist, entweder in alle Bedingungen des Anbieters einzuwilligen oder – mangels Alternative bzw. offenen Schnittstellen – auf das Hilfsmittel zu verzichten. Ähnliches gilt für Apps, die bei psychischen Krankheiten unterstützen sollen und können. Hier ergibt sich zusätzlich das Problem, dass diese Anwendungen häufig als Tagebuch fungieren und/oder die regelmäßige Eingabe intimer Daten erfordern (z. B. Schlafzeiten und -qualität).

Sehr häufig sind Menschen mit Behinderungen gezwungen, die eigentlich besonders schützenswerte Information, dass sie behindert sind, preiszugeben. So lässt sich beispielsweise nicht verhindert, dass auf der technische Ebene durch Server ausgelesen wird, wenn jemand einen Screenreader verwendet, ein Tool, das durch Sprachausgabe Blinden/Sehbehinderten die Nutzung digitaler Endgeräte ermöglicht. Nutzt jemand im Kino die App „Greta“, um sich Untertitel anzeigen zu lassen, wird zumindest für die Umsitzenden die Hörschädigung offensichtlich.

Eine weitere, neuartige Variante des Konflikts zwischen Privacy und Accessibility ergibt sich bei Diensten, die große Datenmengen sammeln und auswerten, unabhängig davon, ob dies mit Mitteln der „Künstlichen Intelligenz“ (KI) geschieht oder nicht. Hier ist häufig nur erkennbar, dass Daten gesammelt werden, aber nicht, welche es sind, ob sie anonymisiert und verarbeitet werden. Typische Beispiele sind vor allem Bilderkennungs-Apps, die sich an Sehbehinderte/Blinde richten und anbieten, per Sprachausgabe anzusagen, was gerade mit der Kamera aufgenommen wurde. Abgesehen davon, dass die Ergebnisse der Identifikation zweifelhaft und unzuverlässig sind[4] [2, S. 38 f.], erweckt zumindest ein Teil dieser Apps den Eindruck, dass sie lediglich entwickelt wurden, um Daten als Trainingsmaterial für die Anwendung zu sammeln.

Persönliche Daten – auch von Menschen mit Behinderungen – werden also auch eher als Ware, denn als schützenswertes Gut behandelt. Aufgrund mangelnder Accessibility oder – vor allem bei assistiver Technologie – völliger Alternativlosigkeit, haben gerade Menschen mit Behinderungen wenig bis keine Auswahl, sodass selbst einfachste Möglichkeiten des Selbstdatenschutzes nicht zur Verfügung stehen. Konflikte zwischen Accessibility und Privacy sind also nicht selten.

[4] Für einen direkten Eindruck: https://www.you-tube.com/watch?v=oay7YfiXA9Q [Letzter Abruf: 02.10.2020].

Für diese missliche Situation gibt es vielfältige Gründe. Sie reichen von den dominierenden Interessen der großen Player an persönlichen Daten (Stichwort „Überwachungskapitalismus“ [8]) über technische Hürden bis hin zu veralteten Standards. Häufig liegen die Ursachen sehr früh und sehr tief in den Entwicklungsprozessen moderner Software und IT-Systemen. Prinzipiell lautet die Lösung dann „Accessibility by design“ und „Privacy by design“. Hierzu besteht auf konzeptioneller wie technischer Ebene noch viel Forschungs- und Entwicklungsbedarf. Hinzu kommt: Diejenigen, die Software und IT-Systeme spezifizieren, entwickeln und verantworten müssen über das notwendige Bewusstsein und Wissen verfügen. Beides ist weder selbstverständlich noch einfach zu realisieren: So spielen beispielsweise in den aktuellen Empfehlungen[5] der GI (Gesellschaft für Informatik) für Informatik-Studiengänge, ihre Strukturen und Curricula Datenschutz und Privacy nur ganz am Rande eine Rolle (typischerweise unter dem Oberthema „Informatik und Gesellschaft“) und Accessibility/Barrierefreiheit gar keine. Dazu kommt: Es handelt sich um typische Querschnittsthemen, die in konkreten Entwicklungsprozessen in der Praxis fast überall relevant sein können, gerade deswegen aber auch schwer fassbar sind.

4 „Transversal Aspects“ im Europäischen e-Competence Framework für Fach- und Führungskräfte

Einen Beitrag zur Lösung dieser Problematik bieten die „transversal aspects“, eine neue normative Dimension in der aktuellen Version des Europäischen Standards EN 16234-1:2019 „e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in all industry sectors“ [9][6].

Der e-CF ist ein Sektorrahmen, der eine europaweit verständliche Sprache für Kompetenzen, Fähigkeiten und Wissen von IT-Fach- und Führungskräften auf fünf Niveaustufen bereit stellt. Die erste Version wurde 2008 veröffentlicht, als

[5] vgl. GI: Empfehlung: Curriculum für Bachelor- und Masterstudiengänge Technische Informatik (März 2018); Rahmenempfehlung für die Ausbildung in Wirtschaftsinformatik an Hochschulen (März 2017); Empfehlungen für Bachelor- und Masterprogramme im Studienfach Informatik an Hochschulen (Juli 2016) https://gi.de/service/publikationen/empfehlungen [Letzter Abruf: 05.10.2020].

[6] Nur die neueste Version 4 des e-CF, als EN 16234:1–2019 enthält die „transversal aspects“ sowie die gültige Weiterentwicklung. Bezugsquellen für den Standard in der empfohlenen englischen Fassung: https://www.ecompetences.eu/get-the-e-cf/ [Letzter Abruf: 05.10.2020]

Version 3 des e-CF erschien 2014 als CWA 16.234 und steht aus Dokumentationszwecken noch zur Verfügung: https://www.ecompetences.eu/e-cf-3-0-download/ [Letzter Abruf: 05.10.2020].

Ergebnis einer zweijährigen Arbeit von IKT- und HR-Experten aus verschiedenen europäischen und nationalen Organisationen und Unternehmen (u. a. Bitkom, e-Skills UK, CIGREF, IG Metall, Airbus, Michelin, Telekom). Sie arbeiteten unter dem Dach des CEN ICT Skills Workshop, der seinerseits durch die Europäische Kommission im Rahmen des Programms „e-Skills für das 21. Jahrhundert" unterstützt wurde. Rund um den e-CF, seine Ergänzungen und Weiterentwicklungen hat sich in den vergangenen Jahren ein umfassendes Ökosystem entwickelt. Der Kompetenzrahmen wird in Unternehmen zur betrieblichen Personal- und Kompetenzentwicklung genutzt, zunehmend auch zur Grundlage beruflicher Ausbildung wie akademischer Bildung. In einigen europäischen Ländern (z. B. Niederlande, Italien) ist die Nutzung des e-CF verpflichtend.

Den Kern des e-CF bildet die Darstellung von 41 Kompetenzen, die typischerweise an Arbeitsplätzen der Informations- und Kommunikationstechnologie (IT) erforderlich sind. Dazu gehören „Architecture Design" und „ICT Systems Engineering" genauso wie „Needs Identification" und „Information Security Management" (Abb. 1).

Dimension 1 5 e-CF areas	Dimension 2 41 e-Competences identified	Dimension 3 5 e-Competence proficiency levels				
		e-1	e-2	e-3	e-4	e-5
A. PLAN	A.1. Information Systems and Business Strategy Alignment				■	■
	A.2. Service Level Management			■	■	
	A.3. Business Plan Development			■	■	■
	A.4. Product / Service Planning		■	■	■	
	A.5. Architecture Design			■	■	■
	A.6. Application Design	■	■	■		
	A.7. Technology Trend Monitoring			■	■	■
	A.8. Sustainability Management			■	■	
	A.9. Innovating				■	■
	A.10. User Experience		■	■	■	
B. BUILD	B.1. Application Development	■	■	■		
	B.2. Component Integration		■	■	■	
	B.3. Testing	■	■	■	■	
	B.4. Solution Deployment	■	■	■		
	B.5. Documentation Production	■	■	■		
	B.6. ICT Systems Engineering			■	■	
C. RUN	C.1. User Support	■	■	■		
	C.2. Change Support		■	■		
	C.3. Service Delivery	■	■	■		
	C.4. Problem Management		■	■	■	
	C.5. Systems Management	■	■	■		

Abb. 1 Überblick (Auszug) European e-Competence Framework

Eine Kompetenz im e-CF besteht aus Namen und Beschreibung, den definierten Niveaus dieser Kompetenzen und ihren Beschreibungen sowie aus Beispielen für Wissen und Fertigkeiten, die Bestandteil der Kompetenz sein können. Die Kompetenzbeschreibung und die definierten Niveaus sind normativ, alles andere ist informativ (Abb. 2).

Mit Hilfe der e-CF Kompetenzen lassen sich typische Anforderungen einer Rolle oder eines Arbeitsplatzes in der IT genauso beschreiben, wie diejenigen Kompetenzen, die eine Mitarbeiterin, ein Mitarbeiter mitbringt oder die sie/er gerne erwerben möchte. Entscheidend ist dabei, dass die e-CF-Kompetenzen aus der Praxis heraus definiert wurden und werden. Kompetenz ist im e-CF allgemein definiert als „die nachgewiesene Fähigkeit, Wissen, Fertigkeiten und

Dimension 1 e-Comp. area	A. PLAN				
Dimension 2 e-competence: Title + generic description SHALL APPLY	A.6. Application Design Analyses, specifies, updates and makes available a model to implement applications in accordance with IS policy and user/customer needs. […] Ensures that all aspects take account of interoperability, usability, accessibility and security. Identifies a common reference framework to validate the models with representative users, based upon development models (e.g. iterative approach).				
Dimension 3	Level 1	Level 2	Level 3	Level 4	Level 5
e-Competence proficiency levels e-1 to e-5 SHALL APPLY	Contributes to the design and general functional specification and interfaces.	Organises the overall planning of the design of the application.	Accounts for own and others' actions in ensuring that the application is correctly integrated within a complex environment and complies with user/customer needs.	--	--
Dimension 4 Knowledge examples Knows/aware of/familiar with MAY APPLY	K1 requirements modelling and need analysis techniques K2 software developments methods and their rationale (e.g. prototyping, agile methods, DevOps concepts, reverse engineering, etc.)[…]				
Skills examples Is able to MAY APPLY	S1 identify customers, users & stakeholders S2 collect, formalise and validate functional and non-functional requirements […]				

Abb. 2 Beispiel Komptenz A.6: Application Design

Einstellungen anzuwenden, um beobachtbare Ergebnisse zu erzielen“[7]. Mit diesem ganzheitlichen Kompetenzbegriff beziehen sich Kompetenzen direkt auf die Aktivitäten am Arbeitsplatz und schließen komplexe menschliche Einstellungen und daraus resultierende Verhaltensweisen ein. Nur sie ermöglichen die erfolgreiche Anwendung von Wissen und Fähigkeiten und ihre Integration ist konstitutiv für alle im Kompetenzen im e-CF.

Mit den in der neuesten Version definierten „transversal aspects“ werden für alle Kompetenzen bestimmte Einstellungen bzw. zumindest die Berücksichtigung bestimmter Querschnittsthemen verpflichtend. Dabei geht es darum, sich passend zum jeweiligen Arbeits- bzw. Handlungskontext, bewusst und proaktiv in Bezug auf den jeweiligen Aspekt zu verhalten. Insgesamt sind sieben „transversal aspects“ definiert:

- Ethics
- ICT legal issues
- Security
- Sustainability
- Usability

Sowie natürlich

- Accessibility: „Accessibility is applicable to the design of products, devices, services or environments to ensure that they are usable by all, irrespective of their personal capacities. It is relevant to the extent to which products, systems, services, environments and facilities can be used by people from a population with the widest range of characteristics and capabilities to achieve a specified goal. For example, web accessibility allows people with visual impairment to gain access to online content such as webpages, electronic documents, and multimedia. Accessibility is also relevant, for example, when working in adverse conditions (such as noisy or badly illuminated environments) or stressful situations.“ [9] und
- Privacy: „Data privacy, also known as information privacy, is the ability an organisation or individual has to determine what data can be shared with third parties. The importance of protecting data privacy is underlined by the introduction of the European General Data Protection Regulation (GDPR) law on data protection and privacy for all individuals.“ [9]

[7] „Competence is a demonstrated ability to apply knowledge, skills and attitudes for achieving observable results.“ [9].

Natürlich wird sich in der Praxis die Berücksichtigung von accessibility, privacy und den anderen „transversal aspects“ bei unterschiedlichen Kompetenzen, in unterschiedlichen Situationen je nach Anforderungen sowie Beteiligten auch unterschiedlich ausdrücken. Um die beschriebenen Konflikte zu vermeiden und Accessibility wie Privacy „by design“ sicherzustellen, müssen diese Aspekte vor allem in den frühen Phasen von Entwicklungsprozesse, und damit bei den korrespondierenden Tätigkeiten und Kompetenzen wie beispielsweise „Architecture“ oder „Application Design“, „Needs Identification“ oder auch „Information Systems Governance“ explizit als Anforderungen berücksichtigt werden. Dies heißt zunächst einmal, dass ein Bewusstsein für die mit den „transversal aspects“ beschriebenen Anforderungen vorhanden ist. In Bezug auf Accessibility bedeutet dies vor allem auch „unübliche“ Nutzer:innen und Nutzungsszenarien zu imaginieren oder besser noch gerade Nutzer:innen mit Einschränkungen unterschiedlicher Art zu ihren Anforderungen zu befragen und in den Entwicklungsprozess einzubeziehen. Denn dann würde beispielsweise (vgl.o.) schnell deutlich, dass nicht alle Nutzer:innen von Videokonferenz-Diensten mit der Funktion „Sprecher:in automatisch hervorgehoben“ glücklich sind. In Bezug auf Privacy gilt es vor allem von einem technisch-funktionalen Verständnis der Verarbeitung von Daten wegzukommen hin zu wenigstens punktuell inhaltlichen Fragen danach, ob die jeweiligen Daten überhaupt erhoben werden dürfen bzw. inwieweit ihre Speicherung und Verarbeitung und/oder Verschlüsselungsmechanismen sinnvoll sind, Für die IT-Fachkräfte wie die Entscheider:innen stellen die „transversal aspects“ natürlich eine Herausforderung dar, zumal eine bessere Integration in Aus- und Weiterbildung sowie Kompetenz- und Organisationsentwicklung vielerorts noch aussteht.

Trotzdem ist mit der Betonung dieser Querschnittsthemen im europäischen e-Competence Framework ein wichtiger Schritt in Richtung Privacy und Accessibility „by design“ getan, der zukünftig hoffentlich dazu beiträgt, Datenschutz wie Zugänglichkeit von Software und IT-Systemen zu verbessern und Konflikte zwischen ihnen sowie zu anderen Anforderungen zu vermeiden.

Literatur

1. Rogalla, I., Reichert, T.: Potenziale von mobilem Internet und digitalen Technologien für die bessere Teilhabe von Menschen mit Behinderungen. Gutachten im Auftrag des Deutschen Bundestages vorgelegt dem Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag. TAB, Berlin (2017) [unveröffentlicht]

2. Rogalla, I., Reichert, T.: Potenziale von mobilem Internet und digitalen Technologien für die bessere Teilhabe von Menschenmit Behinderungen. Vertiefende Betrachtung des Innovationsprozesses: Akteure, Produktanforderungen, Entwicklungsphasen, Marktbesonderheiten, Geschäftsmodelle. Gutachten im Auftrag des Deutschen Bundestages vorgelegt dem Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag. TAB, Berlin (2018) [unveröffentlicht]
3. Masur, P.K., Teutsch, D., Dienlin, T.: Privatheit in der Online-Kommunikation. In: Schweiger, W., Beck, K. (Hrsg.) Handbuch Online-Kommunikation. Springer ReferenceSozialwissenschaften. https://doi.org/10.1007/978-3-658-18017-1_16-1 (2018) Zugegriffen: 9. Okt. 2020
4. Berliner Beauftragte für Datenschutz und Informationsfreiheit: Hinweise für Berliner Verantwortliche zu Anbietern von Videokonferenz-Diensten. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf (Version 1.0 vom 3.Juli 2020). Zugegriffen: 9. Okt. 2020
5. Bundesamt für Sicherheit in der Informationstechnik (BSI): Kompendium Videokonferenzsysteme KoViKo – Version 1.0.1. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Kompendium-Videokonferenzsysteme.pdf?__blob=publicationFile&v=4 (2020). Zugegriffen: 9. Okt. 2020
6. Borgstedt, S., Möller-Slawinski, H.: Digitale Teilhabe von Menschen mit Behinderung. Aktion Mensch e. V. und SINUS-Institut, Bonn (2020)
7. t3n – News: Apple soll Plan zur Vollverschlüsselung von iCloud-Backups nach FBI-Beschwerde aufgegeben haben. https://t3n.de/news/apple-plan-vollverschluesselung-1244459/ 25.01.2020 Zugegriffen: 17. Aug. 2020
8. Zuboff, S.: Das Zeitalter des Überwachungskapitalismus. Campus, Frankfurt (2018)
9. EN 16234-1:2019: e-Competence Framework (e-CF) 4.0 – A common European Framework for ICT Professionals in all industry sectors – Part 1: Framework

Fortentwicklung des Datenschutzrechts

Datenschutzrechtliche Gestaltungsmöglichkeiten jenseits der Ermächtigung des Individuums: Die Multi-Stakeholder-Datenschutz-Folgenabschätzung

Murat Karaboga

Zusammenfassung

Die fortschreitende Digitalisierung umfasst immer mehr Bereiche des Alltagslebens. Die damit verbundenen Gefahren waren ein wesentlicher Grund für die Entstehung der Datenschutz-Grundverordnung (DS-GVO), mit der die Ermächtigung des Individuums verfolgt wurde. Ähnlich wie schon in der Vergangenheit in anderen Bereichen (etwa im Verbraucher- oder Umweltschutz), ist angesichts der komplexen Digitalisierungsprozesse in den letzten Jahren jedoch in zunehmendem Maße die Frage in den Vordergrund gerückt, ob und inwiefern sich ein wirksamer Datenschutz auf Grundlage eines individualistischen Konzepts in Form der Ermächtigung des Individuums realisieren lässt. Vor dem Hintergrund dieser Debatten diskutiert der vorliegende Beitrag die Herausforderungen, denen sich individualistische Datenschutz-Konzeptionen ausgesetzt sehen und anschließend anhand ausgewählter Teilbereiche des Datenschutzrechts Lösungsansätze, die über die Fokussierung auf das Individuum hinausgehen und die als eine Art Mittelweg zwischen individualistischen und kollektivistischen Ansätzen verstanden werden können. Im Zentrum der Gestaltungsvorschläge steht die sog. Multi-Stakeholder-Datenschutz-Folgenabschätzung, die gemeinsam mit weiteren überindividuellen Maßnahmen geeignet wäre, die Gefahren moderner Datenverarbeitungen in angemessener Weise zu adressieren.

M. Karaboga (✉)
Fraunhofer-Institut für System- und Innovationsforschung ISI, Competence Center Neue Technologien, Karlsruhe, Deutschland
E-Mail: murat.karaboga@isi.fraunhofer.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_14

Schlüsselwörter

Datenschutz • Privatheit • Schutz personenbezogener Daten • Liberal-individualismus • Kollektivschutz • Soziale Privatheit

1 Einführung und Fragestellung

Die Frage, inwieweit der geltende Datenschutzrahmen überhaupt oder noch dafür geeignet ist, einen angemessenen Schutz vor den mannigfaltigen Gefahren moderner Datenverarbeitungen zu gewährleisten, ist in den vergangenen Jahren zunehmend in den Mittelpunkt der Privatheits- und Datenschutzdebatte gerückt. Kritisiert wird insbesondere, dass herrschende Datenschutzgesetze auf Grundlage einer als überholt angesehenen liberal-individualistischen Perspektive das Individuum fokussieren und damit gleich in mehrfacher Hinsicht Privatheit und Datenschutz nur unzureichend erfassen und schützen. Die Vielzahl an Texten zur Kritik an der liberal-individualistischen Aufladung von Privatheitskonzepten lässt sich grob in zwei Kategorien unterteilen. Der erste Literaturstrang befasst sich stärker mit dem Wert bzw. der Bedeutung, welcher Privatheit beigemessen wird. In diesem Literaturstrang wird insbesondere das individualistische anthropologische Grundverständnis kritisiert und etwa danach gefragt, ob Privatheit das Individuum schützt, wie Privatheit und Individualität zusammenhängen, worin der überindividuelle Wert von Privatheit liegt und ob Privatheit den selbstbestimmten Rückzug aus der Gesellschaft meint oder auch die selbstbestimmte Teilhabe meinen kann bzw. vielmehr meinen muss. Der zweite Literaturstrang befasst sich hingegen stärker mit den rechtlichen und praktischen Auswirkungen liberal-individualistisch aufgeladener Datenschutzgesetze. Hier wird einerseits gezeigt, dass die praktische Gestaltung von Datenschutzgesetzen die mit den erlassenen Gesetzen verfolgten Schutzziele konterkariert [1] und auf dieser Grundlage andererseits diskutiert, ob und inwiefern bestimmte datenschutzrechtliche Elemente den erwünschten Schutz besser gewährleisten könnten [2, 3]. Im vorliegenden Beitrag fokussiere ich auf den zweiten Literaturstrang und führe die bestehenden Arbeiten in Richtung der Konzeption konkreter Datenschutzrechte hin. Die forschungsleitende Frage dabei ist, wie Datenschutzrechte ausgestaltet werden könnten, die über die Ermächtigung des Individuums hinausgehen und mit denen die Adressierung der Folgen moderner Datenverarbeitungen besser gelingen könnte, denn die bestehende Literatur behandelt das Thema aktuell auf einer abstrakt-konzeptionellen Ebene [4, 5] oder beachtet auf isolierte Weise

nur einzelne datenschutzrechtliche Elemente [6, 7]. Um die genannte Frage zu beantworten führe ich zunächst anhand einer Diskussion von Teilbereichen der DS-GVO näher aus, worin sich der liberal-individualistische Fokus der Datenschutzgesetzgebung genau äußert. Im Anschluss zeige ich auf, in welcher Hinsicht die liberal-individualistischen Elemente der Datenschutzgesetzgebung kritisiert werden und weshalb die Idee der Ermächtigung des Individuums durch Datenschutzrechte regelmäßig in der Kritik steht. Schließlich diskutiere ich konkrete datenschutzrechtliche Gestaltungsmöglichkeiten, die über die Ermächtigung des Individuums hinausgehen. Hierbei fokussiere ich insbesondere auf das Element einer sog. Multi-Stakeholder-Datenschutz-Folgenabschätzung und zeige auf, wie sich deren Vorgaben mit anderen überindividuellen datenschutzrechtlichen Elementen zu einem soliden Schutzgerüst verbinden lassen könnten, das zur Adressierung der Gefahren moderner Datenverarbeitungen besser geeignet wäre, als das gegenwärtige Schutzregime.

2 Liberal-individualistische Elemente in der DS-GVO

Trotz der inzwischen vorhandenen Fülle an Kritik am liberal-individualistischen Datenschutz-Paradigma, bleibt in aller Regel unklar, welche datenschutzrechtlichen Elemente dem Paradigma der individuellen Kontrolle hinzugezählt werden. Mittels der folgenden Aufzählung bzw. Diskussion sollen anhand der einschlägigen Literatur [1–3, 8] nun daher zunächst die zentralen, dem liberal-individualistischen Datenschutz-Paradigma zuzuordnenden datenschutzrechtlichen Elemente der DS-GVO erörtert werden:

- Datenschutz-Grundsatz der Zweckbindung (Art. 5 (1) b)
- Datenschutz-Grundsatz der Datenminimierung (Art. 5 (1) c)
- Einwilligung (insb. Art. 4 (11), Art. 6 und 7)
- Informations- und Transparenzvorgaben bei der Verarbeitung personenbezogener Daten (Art. 12–14)
- Betroffenenrechte, das Auskunftsrecht (Art. 15), das Recht auf Berichtigung (Art. 16), auf Löschung (Art. 17), auf Einschränkung der Verarbeitung (Art. 18), das Recht auf Datenübertragbarkeit (Art. 20) sowie das Widerspruchsrecht (Art. 21)
- Einwilligung in automatisierte Einzelentscheidungen im Einzelfall einschließlich Profiling (Art. 22 (2) c)
- Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Art. 34)
- Rechtsbehelfe (Art. 77–79) und Haftung (Art. 82)

Die *Zweckbindung* stellt zusammen mit dem Recht auf Einwilligung ein zentrales Prinzip des EU-Datenschutzrechts dar. Ebenso wie die Einwilligung, ist auch sie eng verwandt mit dem Grundrecht auf informationelle Selbstbestimmung bzw. der ihr zugrunde liegenden Idee der persönlichen Kontrolle von Datenverarbeitungen [9]. Mit der Zweckbindung soll sichergestellt werden, dass ein Individuum Sicherheit darüber hat, dass eine Verarbeitung nur zu dem vom Individuum eingewilligten oder dem gesetzlich erlaubten Zweck dient [10]. Die Beschränkung der Datenverarbeitung auf das zur Erreichung des angegebenen Zwecks erforderliche Maß, wäre ohne die Angabe jenes Zwecks nicht möglich, sodass die Einwilligung wie auch die anderen Erlaubnistatbestände sowie die Datenschutz-Grundsätze nicht mehr wirksam wären [11]. Das datenschutzrechtliche Prinzip der *Datenminimierung* etwa, bindet die Verarbeitung personenbezogener Daten an den jeweiligen Zweck und verfolgt damit das Ziel, dass keine für die Erreichung eines zuvor bestimmten Zwecks nicht notwendigen personenbezogenen Daten verarbeitet werden: „Wenn etwa der Browser-Fingerprint des Kundenrechners, die zuvor besuchten Seiten sowie Alter und Geschlecht nicht für die Erfüllung eines E-Commerce-Vertrags erforderlich sind, ist die Erhebung dieser Daten zu unterlassen.“ [12] Damit ist das Zweckbindungsprinzip das zentrale Mittel zur „Erzeugung von Kontrollierbarkeit der Informationserhebung, -verarbeitung und -nutzung sowie der dabei verwendeten technischen wie nicht-technischen Mittel, indem es wohlgeordnete Organisationsstrukturen und Prozesse erzeugt, die zugleich transparent gemacht werden können – den Organisationen selbst, vor allem jedoch den Betroffenen und den Aufsichtsbehörden.“ [13]

Deren de lege lata enge Verzahnung mit und der übermäßige Fokus auf die individuelle Einwilligung bzw. individuelle informationelle Selbstbestimmung lassen sie zwar als liberal-individualistische Grundsätze erscheinen, doch sind sowohl das Zweckbindungs- als auch das Datenminimierungsprinzip darüber hinaus auch allgemeine Gestaltungskriterien informationstechnischer Systeme. Gerade die Zweckbindung „dient als konzeptionelle und operationale Klammer um den Prozess von Informationserhebung, -verarbeitung und Entscheidungsfindung, indem sie als Konstante in einem dynamischen Umfeld wirkt und damit einen festen Anker für die Prüfung sowohl der Handlungen wie der eingesetzten Mittel bietet.“ [13]

Der *Einwilligung* kommt im Datenschutzrecht zusammen mit dem Zweckbindungsprinzip eine zentrale Stellung zu: „Die Einwilligung ist der genuine Ausdruck des Rechts auf informationelle Selbstbestimmung.“ [10] Dem Recht auf Einwilligung ist es zu verdanken, dass das seit Mitte der 1970er-Jahre bestehende Problem ausufernder Spezialregelungen und Schutzlücken im Datenschutzrecht adressiert werden konnte [14, 15]. Ein wesentlicher Bestandteil dieses Rechts ist

die Vorstellung, dass die Einwilligung, etwa gemäß Art. 4 (11) DS-GVO, „in informierter Weise“ zu erfolgen hat.

Die detaillierte Bestimmung dessen, was unter „in informierter Weise“ zu verstehen ist, erfolgt in den Artikeln 12 bis 14 DS-GVO. Die informationelle Selbstbestimmung soll insbesondere dadurch erleichtert werden, dadurch dass alle Informationen, die dem Betroffenen dargestellt werden, *in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln* (Art. 12 (1)) sind. In den Folgeartikeln ist schließlich der lange Informationskatalog geregelt, der dem Betroffenen bereitzustellen ist, sofern die Daten beim Betroffenen (Art. 13) oder nicht beim Betroffenen (Art. 14) erhoben werden. Darunter fallen beispielsweise Namen und die Kontaktdaten des Verantwortlichen (Art. 13 (1) a und 14 (1) a), die Verarbeitungszwecke (Art. 13 (1) c und Art. 14 (1) c) oder die geplante Speicherdauer der Daten (Art. 13 (2) a bzw. Art. 14 (2) a).

Einen weiteren Eckpfeiler im liberal-individualistischen Datenschutzrechtsverständnis bildet der Komplex der *Betroffenenrechte.* Mit diesen soll gewährleistet werden, dass die von einer personenbezogenen Datenverarbeitung betroffenen Personen Mitwirkungsmöglichkeiten an der Datenverarbeitung erhalten und diese in ihrem Sinne beeinflussen können. Das Auskunftsrecht bildet dabei die Grundlage für die Wahrnehmung der weiteren, sog. Mitwirkungsrechte (d. h., die Rechte auf Berichtigung, Löschung, Sperrung und Widerspruch), indem sie es dem Betroffenen erlaubt, zu wissen, welche auf die eigene Person bezogenen Daten aus welcher Quelle stammen, zu welchen Zwecken sie verwendet und an wen sie ggf. transferiert werden. Der Idee nach soll sie als sog. *Instrument vorgelagerten Rechtsschutzes* die laufende Kontrolle der Verwendung der eigenen personenbezogenen Daten erlauben, sodass die Möglichkeit eines potenziellen negativen Eingriffs in die informationelle Selbstbestimmung bereits vorab sichtbar wird und der Betroffene entsprechende Maßnahmen ergreifen kann [10]. Ein Beispiel wäre, dass ein mögliches Fehl-Scoring einer Person durch die SCHUFA dadurch verhindert wird, dass jene Person zuvor Gebrauch von ihrem Auskunftsrecht macht, dadurch fehlerhafte Daten entdeckt und diese berichtigen, löschen oder die Verarbeitung einschränken lässt, sodass keine Fehlberechnung stattfindet und auch keine weiteren Schäden entstehen.

Trotz der zentralen Rolle der Einwilligung in der DS-GVO sind Verarbeitungen auch ohne diese zulässig. Dies betrifft insb. die Buchstaben b) bis f) des Artikels 6 der DS-GVO. Insbesondere für die Fälle von Art. 6 e) und f) sieht das *Widerspruchsrecht* die Möglichkeit des Opt-out vor, indem die betroffene Person ihre überwiegenden Interessen bekannt macht [10].

Mittels *Rechtsbehelfen* (Art. 77–79 DS-GVO) sollen die Betroffenen schließlich in die Lage versetzt werden, eine Verletzung ihrer Datenschutzrechte vor Gericht zu bringen und gegebenenfalls einen Schadensersatz (Art. 82 DS-GVO) einzuholen.

3 Kritik an liberal-individualistischen Datenschutzrechten

Konfrontiert ist der im liberal-individualistischen Datenschutzparadigma eingebettete Fokus auf die Ermächtigung des Individuums mit mehreren Problemkomplexen. Erstens findet bereits seit Jahrzehnten eine anhaltende *Überforderung der Individuen* statt, die angesichts omnipräsenter Datenverarbeitungen in einer in zunehmendem Maße digitalisierten Welt nur noch größere Ausmaße annehmen wird. Zweitens entstehen neue Gefahren im Zuge der Verbreitung von Big Data-Analysen, die personenbezogene Entscheidungen und Ergebnisse auch ohne die Nutzung personenbezogener Daten ermöglichen können, sodass die Gewährleistung *der informationellen Selbstbestimmung im Kontext moderner Datenanalyseverfahren unmöglich* wird.

3.1 Überforderung des Individuums

Das Problem der zunehmenden Überforderung des Individuums basiert auf vielen Ursachen und stellt eine auf absehbare Zeit unumkehrbare Entwicklung dar [16]. Immer mehr Bereiche des Lebens werden verdatet, indem eine Verknüpfung der digitalen und analogen Welt mittels Sensoren stattfindet. Im Ergebnis nimmt die Menge erhobener personenbezogener Daten enorm zu. Die auf diese Weise erzeugte Masse an Daten kann auf unbegrenzte Zeit gespeichert werden, da die Speicher-Kosten inzwischen sehr gering sind [17, 18]. Da zudem immer mehr Bereiche des Lebens digitalisiert werden, fällt es den Individuen zunehmend schwerer, sich der ständigen Erhebung personenbezogener Daten zu entziehen. Ein Anspruch oder gar Recht auf Offline-Alternativen ist politisch nicht in Sicht [19]. Lange Zeit erstreckte sich die Erhebung personenbezogener Daten auf Name, Wohnort, Telefonnummer usw. Durch den Einsatz moderner Sensortechnik und durch das Zusammenwachsen von digitaler und analoger Welt nimmt nicht nur die Datenmenge zu, sondern auch die Verschiedenheit und Aussagekraft der erhobenen Daten. Möglich werden so extrem detaillierte Einblicke in vielerlei individuelle Lebensbereiche und Alltagspraktiken [20].

Sehr tiefgehende Rückschlüsse über Individuen werden allerdings nicht nur mittels Sensorik und unmittelbarer Datenerhebung möglich, sondern auch durch fortschrittliche Verarbeitungsmethoden, deren genaue Funktionsweise das Verständnis der Betroffenen, aber zunehmend auch das Verständnis selbst der für eine Verarbeitung Verantwortlichen übersteigt [21]. Zudem werden personenbezogene Daten auf für Außenstehende, d. h. insbesondere für Betroffene, intransparente Weise, weltweit über Datenbroker gehandelt und aus verschiedensten Quellen zusammengeführt [22]. Sowohl moderne Verarbeitungsmöglichkeiten als auch die Nutzungspraktiken anderer Nutzerinnen und Nutzer digitaler Technologien und Dienste haben Auswirkungen auf die individuelle Privatheit, indem Informationen zum Teil entgegen dem Wunsch eines Individuums über soziale Kontexte hinweg zirkulieren [23]. Personenbezogene Daten legen dabei für den Einzelnen unüberschaubare Strecken zurück und passieren auch die Hoheitsgebiete von Staaten mit einem problematischen Datenschutzniveau, die unerlaubten Zugriff auf die Daten erhalten [24]. Im Ergebnis dieser Entwicklungen sind die Betroffenen damit konfrontiert, immer mehr datenschutzrelevante Entscheidungen in Bezug auf immer mehr und zunehmend wichtigere Bereiche ihres Lebens treffen zu müssen [25], die sie immer schlechter überblicken können [16, 25].

Damit die Betroffenen ihre Person betreffende Datenverarbeitungen überblicken und an diesen mitwirken können, sind Verarbeiter zu Transparenz gegenüber den Betroffenen verpflichtet, die in der Regel in Form von Datenschutzerklärungen erfolgt. Sobald datenverarbeitende Prozesse allerdings wirklich transparent, d. h. umfassend hinsichtlich der stattfindenden Verarbeitungen dargestellt werden, sind die Betroffenen meist überfordert. Der Wunsch der Betroffenen nach mehr Transparenz über immer komplexer werdende Verarbeitungsprozesse einerseits und nach einer einfach verständlichen, kurzen Darlegung dieser Komplexität andererseits, sind widerstreitende Ziele und verlangen nach einem Kompromiss. Beides gleichzeitig zu erreichen wird nicht möglich sein, weswegen Transparenzanforderungen unter Kritik stehen [26, 27]. Zuletzt hatten sich EU-Kommission und EU-Parlament während der Datenschutzreform die Verbesserung von Transparenz vorgenommen [28, 29]. Die bisherigen Erfahrungen mit der Anwendung der DS-GVO demonstrieren, dass wesentliche Verbesserungen weder im Hinblick auf die informierte Einwilligung [30, 31] festzustellen sind, noch im Hinblick auf die Wahrnehmung der Auskunftsrechte [32].

Dass ein Großteil der Betroffenen die Datenschutzerklärungen der von ihnen genutzten datenverarbeitenden Dienste vor einer Einwilligung nicht durchliest,

ist ein in diesem Zusammenhang lange bekanntes Problem. Datenschutzerklärungen gelten für die meisten Menschen als zu komplex und zu lang.[1] Aufgrund der vielen zu treffenden Nutzungs- bzw. Einwilligungsentscheidungen, die mittels individueller Aufmerksamkeits- und Zeitressourcen nicht zu bewältigen sind, entsteht schließlich das Problem der *Ermüdung* hinsichtlich der Zustimmung zu einer Verarbeitung *(consensual exhaustion).* Im Ergebnis willigen die meisten Nutzerinnen und Nutzer in die Nutzung eines Dienstes ein, ohne dass sie sich weitergehende Gedanken über die Konsequenzen machen. Entscheidend ist, ob sich mit der Nutzung eines Dienstes bestimmte kurzfristige Bedürfnisse befriedigen lassen und nicht, ob aufgrund von Privatheitsgefährdungen in der Zukunft möglicherweise ein individueller oder auch die Gesellschaft betreffender Nachteil erwachsen kann. Zudem manipulieren Verantwortliche mittels vielfältiger Design-Entscheidungen (sog. *nudging,* bzw. auf Deutsch: Anstupsen) das Nutzerverhalten in die von ihnen gewünschten Richtungen und bringen Betroffene so beispielsweise dazu, mehr personenbezogene Daten preiszugeben [25, 26, 34, 35].

Dass viele Datenschutzerklärungen gar nicht darauf eingehen, welche künftigen Verarbeitungen stattfinden werden, da sie dies zum Zeitpunkt der Erstellung der Datenschutzerklärung selbst gar nicht wissen können, stellt eine weitere Herausforderung dar. Folglich kann auch keine selbstbestimmte Einwilligung erfolgen, da die Betroffenen dies noch weniger wissen können [1].

Über das Thema Einwilligung hinaus gestaltet sich die Wahrnehmung von z. B. Auskunfts-, Korrektur- oder Löschungswünschen als umso schwieriger, je mehr Daten (teils gänzlich ohne das Wissen der Betroffenen) bei verschiedenen Verarbeitern lagern [24]. Zudem verpflichtet die bloße Existenz der Betroffenenrechte die Verantwortlichen zu keiner Aktion, die nicht vom Betroffenen initiiert wird. Damit hängt ihre Effektivität vom Interesse der Betroffenen an der tatsächlichen Ausübung ihrer Rechte ab – doch gerade dieses Interesse wurde bereits seit längerem angezweifelt [36]. So wurde zwar nach Inkrafttreten der DS-GVO ein Anstieg an Auskunftsersuchen festgestellt, die Zahlen pendelten sich seither allerdings auf einem sehr niedrigen Niveau ein [37, 38].

[1] Eine Studie aus dem Jahr 2008 rechnete aus, dass eine durchschnittliche US-amerikanische Person, die alle Datenschutzerklärungen aller von ihr genutzten datenverarbeitenden Produkte lesen möchte, jährlich 201 h (das sind mehr als acht volle Tage bzw. auf achtstündige Arbeitstage gerechnet 25 Arbeitstage) mit dieser Aufgabe verbringen würde [33].

3.2 Unmöglichkeit der informationellen Selbstbestimmung im Kontext moderne Datenanalyseverfahren (Big Data-Analysen)

Die zweite große Herausforderung, mit der das liberal-individualistische Datenschutz-Paradigma konfrontiert ist, stellen moderne Datenanalyseverfahren dar. Diese erschweren die informationelle Selbstbestimmung nicht nur, sondern machen sie bisweilen unmöglich.

Bei der Nutzung personenbezogener Daten für vielfältige Zwecke nehmen das Data-Mining und das Profiling eine zentrale Rolle ein. Während der Begriff des Data-Mining eher den Aspekt der systematischen Anwendung statistischer Auswertungsmethoden (heutzutage in der Regel und auch im Rahmen dieser Schrift etwas verkürzt als Big Data-Analysen bezeichnet) auf Datenbestände umfasst [39], wird mit Profiling die Anwendung der durch Data-Mining erzielten Ergebnisse in Form von Wahrscheinlichkeitswerten *(Scores)* auf personen- oder gruppenbezogene Entscheidungsprozesse bezeichnet [40, 41].[2] Ein sehr verbreiteter Einsatzzweck derartigen Scorings ist das Risikoprofiling bzw. die Risikobewertung z. B. im Rahmen der Vergabe von Krediten, wie sie in Deutschland seitens der Schutzgemeinschaft für allgemeine Kreditsicherung (SCHUFA) [42] und vergleichbarer Organisationen (etwa im Bereich der Flugsicherung) praktiziert wird [43]. Werbetreibende können auf Basis derartiger Wahrscheinlichkeitswerte ihr Klientel zunehmend zielgerichteter adressieren. Je fortschrittlicher die während des Data-Mining angewendeten Analysealgorithmen sind und je mehr Daten Gegenstand der Analyse sind, umso präzisere Ergebnisse werden möglich (ebd.).

Die DS-GVO setzt in Art. 22 dem Scoring Grenzen, indem automatisierte Entscheidungen im Einzelfall, die der betroffenen Person gegenüber rechtliche Wirkung entfalten oder sie in ähnlicher Weise beeinträchtigen können, nur unter besonderen Umständen zulässig sind. D. h., dass das Datenschutzrecht erst greifen kann, sobald ein Profil auf eine *identifizierbare Person* bezogen wird, deren Identität dem Verantwortlichen bekannt ist, wie es etwa im Kredit-Scoring der SCHUFA der Fall ist [44]. Nicht betroffen von der Regelung ist dagegen die Erstellung von Profilen über Personen, deren Identität dem Verantwortlichen nicht

[2] Bei Profiling geht es vor allem darum, Gruppenattribute zu identifizieren (Menschen die X tun, tun auch Y, aber nicht Z). Derartige Ergebnisse können also Fahrer von blauen PKWs sein, die z. B. täglich um 14 Uhr die Kirche und im Anschluss das Altersheim besuchen. Entsprechend sind die Daten nicht zwingend auf einzelne identifizierbare Individuen bezogen, weshalb sie auch nicht als personenbezogene Daten gelten [3].

bekannt ist. Denn Datenverarbeitungsprozesse rücken zum Teil weg vom Individuum *(Vorkommnis)* hin zur Identifikation algorithmisch generierter Gruppen auf Grundlage gemeinsamer Eigenschaften *(Typen),* damit eine gruppenspezifische Behandlung (bspw. Kundenansprache) ermöglicht bzw. optimiert wird. Ob und warum ein Individuum Teil einer Gruppe ist, bleibt den Betroffenen verborgen. Zudem besteht die Gefahr, dass das Zustandekommen und die Diskriminierung einer Gruppe sogar den Datenanalysten selbst niemals bekannt werden wird, da die zugrunde liegenden Berechnungen oftmals intransparent oder zu komplex sind [21]. Dadurch, dass derartige (Gruppen-)Profile nicht dem Datenschutz unterliegen, nehmen die Betroffenen auch keine Notiz von der erfolgten Profilierung. In der Folge können die von einem derartigen nicht-personenbezogenem Gruppenprofiling Betroffenen auch keine Maßnahmen gegen möglicherweise verzerrende Darstellungen ihrer selbst ergreifen – die datenschutzrechtlichen *Betroffenenrechte* greifen in diesen Fällen schlicht nicht [3].

Das Recht auf *Einwilligung* beispielsweise baut darauf, dass diese in Kenntnis über die Verarbeitungszwecke erfolgt. Das Prinzip der *Zweckbindung* allerdings ist bereits seit längerem durch die Praxis datenverarbeitender Unternehmen herausgefordert, die die Zweckbindung missachten und jene für einen Zweck erhobenen Daten auch für viele weitere Zwecke verarbeiten, indem personenbezogene Daten anonymisiert oder pseudonymisiert und somit den Vorgaben des Datenschutzrechts entzogen werden (bspw. seitens Suchdiensten, Sozialen Online-Netzwerken oder Datenaggregatoren und -händlern). Neu hinzugekommen ist die Gefahr moderner Big Data-Analyseverfahren, deren Ziel darin besteht, dass sich mögliche Nutzungszwecke erst durch vielfache Analyseschleifen ergeben. Insofern stehen sich das Zweckbindungsprinzip und Big Data konträr gegenüber, weil eine Zweckbindung immer dann nicht erfolgen kann, wenn sich der Zweck erst im Laufe einer Analyse ergibt [11]. Mit der Erosion der Zweckbindung im Zuge von Big Data-Analysen schwindet zudem auch die Möglichkeit der Schaffung transparenter Organisationsstrukturen und Prozesse. Dieser Aspekt betrifft außerdem nicht mehr nur die Betroffenen und Aufsichtsbehörden, sondern, in dem Maße, in dem die Komplexität von Verarbeitungen zunimmt, auch die Verantwortlichen selbst, die zwar Ergebnisse erhalten, aber selbst zunehmend weniger begreifen, wie und auf Grundlage welcher Daten und Berechnungen diese im Detail zustande gekommen sind [45]. Erschwerend kommt hinzu, dass Big Data-Analysen gruppen- und personenbezogene Ergebnisse, die vom Datenschutzrecht nicht umfasst sind [3, 46] auch dann nach sich ziehen können, wenn die Analyse ausschließlich auf nicht personenbezogenen, anonymisierten oder pseudonymisierten Daten beruht. Eine auf diese Weise betroffene Person kann

in die Verarbeitung gar nicht einwilligen oder eine selbstbestimmte Informationskontrolle praktizieren, weil sie zu keinem Zeitpunkt selbst Daten über sich preisgibt und vielfach auch gar nicht wissen kann, dass sie betroffen ist [27].

Dies betrifft in besonderer Weise die Gewährleistung des Prinzips der *Datenminimierung*. Denn das Prinzip der Datenminimierung bezieht sich ausschließlich auf personenbezogene Daten bzw. darauf, dass auf zulässige Weise erhobene personenbezogene Daten so früh wie möglich gelöscht, anonymisiert oder pseudonymisiert werden. Das bedeutet, dass das Prinzip der Datenminimierung immer dann nicht greift, wenn der Zweck einer Verarbeitung nicht bekannt ist, aufgrund von Anonymisierung bzw. Pseudonymisierung kein Personenbezug vorhanden ist oder sich der Personenbezug eines Datums erst im Ergebnis einer Big Data-Analyse ergibt. Zwar könnte mithilfe des Datenminimierungsprinzips eine radikale Begrenzung von Big Data-Analyseverfahren erfolgen, doch würden damit nicht nur potenziell unerwünschte Auswirkungen von Big Data-Verfahren vermieden, sondern auch potentiell erwünschte Auswirkungen [41].

4 Datenschutzrechtliche Gestaltungsmöglichkeiten jenseits der Fokussierung auf die Ermächtigung des Individuums

Auf welche Weise könnte also informationelle Privatheit im Recht verbrieft werden, sodass die zentrale Rolle des Individuums zwar erhalten bleibt, aber zugleich auch die Grenzen der individuellen informationellen Selbstbestimmung berücksichtigt werden?

4.1 Konzeptionelle Vorüberlegungen

Zur Beantwortung dieser Frage konzentriere ich mich im Folgenden auf den in den letzten Jahren zunehmend prominenter gewordenen Ansatz, einen Teil der Verantwortung zur Gewährleistung des Datenschutzes weg von den Betroffenen hin zu anderen Entitäten – darunter insbesondere die Verantwortlichen, aber auch Vertreter von Betroffeneninteressen – zu übertragen [47–50]. Viele der Autorinnen und Autoren, die diesen Ansatz vertreten, gehen davon aus, dass das Rechtssystem zwar durchaus am Grundsatz festhalten sollte, dass das Individuum im Mittelpunkt des Rechts steht. Des Weiteren gehen sie aber auch davon aus, dass die absehbaren technischen und sozialen Veränderungen auf einem Meta-Level ansetzen, wo es weniger um das Individuum als solches, denn um Strukturen geht, die

sowohl ein einzelnes Individuum betreffen als auch darüber hinaus reichen und die Gesellschaft als Ganzes betreffen können. Deshalb wird vorgeschlagen, den Problemen nicht nur individuell, sondern vor allem kollektiv zu begegnen [49]. Entsprechend wird vom überwiegenden Teil dieser Autorinnen und Autoren auch nicht die vollständige Ersetzung der gegenwärtigen, am Individuum fokussierenden Datenschutzgesetze gefordert, sondern die Ergänzung bestehender Gesetze um nicht-individualistische Schutzmomente [49, 51, 52].[3]

Die Forderung nach der Übertragung eines größeren Teils der Verantwortung hin zu den Verarbeitern baut auf der Feststellung auf, dass sie es sind, die die Rahmenbedingungen festlegen, welche die Konstituierung des Subjekts je nach Technologie und Kontext in unterschiedlichem Maße beeinflussen. Allerdings gestaltet sich die Beantwortung der Frage, inwiefern nichtstaatliche Akteure stärker in die Verantwortung genommen werden können, nicht als trivial. Grundsätzlich gilt, dass aufgrund seiner besonderen Machtposition nur der Staat gegenüber den Bürgerinnen und Bürgern grundrechtsverpflichtet ist. Sofern Individuen Akteuren des Marktes gegenüberstehen, handelt es sich also im rechtlichen Sinne grundsätzlich um ein Verhältnis Gleicher unter Gleichen, da auch Marktakteure (also auch privatwirtschaftliche Unternehmen) ihrerseits Träger von Grundrechten sind. Während das oben skizzierte Verständnis nahelegt, im Falle eines Machtungleichgewichts zwischen Individuen einerseits und insbesondere marktbeherrschenden privatwirtschaftlichen Unternehmen andererseits, letzteren zusätzliche Pflichten aufzuerlegen, um einen Missbrauch ihrer Machtstellung zu verhindern, war die Umsetzbarkeit dieses Vorhabens aus juristischer Perspektive längere Zeit umstritten. Dies änderte sich im Laufe der letzten Jahre mit einigen neueren Urteilen[4] des Bundesverfassungsgerichts. Diese besagen im Grundsatz, dass anderen privaten Akteuren insbesondere dann zusätzliche grundrechtsschützende Pflichten auferlegt werden können, wenn diese durch die Organisation von Kommunikationsräumen in vergleichbare Pflichten und Garantenstellungen hineinwachsen, wie sie ansonsten nur der Staat wahrnimmt [31].

[3] Für weniger hilfreich halte ich hingegen den Vorschlag hinsichtlich der Einführung von Gruppenrechten in das Datenschutzrecht. Zwar kann diese Frage aus Platzgründen an dieser Stelle nicht erschöpfend erörtert werden, doch ist die Umsetzung von Gruppenrechten bereits bei klar identifizierbaren Gruppen mit zahlreichen Schwierigkeiten konfrontiert [53]. Im Falle von algorithmisch generierten Gruppen potenzieren sich diese noch weiter, sodass sie praktisch kaum infrage kommen dürften [45, 54].

[4] BVerfGE 128, 226 (Fraport); BVerfG, NJW 2015, 2485 (Bierdosen-Flashmob; BVerfGE 148, 267 (Stadion-Verbot); BVerfG, NJW 2019, 1935 (1936) (III. Weg).

Über die Verlagerung von Verantwortung hin zu den Verarbeitern hinaus, kann auch die Forderung nach einer verstärkten Kontrolle der Einhaltung der Regelungen seitens unabhängiger Aufsichtsbehörden sowie die kollektive Unterstützung der Individuen bei schwierigen Entscheidungen und Handlungen (beispielsweise durch Verbraucherschutzorganisationen, an denen bestimmte Betroffenenrechte in einem bestimmten Rahmen freiwillig abgetreten werden können) als Teil eines solchen überindividuellen Datenschutzes verstanden werden [49]. In ähnlicher Weise deuten Matzner und Richter auf ein demokratisch gesichertes *Standard*-Schutzniveau, das bereits im Normalzustand Raum für individuelle Privatheitspraktiken lässt, darüber hinaus aber auch kontextspezifische Spezialregelungen unterhalb und oberhalb des festgelegten Niveaus ermöglicht:

> „Die Idee [sic!] dass Individuen grundsätzlich das Recht haben, selbst über die Nutzung ihrer Daten zu bestimmen, bleibt wichtig und richtig. Notwendig ist aber ein Zusammenspiel aus Eigenverantwortung und kollektivem, demokratisch legitimiertem Schutz. Hier müssen mehrere Elemente ineinandergreifen: Ein interessengerechter Handlungsrahmen, der staatlich reguliert und durchgesetzt wird; in diesem Handlungsrahmen ein eigenverantwortlicher Selbstdatenschutz; und schließlich kollektive Prozesse der Aushandlung von Datenschutz unterhalb und oberhalb der staatlichen Ebene. Wenn Menschen selbst über den Umgang mit Informationen bestimmen, muss das nicht heißen [sic!] jede und jeder Einzelne bestimmt egozentrisch für sich. Auch Gruppen, Gemeinschaften, Gesellschaften, Angestellte einer Firma, Mitglieder eines Berufsverbandes, Bürger eines demokratischen Rechtsstaats und viele mehr können auf überindividueller Ebene für sich selbst bestimmen.“ [55]

Die Orientierung der gesetzlichen Regelungen an den für eine Verarbeitung Verantwortlichen ist kein Novum, sondern bildete den Ausgangspunkt der Datenschutzdiskurse der 1970er-Jahre. Der Fokus auf das Individuum kam erst im Laufe der Zeit hinzu und verdrängte nach und nach die vorherigen Schutzmomente. Davon zu sprechen, dass das EU-Datenschutzrecht einem liberal-individualistischen Datenschutz-Paradigma folgt, heißt aber auch nicht, dass keine nicht-individualistischen Elemente enthalten sind. Zu diesen können nach Sloot [2, 49] folgende Elemente der DS-GVO hinzugezählt werden:

- Die Datenschutzprinzipien bzw. -grundsätze („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“, „Zweckbindung“, „Datenminimierung“, „Richtigkeit“, „Speicherbegrenzung“ sowie „Integrität und Vertraulichkeit“) (Art. 5 DS-GVO)
- Sondervorschriften bei der Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DS-GVO)

- Informations- und Transparenzvorgaben bei der Verarbeitung personenbezogener Daten (Art. 12–14 DS-GVO)
- Vorgaben im Kontext automatisierter Einzelentscheidungen (Art. 22 DS-GVO)
- Vorgaben zur Datensicherheit zur Durchführung angemessener technischer und organisatorischer Maßnahmen (Art. 32 DS-GVO)
- Vorgaben zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DS-GVO)
- Allgemeine Vorgaben zur Rechenschaftspflicht und der Verantwortung der für die Verarbeitung Verantwortlichen (Art. 24 DS-GVO)
- Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DS-GVO)
- Vorgaben zur Zusammenarbeit mit den Datenschutzaufsichtsbehörden (Art. 31 DS-GVO)
- Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 und 34 DS-GVO)
- Datenschutz-Folgenabschätzung und vorherige Konsultation (Art. 35 und 36 DS-GVO)
- Beachtung der Regelungen bei der Übermittlung personenbezogener Daten in Drittländer (Art. 44–49 DS-GVO)
- Ziel von Sanktionen und Geldbußen bei Nichteinhaltung der Vorgaben (Art. 83–84 DS-GVO)

Zudem regeln die Art. 51–76 DS-GVO die Befugnisse der Datenschutzaufsichtsbehörden, denen die Rolle der Überwachung der Einhaltung der Verarbeiterpflichten zukommt. Diese Rechtselemente bilden eine gute Grundlage, von denen ausgehend ich im Folgenden erörtern möchte, wie weitere überindividuelle Datenschutz-Elemente Eingang in die Gesetzgebung finden könnten.

4.2 Die Multi-Stakeholder-Datenschutz-Folgenabschätzung (MS-DSFA)

Im Hinblick auf die Schwächen liberal-individualistischer Datenschutzrechte arbeitete ich im vorangegangenen Abschnitt zwei Herausforderungen heraus. Die erste große Herausforderung besteht in der Überforderung der Individuen, die mit der Masse der Individualrechte angesichts allgegenwärtiger Datenverarbeitungen und zahlreicher Entscheidungshürden schlicht überfordert sind. Die zweite große Herausforderung besteht in der Unmöglichkeit der informationellen Selbstbestimmung im Kontext moderner Datenanalyseverfahren. Die im Folgenden diskutierten Vorschläge adressieren in erster Linie die zweite Herausforderung.

Teilweise könnten sie aber durchaus auch zur Eindämmung der im Rahmen der ersten Herausforderung diskutierten Probleme herangezogen werden.

Aufgrund der vielfältigen negativen individuellen und gesellschaftlichen Auswirkungen moderner Datenverarbeitungen wurde immer wieder eine Einschränkung solcher Praktiken zwar begrüßt [56, 57], aber häufig blieb unklar, wie genau eine Einschränkung rechtlich verankert werden könnte. Ein meines Erachtens vielversprechender Diskussionsstrang widmet sich der Verschiebung des Fokus der Datenschutzgesetzgebung von der Regulierung personenbezogener Daten hin zur Regulierung personenbezogener Entscheidungen. Möglich würde dadurch, dass nicht nur die personenbezogenen, sondern alle für eine personenbezogene Entscheidung verwendeten Daten rechtlich adressierbar würden [3, 46]. Damit personenbezogene Entscheidungen wiederum rechtlich adressierbar werden können, ist jedoch zunächst die Herstellung von Transparenz über die Prozesse der Entscheidungsfindung notwendig [46, 58], die allerdings seitens datenverarbeitender Akteure regelmäßig unter Verweis auf die aus Sicht der Unternehmen dabei drohende Offenlegung von Geschäftsgeheimnissen zurückgewiesen wurde [59, 60].

Eine Möglichkeit der konkreten, rechtlichen Operationalisierung dieser Vorschläge, die das Risiko der Offenlegung von Geschäftsgeheimnissen auf ein Minimum reduziert, findet sich in jener Datenschutzliteratur, die von ähnlichen Lösungsvorschlägen aus den Bereichen des Verbraucher-, Arbeitnehmer- und Umweltschutzes inspiriert wurde [50, 61]. Kollektive Interessenvertretungen würden es in diesen Bereichen erlauben, dass die Interessen der Betroffenen trotz massiver Machtasymmetrien besser gewahrt bleiben, als wenn der Einzelne alleine gegenüber dem Arbeitgeber, Händler, Umweltsünder usw. auftritt [50].

Die auf diesen Feldern vorherrschende strukturelle Machtasymmetrie ist vergleichbar mit der Situation, der sich die Betroffenen bei modernen Datenverarbeitungskotexten gegenübersehen: Lock-In-Effekte, Unwissen über Datenverarbeitungen, Rechtsbehelfe usw. Allerdings gestaltet sich die Bestimmung des zu schützenden kollektiven Interesses im Falle moderner Datenanalyseverfahren als deutlich schwieriger als in traditionellen Kontexten, wie z. B. dem Arbeitnehmerschutz. Denn ArbeitnehmerInnen stellen eine klar umreißbare Gruppe dar, deren kollektives Interesse (bessere Löhne, mehr Freizeit, Gewährleistung der Arbeitssicherheit, usw.) sich aus ihrer Arbeitnehmerposition gegenüber dem Arbeitgeber unmittelbar ergibt. Das Verhältnis der von Big Data-Analysen Betroffenen zueinander ist dagegen schwer zu fassen. Die geteilten Attribute etwa, auf deren Grundlage algorithmisch generierte Gruppen konstituiert werden, sind den diesen Gruppen zugeordneten Betroffenen in der Regel nicht bekannt. Entsprechend kennt jemand, der auf diese Weise einem Profil zugeordnet wurde,

weder die Gründe für die eigene Profilierung noch die restlichen Mitglieder der Gruppe und besitzt daher kein oder nur sehr begrenztes Wissen über potenzielle kollektive Interessen, die geschützt werden könnten. Schließlich können sich die Parameter, auf deren Grundlage Gruppen konstituiert werden, aufgrund der Natur von Big Data-Analysen, Analyseschleifen vielfach zu wiederholen, ständig ändern. Zusätzlich kann abhängig vom Daten-Input auch die Gruppenzugehörigkeit einzelner Betroffener ständig variieren. Die beschriebenen Einschränkungen erschweren somit die Identifikation und Vertretung kollektiver Interessen (etwa durch die bewusste Wahl eines Repräsentanten) [50].

Die von derartigen Big Data-Analysen Betroffenen können eher mit Verbrauchern verglichen werden, die sich zwar untereinander ebenfalls nicht kennen, jedoch alle gleichsam unter ungesunden Lebensmitteln, unsicheren Produkten, unseriösen Geschäftspraktiken usw. leiden. Das kollektive Verbraucherinteresse besteht dabei etwa in der Bereitstellung gesunder Lebensmittel, sicherer Produkte und fairer Geschäftspraktiken. Im Bereich des Verbraucherschutzes stehen den Betroffenen in derartigen Fällen sowohl individuelle als auch kollektive rechtliche Schritte zur Verfügung. Darüber hinaus können sich Verbraucher an für den Verbraucherschutz zuständige Behörden und Verbraucherverbände wenden oder auch *Verbands- und/oder Sammelklagen* initiieren [50]. Der Einführung derartiger kollektiver Rechtsbehelfe kommt daher eine zentrale Rolle zu. Ihr Vorteil ist, dass sie sowohl dem Einzelnen weiterhin die Möglichkeit überlassen, eine individuelle Klage zu eröffnen, als auch all jenen Menschen, die mit einer individuellen Klage überfordert wären, die Möglichkeit bieten, sich an kollektiven Verfahren zu beteiligen [61]. Art. 80 DS-GVO greift hier eindeutig zu kurz, da er im ersten Absatz lediglich die Beauftragung klar regelt, die Klagemöglichkeit für Verbände etc. ohne eine explizite Beauftragung allerdings im zweiten Absatz der Entscheidungshoheit der Mitgliedstaaten überlässt.

Dass eine Privatheitsverletzung seitens einer kollektiven Interessenvertretung überhaupt angegangen werden kann, ist davon abhängig, ob Wissen über Datenschutzverletzungen besteht. Denkbar und praktisch umsetzbar wäre beispielsweise eine *Meldepflicht im Falle potentiell besonders riskanter Verarbeitungen* [62]. Die dabei als Maßstab heranzuziehende – im Rahmen der DS-GVO allerdings nicht-geregelte – Kritikalität bzw. das Risiko einer Verarbeitung könnte sich beispielsweise an den Vorschlägen der Datenethikkommission orientieren [63]. Damit zusammenhängend, besteht eine weitere Möglichkeit, den Herausforderungen gesellschaftlich unerwünschter Datenverarbeitungen zu begegnen, im Konzept der Risiko-Abschätzung, das in die DS-GVO Eingang in Form der *Datenschutz-Folgenabschätzung* (bzw. DSFA) in Art. 35 bzw. zur *Vorherigen Konsultation* in Art. 36 gefunden hat. Demnach sollen Verantwortliche hohe Risiken für

die Rechte und Freiheiten natürlicher Personen, die aus einer Datenverarbeitungsform hervorgehen können, identifizieren, analysieren und mittels geeigneter Maßnahmen eindämmen. Seit der Verabschiedung der DS-GVO ist eine EU-weite intensive Debatte rund um die Festlegung einer effektiven und effizienten DSFA-Methodik entstanden [64]. Es gibt zwar aktuell noch keine gesicherten Zahlen dazu, wie häufig DSFAs zur Anwendung kommen, doch zeichnet sich bereits seit längerem ab, dass das Instrument für Verantwortliche eher ein notwendiges Übel darzustellen scheint, als eine beliebte Methode zur Eindämmung von Grundrechtsrisiken [65, 66]. Diese Annahme deckt sich mit Erfahrungen aus der Vergangenheit: Selbstregulierungsinstrumente werden immer dann nicht ernst genommen, wenn der Zweck des Instruments darin liegt, eine Selbstbeschränkung von Organisationspraktiken zu erreichen [67, 68].

Abhilfe könnte ein Vorschlag schaffen, der das Moment der Interessenvertretung in der DSFA stärkt und die Risiko-Abschätzung stärker als *Multi-Stakeholder-Prozess* zu strukturieren vorschlägt, an dem, abhängig von der Art der Verarbeitung, neben dem Verarbeiter selbst, weitere Stakeholder aktiv partizipieren [50, 61]. Der Vorschlag würde somit zunächst insbesondere die Erweiterung des in Art. 35 Abs. 9 formulierten möglichen Einbezugs der von einer Verarbeitung Betroffenen oder ihrer Vertreter vorsehen. Denn ein weithin bekanntes Problem von Multi-Stakeholder-Prozessen ist die Unterrepräsentation zivilgesellschaftlicher Akteure und die Überrepräsentation (wirtschafts-)mächtiger Akteure. Die in Art. 35 (9) festgeschriebene Formulierung, wonach der Standpunkt von Betroffenen oder ihren Vertretern nur „gegebenenfalls“ einzuholen ist, öffnet Tür und Tor für die Durchführung einer DSFA als Checkbox-Tätigkeit, die von keiner anderen Instanz in relevantem Maße kontrolliert wird und letztlich nur als Vorwand zur Rechtfertigung einer umstrittenen Verarbeitung genutzt wird.

Ein solcher Multi-Stakeholder-DSFA-Prozess könnte folgendermaßen ablaufen (vgl. auch Abb. 1): Ein Unternehmen, das eine datenbasierte Verarbeitung plant, die aufgrund ihres Umfangs und/oder ihres Eingriffs in individuelle Rechte oder in gesellschaftliche Strukturen wahrscheinlich zu Privatheits-, Datenschutz- oder sonstigen gesellschaftlichen Risiken führen könnte, müsste verpflichtet sein, jene Verarbeitung einer Risikoanalyse zu unterziehen. Vor Durchführung der Risikoanalyse müsste sie die geplante Verarbeitung bei der zuständigen Datenschutzaufsichtsbehörde ankündigen bzw. melden. Je nachdem, welche gesellschaftlichen Bereiche betroffen sind, müssten weitere Akteure, die das Betroffeneninteresse vertreten, hinzugezogen werden, bspw. Verbraucherschutzorganisationen oder Anti-Diskriminierungsstellen. Die am Risikoabschätzungsprozess beteiligten Organisationen müssten, abhängig von der Art der jeweils geplanten Verarbeitung,

Abb. 1 Vorschlag für einen Multi-Stakeholder-DSFA-Prozess. (Eigene Darstellung, inspiriert von Mantelero 2016)

weitreichende Partizipationsrechte erhalten, damit das Ziel einer gesellschaftsverträglichen Datenverarbeitung erreicht werden kann. Je nach Verarbeitung und Risiko könnten die jeweiligen Vertreter z. B. von den Betroffenen Vollmachten einholen, um weitergehenden Zugriff auf personenbezogene Daten zu erhalten, Auskunftsersuchen zu stellen usw. Dies müsste in solchen Fällen, in denen die gesellschaftlichen Folgen einer Verarbeitung sehr weitreichend oder besonders unklar sind, auch die Einsicht in Staats- und Geschäftsgeheimnisse, etwa nähere Informationen zu den verwendeten Algorithmen aufseiten der Verantwortlichen umfassen. Um die nicht-legitime Veröffentlichung von Staats- oder Geschäftsgeheimnissen zu unterbinden, müssten derartige Einblicke allerdings hohen Verschwiegenheitsansprüchen genügen, solange kein sehr weitreichendes und gesellschaftlich relevantes Risiko von einer Verarbeitung ausgeht [50, 61].

Das überwiegende öffentliche Interesse sollte in solchen, besonders riskanten Fällen ausreichend sein, um den Eingriff in die unternehmerische Freiheit bzw. die Offenlegung von Staatsgeheimnissen zu begründen. Dadurch, dass entsprechende Geheimnisse, Algorithmen etc. nicht der allgemeinen Öffentlichkeit, sondern nur den konkret am Prozess mitwirkenden Personen aus den beteiligten Organisationen bekannt würden, könnte die missbräuchliche Weitergabe entsprechenden Wissens schließlich deutlich besser verhindert bzw. nachvollzogen werden.

Der abschließende Vorteil einer Multi-Stakeholder-DSFA gegenüber üblichen Risikoabschätzungsprozessen müsste schließlich in der Generierung von möglichst konkreten Ergebnissen liegen. Hier ist an eine weite Maßnahmenspanne zu denken, von der Definition von Zertifizierungskriterien über spezifizierte Datensicherheitsvorgaben bis hin zu risikoadäquater Regulierung (vgl. Abb. 2).

Zertifizierungen etwa hätten den Vorteil, dass sie ein stärkeres Anreizsystem für Unternehmen bzw. staatliche Stellen zur Durchführung von Multi-Stakeholder-DSFAs schaffen. Denkbar wäre, dass gewisse Verarbeitungen, weil die mit ihnen verbundenen Risiken ausreichend gesellschaftsverträglich vermindert wurden, auch ohne die Einwilligung der Betroffenen als rechtmäßig gelten. Dieser

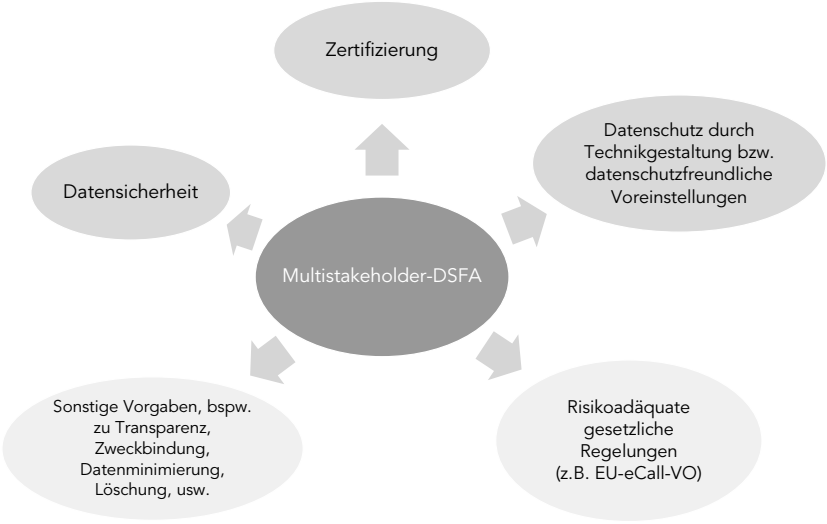


Abb. 2 Mögliche Ergebnisse eines Multi-Stakeholder-DSFA-Prozesses. (Eigene Darstellung)

Vorschlag wäre somit ein Kompromiss, der potenziell riskante Verarbeitungen unter Sicherheitsvorkehrungen erlauben würde und aufgrund der durch den Risikoabschätzungsprozess entstehenden bürokratischen Hürden zugleich der verantwortlichen Stelle durch anderweitige Zugeständnisse entgegenkommen würde. Die auf diese Weise begutachteten Verarbeitungen würden schließlich mittels Zertifizierung so gekennzeichnet werden können, dass ihre Gesellschaftsverträglichkeit deutlich wird und sie als Wettbewerbsvorteil fungieren kann. Neben Big Data-Analysen müssten Zertifizierungen auch für weniger umfangreiche Verarbeitungen möglich sein und unter staatlicher bzw. behördlicher Aufsicht ein hohes Schutzniveau signalisieren [50, 61]. Beim Zustandekommen der DS-GVO wurden aufgrund des Drucks aus der Wirtschaft keine qualitativen Zertifizierungskriterien festgelegt, sodass die in Art. 42 festgeschriebenen Vorgaben lediglich die Konformität einer Verarbeitung mit den Regeln der DS-GVO signalisieren, die Datenverarbeiter ohnehin befolgen müssen.

Die von einer derartigen Verarbeitung Betroffenen würden von dem Risikoabschätzungsverfahren deshalb profitieren, weil die am Verfahren partizipierenden Vertreter von Betroffeneninteressen aufgrund ihrer Verhandlungsposition und der größeren Sachkenntnis eine ansonsten nicht-regulierte Verarbeitung so mitgestalten würden, dass die Interessen der Betroffenen möglichst umfassend gewahrt bleiben. Freilich müsste jeder Betroffene, trotz der im o. g. Beispiel vorgeschlagenen Aushebelung der individuellen Einwilligung mittels kollektiver Einigungen, zu jedem Zeitpunkt die Möglichkeit haben, die zur Debatte stehende Verarbeitung mittels Opt-out zu widerrufen, sofern ein Personenbezug vorhanden ist. Je nach Verarbeitung und Risiko wäre auch die Einrichtung unterschiedlicher Opt-out-Möglichkeiten denkbar, um die Nachteile eines Alles-Oder-Nichts-Ansatzes zu vermeiden. So lange von einer Verarbeitung keine fundamentalen gesellschaftlichen Risiken ausgehen, die eine Übergehung des Individuums rechtfertigen, ist entscheidend, dass die Abtretung individueller Rechte an Interessenvertretungsorganisationen keine Verringerung der individuellen Entscheidungsmöglichkeiten gegenüber dem Falle der Nicht-Abtretung zur Folge hat. Dies schließt ein, dass die Abtretung der individuellen Einwilligungskompetenz vollständig beim jeweiligen Individuum liegen sollte [34, 69]. Im Zweifelsfall, wenn die Reichweite des gesellschaftlichen Interesses strittig ist, müsste die Entscheidungskompetenz stets weiterhin beim Individuum verbleiben. Ein grundlegendes Standard-Datenschutzniveau müsste allerdings auch in solchen Fällen absehbare Risiken minimieren. Wichtig wären in diesem Zusammenhang weitreichende *Datensicherheitsvorgaben,* aber auch Vorgaben zu *Privacy by Design und Default.* Das Ziel des Konzepts von Privacy by Default besteht in der technischen Umsetzung von Datenminimierungs-, Zweckbindungs- und Speicherfristvorgaben [70]. Das

Problem beim Erlassen derartiger Vorgaben resultiert daraus, dass die Festlegung von beispielsweise Standardeinstellungen, die Gültigkeit für alle Verarbeitungstypen beanspruchen müssen, sehr schwierig ist [71]. Eine Lösung dieses Problems könnte dadurch erreicht werden, dass die zu befolgenden Vorgaben im Ergebnis einer Multi-Stakeholder-DSFA oder eines partizipativen Privacy by Design, wie es bei Ochs und Lamla [6] diskutiert wird, erarbeitet werden. Derartige Vorgaben hätten den Vorteil, dass sie nur für bestimmte Verarbeitungen oder Verarbeitungsfelder anwendbar wären und die erwünschte Abstraktheit der gesetzlichen Regelungen somit unangetastet bliebe. Entscheidend für die Wirksamkeit von Privacy by Design- und Default-Vorgaben ist schließlich auch, dass sie sich sowohl an die für eine Datenverarbeitung Verantwortlichen als auch an die Hersteller datenverarbeitender Systeme richten [72].

Eine weitere Bedingung für das Gelingen des dargestellten Risikoabschätzungsprozesses, aber auch für die Gewährleistung der Einhaltung der weiteren in dem Abschnitt vorgeschlagenen, die verantwortliche Stelle betreffenden Vorgaben ist die *Ausstattung von Datenschutzaufsichtsbehörden mit ausreichender finanzieller und politischer Autonomie.* Das würde etwa bedeuten, dass die Behörden keinesfalls an ein Ministerium angegliedert und weisungsgebunden sein dürfen, sondern ausschließlich dem Parlament gegenüber rechenschaftspflichtig sind [50, 73].

Falls im Laufe von Risikoabschätzungsprozessen besonders riskante Verarbeitungssektoren oder -typen identifiziert werden, müssten zudem risikoadäquate gesetzliche Regelungen erlassen werden können. Beispielhaft für eine solche, risikoadäquate Regulierung ist die EU-eCall-Verordnung 2015/758 [74]. Darin wird auf detaillierte Weise geregelt, welche Vorkehrungen die Hersteller von eCall-Systemen treffen müssen, um Datenschutzgefährdungen zu vermeiden [75].

5 Schluss

Vor dem Hintergrund der Kritik am liberal-individualistischen Fokus des bestehenden Datenschutzrechts hat der vorliegende Beitrag datenschutzrechtliche Gestaltungsmöglichkeiten jenseits der Fokussierung auf das Individuum untersucht. Die diskutierten Vorschläge sehen keine bloße Ersetzung individuellen Datenschutzes durch kollektive Schutzmaßnahmen vor, sondern die Ergänzung individualistischer Schutzmomente. Der wesentliche Unterschied zwischen klassisch liberal-individualistischen Datenschutzrechten und den in im Rahmen dieses Papers vorgestellten Vorschlägen liegt einerseits in der (sanktionsbewährten) weiteren Übertragung von Verantwortung auf die für eine Verarbeitung

Verantwortlichen und andererseits im deutlichen Ausbau von kollektiven Vertretungsmöglichkeiten für Betroffene, auf die insbesondere dann zurückgegriffen wird, wenn eine Verarbeitung voraussichtlich zu individuellen und/oder gesellschaftlichen Risiken führt, denen die Individuen isoliert nicht begegnen könnten. Die Verlagerung von mehr Verantwortung an die Verarbeiter und die Ergänzung bestehender Datenschutzrechte durch kollektive Vertretungsmöglichkeiten berücksichtigt somit die gesellschaftlichen Effekte von Datenverarbeitungen, ohne dass die Selbstbestimmungsfähigkeit des Individuums negiert und ausschließlich in die Hände eines Kollektivs gelegt wird [50, 69].

Klar ist auch, dass kollektive Verfahren, wie das hier besprochene Multi-Stakeholder-DSFA-Modell, nicht für die Bearbeitung aller Datenschutz-Herausforderungen geeignet sein kann. Wie Bull [36] bereits vor mehr als zwei Jahrzehnten im Kontext der Nutzung von Gesundheitsdiensten zutreffend bemerkt hatte, stößt die Praxis der Zurateziehung kollektiver Akteure immer dann an ihre Grenzen, sobald es um gesamtgesellschaftlich heikle Themen geht. In anderen Worten: So lange kein gesellschaftlicher Konsens zu spezifischen Datenschutz-Fragen existiert, hilft auch die Delegation an Kollektivakteure nicht weiter.

Abschließend sei noch erwähnt, dass datenschutzrechtliche Lösungsansätze allein ohnehin nicht ausreichend sind: Um die negativen Folgen der im Beitrag beschriebenen modernen Datenverarbeitungen einzudämmen bräuchte es darüber hinaus weitere Strategien, beispielsweise aus dem Diskriminierungs- oder Wettbewerbsrecht, wie sie derzeit im Hinblick auf die Regulierung von Plattformen diskutiert werden [62, 76].

Danksagung Die diesem Beitrag zugrunde liegenden Arbeiten wurden mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) unter den Förderkennzeichen 16KIS0741K gefördert.

Literatur

1. Helm, P., Seubert, S.: Normative Paradoxien der Privatheit in Zeiten von Big Data: Eine sozialkritische Perspektive auf eine digitale „Krise“ der Privatheit. In: Borucki, I., Schünemann, W.J. (Hrsg.) Internet und Staat (2019)
2. van der Sloot, B.: Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. Int. Data Priv. Law **4**, 307 (2014)
3. Koops, B.-J.: The trouble with European data protection law. Int. Data Priv. Law **4**, 250–261 (2014)

4. Steeves, V.M.: Reclaiming the social value of privacy. In: Kerr, I., Steeves, V.M., Lucock, C. (Hrsg.) Lessons from the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society, S. 191–208. Oxford University Press, Oxford (2009)
5. Cohen, J.E.: Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. Yale University Press, New Haven [Conn.] (2012)
6. Ochs, C., Lamla, J.: Demokratische privacy by design. Kriterien soziotechnischer Gestaltung von Privatheit. Forschungsjournal Soziale Bewegungen. 30, 189–199 (2017). https://doi.org/10.1515/fjsb-2017-0040
7. Becker, C., Seubert, S.: Privatheit, kommunikative Freiheit und Demokratie. Datenschutz Datensich.-DuD **40**, 73–78 (2016)
8. Hagendorff, T.: Übersehene Probleme des Konzepts der Privacy Literacy. In: Roßnagel, A., Friedewald, M., Hansen, M. (Hrsg.) Die Fortentwicklung des Datenschutzes, S. 99–120. Springer Fachmedien Wiesbaden, Wiesbaden (2018). https://doi.org/10.1007/978-3-658-23727-1_6
9. BVerfG: Urteil vom 15.12.1983. (1983)
10. Roßnagel, A., Pfitzmann, A., Garstka, H.: Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern (2001)
11. Richter, P.: Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO. Datenschutz Datensich. **39**, 735–740 (2015). https://doi.org/10.1007/s11623-015-0510-9
12. Roßnagel, A., Friedewald, M., Geminn, C.L., Hagendorff, T., Heesen, J., Hess, T., Kreutzer, M., Neubaum, G., Ochs, C., Simo Fhom, H.: Policy Paper: Datensparsamkeit oder Datenreichtum? Zur neuen politischen Diskussion über den datenschutzrechtlichen Grundsatz der Datensparsamkeit. Fraunhofer Institut für System- und Innovationsforschung ISI, Karlsruhe (2017)
13. Pohle, J.: Zweckbindung Revisited. DANA – Datenschutz Nachrichten, S. 141–145 (2015)
14. Simitis, S.: Einleitung: Geschichte – Ziele – Prinzipien. In: Simitis, S. (Hrsg.) Bundesdatenschutzgesetz. Nomos, Baden-Baden (2011)
15. Kurz, C.: Spiros Simitis: „Man spielt nicht mehr mit dem Datenschutz!". https://netzpolitik.org/2015/spiros-simitis-man-spielt-nicht-mehr-mit-dem-datenschutz/. Zugegriffen: 7. Juli 2018
16. Hagendorff, T.: Das Ende der Informationskontrolle: digitale Mediennutzung jenseits von Privatheit und Datenschutz. Transcript, Bielefeld (2017)
17. Moor, J.H.: Towards a theory of privacy in the information age. ACM SIGCAS Comput. Soc. **27**, 27–32 (1997)
18. Seemann, M.: Das neue Spiel: Strategien für die Welt nach dem digitalen Kontrollverlust. Orange-Press, Freiburg im Breisgau (2014)
19. Karaboga, M., Matzner, T., Obersteller, H., Ochs, C.: Is there a right to offline alternatives in a digital world? In: Leenes, R., van Brakel, R., Gutwirth, S., De Hert, P. (Hrsg.) Data Protection and Privacy: (In)visibilities and Infrastructures, S. 31–57. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-50796-5_2
20. Karaboga, M., Matzner, T., Nebel, M., Ochs, C., Schütz, P., Simo Fhom, H., Morlok, T., Pittroff, F., von Pape, T., Pörschke, J.V.: White Paper Das versteckte Internet: Zu Hause – Im Auto – Am Körper. Fraunhofer-Institut für System- und Innovationsforschung, Karlsruhe (2015)

21. Taylor, L., Floridi, L., Sloot, B. van der (Hrsg.): Group Privacy: New Challenges of Data Technologies. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-46608-8
22. Bründl, S., Matt, C., Hess, T.: Wertschöpfung in Datenmärkten: Eine explorative Untersuchung am Beispiel des deutschen Marktes für persönliche Daten. Stober GmbH Druck und Verlag, Eggenstein (2015)
23. boyd, danah: Networked privacy. Surveill. Soc. **10**, 348–350 (2012). https://doi.org/10.24908/ss.v10i3/4.4529
24. Pearson, S.: Privacy, security and trust in cloud computing. In: Pearson, S., Yee, G. (Hrsg.) Privacy and Security for Cloud Computing, S. 3–42. Springer London, London (2013). https://doi.org/10.1007/978-1-4471-4189-1_1
25. Acquisti, A., Sleeper, M., Wang, Y., Wilson, S., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L.F., Komanduri, S., Leon, P.G., Sadeh, N., Schaub, F.: Nudges for privacy and security: understanding and assisting users' choices online. ACM Comput. Surv. **50**, 1–41 (2017). https://doi.org/10.1145/3054926
26. Solove, D.J.: Privacy Self-Management and the Consent Dilemma. Social Science Research Network, Rochester (2012)
27. Barocas, S., Nissenbaum, H.: Big data's end run around procedural privacy protections. Commun. ACM **57**, 31–33 (2014). https://doi.org/10.1145/2668897
28. Reding, V.: The European data protection framework for the twenty-first century. Int. Data Priv. Law **2**, 119–129 (2012)
29. Albrecht, J.P.: Hands Off Our Data. AktivDruck, Göttingen (2015)
30. Litman-Navarro, K.: Opinion|we read 150 privacy policies. They were an incomprehensible disaster. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html (2019)
31. Roßnagel, A., Bile, T., Nebel, M., Geminn, C., Karaboga, M., Ebbers, F., Bremert, B., Stapf, I., Teebken, M., Thürmel, V., Ochs, C., Uhlmann, M., Krämer, N., Meier, Y., Kreutzer, M., Schreiber, L., Simo, H.: White Paper Einwilligung: Möglichkeiten und Fallstricke aus der Konsumentenperspektive. Fraunhofer Institut für System- und Innovationsforschung, Karlsruhe (2020)
32. Alizadeh, F., Jakobi, T., Boldt, J., Stevens, G.: GDPR-reality check on the right to access data: claiming and investigating personally identifiable data from companies. In: Proceedings of Mensch und Computer 2019 on – MuC'19, S. 811–814. ACM Press, Hamburg (2019). https://doi.org/10.1145/3340764.3344913
33. McDonald, A.M., Cranor, L.F.: The cost of reading privacy policies. J. Law Policy Inf. Soc. **4**, 543–568 (2008)
34. Bygrave, L.A., Schartum, D.W.: Consent, proportionality and collective power. In: Gutwirth, S., Poullet, Y., De Hert, P., de Terwangne, C., Nouwt, S. (Hrsg.) Reinventing Data Protection?, S. 157–173. Springer Netherlands, Dordrecht (2009). https://doi.org/10.1007/978-1-4020-9498-9_9
35. Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T.: (Un)informed consent: studying GDPR consent notices in the field. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, S. 973–990. ACM, London (2019). https://doi.org/10.1145/3319535.3354212

36. Bull, H.-P.: Aus aktuellem Anlass: Bemerkungen über Stil und Technik der Datenschutzgesetzgebung. Recht der Datenverarbeitung, S. 148–153 (1999)
37. Norris, C.: The Unaccountable State of Surveillance: Exercising Access Rights in Europe. Springer, Berlin (2016)
38. Ausloos, J., Dewitte, P.: Shattering one-way mirrors–data subject access rights in practice. Int. Data Priv. Law **8**(1), 4–28, February 2018, (2018). https://doi.org/10.1093/idpl/ipy001
39. Calders, T., Custers, B.: What is data mining and how does it work? In: Custers, B., Calders, T., Schermer, B., Zarsky, T. (Hrsg.) Discrimination and Privacy in the Information Society, S. 27–42. Springer, Berlin (2013). https://doi.org/10.1007/978-3-642-30487-3_2
40. Hildebrandt, M.: Defining profiling: a new type of knowledge? In: Hildebrandt, M., Gutwirth, S. (Hrsg.) Profiling the European Citizen, S. 17–45. Springer Netherlands, Dordrecht (2008). https://doi.org/10.1007/978-1-4020-6914-7_2
41. Sloot, B. van der: From data minimization to data minimummization. In: Custers, B., Calders, T., Schermer, B., Zarsky, T. (Hrsg.) Discrimination and Privacy in the Information Society, S. 273–287. Springer, Berlin (2013). https://doi.org/10.1007/978-3-642-30487-3_15
42. Schaar, P.: Das Ende der Privatsphäre: der Weg in die Überwachungsgesellschaft. C. Bertelsmann, München (2007)
43. Degeling, M.: Profiling, Prediction und Privatheit: Über das Verhältnis eines liberalen Privatheitbegriffs zu neueren Techniken der Verhaltensvorhersage. In: Garnett, S., Halft, S., Herz, M., Mönig, J. M. (Hrsg.) Medien und Privatheit, S. 69–92. Medien, Texte, Semiotik 7. Passau: Verlag Karl Stutz (2014)
44. Hildebrandt, M.: Profiling: from data to knowledge: the challenges of a crucial technology. Datenschutz Datensich. – DuD **30**, 548–552 (2006). https://doi.org/10.1007/s11623-006-0140-3
45. Kammourieh, L., Baar, T., Berens, J., Letouzé, E., Manske, J., Palmer, J., Sangokoya, D., Vinck, P.: Group privacy in the age of big data. In: Taylor, L., Floridi, L., van der Sloot, B. (Hrsg.) Group Privacy: New Challenges of Data Technologies, S. 37–66. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-46608-8_3
46. Pohle, J.: Personal Data not found: Personenbezogene Entscheidungen als überfällige Neuausrichtung im Datenschutz. DANA – Datenschutz Nachrichten. 14–19 (2016)
47. Regan, P.M.: Legislating Privacy: Technology, Social Values and Public Policy. University of North Carolina Press, Chapel Hill (1995)
48. Marwick, A.E., boyd, danah: Networked privacy: how teenagers negotiate context in social media. New Media Soc. **16**, 1051–1067 (2014). https://doi.org/10.1177/1461444814543995
49. van der Sloot, B.: The individual in the big data era: moving towards an agent-based privacy paradigm. In: van der Sloot, B., Broeders, D., Schrijvers, E. (Hrsg.) Exploring the Boundaries of Big Data, S. 177–203. Amsterdam University Press, Amsterdam (2016)
50. Mantelero, A.: Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection. Comput. Law Secur. Rev. **32**, 238–255 (2016). https://doi.org/10.1016/j.clsr.2016.01.014

51. Matzner, T., Ochs, C.: Chapter three: sorting things out ethically: privacy as a research issue beyond the individual. In: Zimmer, M., Kinder-Kurlanda, K. (Hrsg.) Internet Research Ethics for the Social Age: New Challenges, Cases, and Contexts, S. 39–73. Lang, New York (2017). https://doi.org/10.3726/b11077/16
52. Taylor, L., Sloot, B. van der, Floridi, L.: Conclusion: what do we know about group privacy? In: Taylor, L., Floridi, L., Sloot, B. van der (Hrsg.) Group Privacy, S. 225–237. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-46608-8
53. Jones, P.: Group rights. Stanford encyclopedia of philosophy (2016)
54. Mittelstadt, B.: From individual to group privacy in big data analytics. Philos. Technol. (2017). https://doi.org/10.1007/s13347-017-0253-7
55. Matzner, T., Richter, P.: Ausblick: Die Zukunft der informationellen Selbstbestimmung. In: Friedewald, M., Lamla, J., Roßnagel, A. (Hrsg.) Informationelle Selbstbestimmung im digitalen Wandel, S. 319–323. Springer Fachmedien Wiesbaden, Wiesbaden (2017). https://doi.org/10.1007/978-3-658-17662-4_18
56. Steeves, V.M.: Privacy, sociality and the failure of regulation: lessons learned from young Canadians' online experiences. In: Roessler, B., Mokrosinska, D. (Hrsg.) Social Dimensions of Privacy, S. 244–260. Cambridge University Press, Cambridge (2015). https://doi.org/10.1017/CBO9781107280557.013
57. Sevignani, S.: Privacy and capitalism in the age of social media. Routledge, New York (2016)
58. Koops, B.-J.: On decision transparency, or how to enhance data protection after the computational turn. In: Hildebrandt, M., de Vries, K. (Hrsg.) Privacy, Due Process and the Computational Turn, S. 196–220. Routledge, Abingdon (2013)
59. O'Neil, C.: Weapons of math destruction: how big data increases inequality and threatens democracy. Crown, New York (2016)
60. Krüger, J.: Wie der Mensch die Kontrolle über den Algorithmus behalten kann. https://netzpolitik.org/2018/algorithmen-regulierung-im-kontext-aktueller-gesetzgebung/. Zugegriffen: 11. Nov. 2018
61. Bygrave, L.A.: Data Protection Law : Approaching its Rationale, Logic and Limits. Kluwer Law International, London (2002)
62. Mantelero, A.: Social control, transparency, and participation in the big data world. J. Internet Law 23–29 (2014)
63. DEK: Gutachten der Datenethikkommission der Bundesregierung. Datenethikkommission der Bundesregierung, Berlin (2019)
64. Martin, N., Friedewald, M., Schiering, I., Mester, B.A., Hallinan, D., Jensen, M.: Die Datenschutz-Folgenabschätzung nach Art. 35 DSGVO: Ein Handbuch für die Praxis. Fraunhofer, Stuttgart (2020)
65. Martin, N., Mester, B.A., Schiering, I., Friedewald, M., Hallinan, D.: Datenschutz-Folgenabschätzung: Ein notwendiges „Übel" des Datenschutzes? Datenschutz Datensich. **44**, 149–153 (2020). https://doi.org/10.1007/s11623-020-1241-0
66. EDPS: EDPS Survey on Data Protection Impact Assessments under Article 39 of the Regulation. (2020)
67. Clarke, R.: Computer matching by government agencies: the failure of cost/benefit analysis as a control mechanism. Inf. Infrastruct. Policy **4**, 29–65 (1995)

68. Briegleb, V.: Selbstregulierung von Social Networks gescheitert. https://www.heise.de/newsticker/meldung/Selbstregulierung-von-Social-Networks-gescheitert-1857533.html. Zugegriffen: 12. Febr. 2018
69. Mantelero, A.: The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics. Comput. Law Secur. Rev. **30**, 643–660 (2014). https://doi.org/10.1016/j.clsr.2014.09.004
70. Cavoukian, A.: Privacy by design: leadership, methods, and results. In: Gutwirth, S., Leenes, R., de Hert, P., Poullet, Y. (Hrsg.) European Data Protection: Coming of Age, S. 175–202. Springer Netherlands, Dordrecht (2013). https://doi.org/10.1007/978-94-007-5170-5_8
71. Hansen, M.: Data protection by design and by default à la European general data protection regulation. In: Privacy and Identity Management. Facing up to Next Steps, S. 27–38. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-55783-0_3
72. Husemann, C.: Datenschutz durch Systemgestaltung. In: Roßnagel, A. (Hrsg.) Das neue Datenschutzrecht: Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze, S. 163–171. Nomos, Baden-Baden (2018)
73. Schütz, P.: Zum Leben zu wenig, zum Sterben zu viel? Die finanzielle und personelle Ausstattung deutscher Datenschutzbehörden im Vergleich. In: Roßnagel, A., Friedewald, M., Hansen, M. (Hrsg.) Die Fortentwicklung des Datenschutzes, S. 251–268. Springer Fachmedien Wiesbaden, Wiesbaden (2018). https://doi.org/10.1007/978-3-658-23727-1_14
74. Europäische Union: Verordnung (EU) 2015/758 des Europäischen Parlaments und des Rates vom 29. April 2015 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG. (2015)
75. Husemann, C., Pittroff, F.: Smarte Regulierung in Informationskollektiven – Bausteine einer Informationsregulierung im Internet der Dinge. In: Roßnagel, A., Friedewald, M., Hansen, M. (Hrsg.) Die Fortentwicklung des Datenschutzes, S. 337–359. Springer Fachmedien Wiesbaden, Wiesbaden (2018). https://doi.org/10.1007/978-3-658-23727-1_19
76. Nocun, K.: Datenschutz unter Druck: Fehlender Wettbewerb bei sozialen Netzwerken als Risiko für den Verbraucherschutz. In: Roßnagel, A., Friedewald, M., Hansen, M. (Hrsg.) Die Fortentwicklung des Datenschutzes, S. 39–58. Springer Fachmedien Wiesbaden, Wiesbaden (2018). https://doi.org/10.1007/978-3-658-23727-1_3

Transparenz der polizeilichen Datenverarbeitung: Defizite und technische Lösungsansätze

Jan Fährmann, Hartmut Aden und Clemens Arzt

Zusammenfassung

Dieser Beitrag untersucht aus einer rechts- und verwaltungswissenschaftlichen Perspektive Transparenzdefizite, die bei der Ausgestaltung der polizeilichen Datenerhebung und der weiteren Datenverarbeitung bestehen. Diese können nicht nur für die verdeckte Datenverarbeitung konstatiert werden, sondern auch bei der offenen Datenerhebung. Im Anschluss an diesen Befund werden mögliche Instrumente zur Steigerung von Transparenz analysiert.

Schlüsselwörter

Informationelle Selbstbestimmung • Transparenz polizeilichen Handelns • Datenschutz • Polizeiliche Datenerhebung • Polizeiliche Datenverarbeitung • Technisch-organisatorische Maßnahmen • Polizeiliche Überwachung

J. Fährmann (✉) · H. Aden · C. Arzt
Hochschule für Wirtschaft und Recht, Forschungsinstitut für öffentliche und private Sicherheit (FÖPS Berlin), Berlin, Deutschland
E-Mail: jan.faehrmann@hwr-berlin.de

H. Aden
E-Mail: hartmut.aden@hwr-berlin.de

C. Arzt
E-Mail: clemens.arzt@hwr-berlin.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_15

1 Einleitung[1]

Fast alle Menschen sind durch „smarte“ Geräte zunehmend vernetzt, verarbeiten personenbezogene Daten, tauschen diese mit anderen aus und generieren dabei neue Datensätze. Die Menge der verarbeiteten personenbezogenen Daten steigt dabei seit Jahren exponentiell an. Da Polizeibehörden für ihre Tätigkeit in hohem Maße auf Informationen angewiesen sind, sind sie grundsätzlich bestrebt, neue Datenverarbeitungstechnologien und eine ständig zunehmende Vielfalt personenbezogener Daten für polizeiliche Zwecke zu nutzen.[2] Damit wächst vielfach die Eingriffsintensität polizeilicher Maßnahmen, insbesondere mit Blick auf das Telekommunikationsgeheimnis sowie auf das Allgemeine Persönlichkeitsrecht in seinen Ausprägungen als Grundrecht auf informationelle Selbstbestimmung[3] und als Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme.[4]

Technische Neuerungen können polizeiliche Tätigkeiten und Maßnahmen vereinfachen. In einigen Fällen kann neue Technik auch dazu beitragen, Eingriffsintensitäten zu verringern, etwa wenn Datenabgleiche nicht mehr per Funk, sondern mit einem mobilen Gerät durchgeführt werden können, ohne dass die Einsatzleitzentrale beteiligt werden muss. Dadurch müssen die Betroffenen nicht mehr so lange vor Ort angehalten werden.[5] Stets verfügbare Technik kann aber auch die Schwelle für polizeiliche Kontrollen herabsetzen und zu einem Zuwachs von Kontrollen führen. Neue Technologien können aber auch zu neuartigen

[1] Der Beitrag basiert auf empirischen und rechtswissenschaftlichen Erkenntnissen der Verfasser aus Projekten der BMBF-geförderten Forschung zur zivilen Sicherheit: MEDIAN (Mobile berührungslose Identitätsprüfung im Anwendungsfeld Migration; Förderkennzeichen 13N14799) und AMBOS (Abwehr von unbemannten Flugobjekten für Behörden und Organisationen mit Sicherheitsaufgaben; Förderkennzeichen 13N14270). Die Projekte befass(t)en sich mit Maßnahmen der polizeilichen Datenverarbeitung. Dabei liegt der Fokus im Projekt MEDIAN auf polizeilichen Personenkontrollen, die Identitätsfeststellungen, Befragungen und Datenabgleiche umfassen. Es wird untersucht, wie solche Kontrollen mittels einer mobilen Anwendung bei hohen Datenschutzstandards effektiver ausgestaltet werden können und unter welchen Umständen Kontrollen für Betroffene akzeptabel sind. Im Projekt AMBOS ging es um die Detektion und Abwehr von Drohnen durch die Polizei. Schwerpunkte des Projekts aus rechtlicher Sicht waren die grundrechtliche Relevanz dieser Maßnahmen und die weiteren rechtlichen Anforderungen an solche polizeilichen Maßnahmen, insbesondere an die Datenverarbeitung bei der Detektion.

[2] Vertiefend hierzu Fährmann (2020) [26, S. 228], Aden (2020) [4].

[3] Vom Bundesverfassungsgericht etabliert 1983 in der Volkszählungsentscheidung, BVerfGE 65, 1.

[4] Etabliert durch BVerfGE 120, 274.

[5] Näher hierzu Aden/Bosch/Fährmann (2020) [5, S. 99–100].

Bedrohungslagen führen, z. B. die zunehmende Nutzung von Drohnen durch Privatleute, denen die Polizei nur mittels Überwachungsmaßnahmen begegnen kann, etwa mit Geräten zur Detektion und anschließenden Abwehr von rechtswidrig eingesetzten Drohnen.[6] Der Trend zur Nutzung immer leistungsfähigerer und eingriffsintensiverer Technik im Polizeidienst dürfte sich daher in den nächsten Jahren weiter verstärken.

Polizeiliche (Überwachungs-)Maßnahmen können indes auch Einschüchterungseffekte nach sich ziehen und demokratische Partizipationsmöglichkeiten beeinträchtigen, z. B. bei der Wahrnehmung der Versammlungsfreiheit oder der Nutzung des öffentlichen Raums.[7] Dies ist beim Technikeinsatz stets zu berücksichtigen. So könnten sich etwa Menschen, die eine Beschäftigung in einer Behörde anstreben, gegen die Teilnahme an einer regierungskritischen Versammlung entscheiden, wenn sie Sorge haben, dass dies registriert wird und Nachteile für ihre berufliche Zukunft mit sich bringen könnte.

Der polizeiliche Technikeinsatz kann neben einer Einschüchterung mit Blick auf eine Versammlungsteilnahme[8] auch dazu führen, dass Menschen Orte, an denen sie Kontrollen oder Überwachung mittels technischer Geräte erwarten, nicht mehr aufsuchen oder sich dort bewusst oder unbewusst „anders“ verhalten[9]; zu groß kann die Sorge sein, dass potenziell unerwünschtes Verhalten registriert, dokumentiert und später gegen eine Person verwendet werden könnte.[10] Behördlich „unerwünschtes“ Verhalten kann auch erlaubtes und grundrechtlich geschütztes Verhalten umfassen, oder Verhaltensweisen, die von der Polizei als Störung der öffentlichen Ordnung aufgefasst werden. Der Begriff der öffentlichen Ordnung gibt dabei viel Spielraum für subjektive Wertungen, sodass Menschen beeinflusst durch z. B. Alter, Erziehung oder Einstellungen sehr unterschiedliche Ordnungsvorstellungen haben. Werden Überwachungstechniken eingesetzt, um missliebige Verhaltensweisen – etwa öffentliches Trinken von Alkohol oder das laute Hören von Musik im öffentlichen Raum – zu identifizieren und ggf. auch polizeilich zu kontrollieren und zu sanktionieren, so wird der öffentliche Raum entsprechend bestimmter Ordnungsvorstellungen gestaltet. In diesem Rahmen kann Überwachungstechnik genutzt werden, um bestimmten Menschen die

[6] Vgl. Arzt/Fährmann/Schuster (2020) [18], Marosi/Skobel (2019a) [42], Marosi/Skobel (2019b) [43].

[7] Zur Drohnenabwehr vgl. etwa Heesen/Schuster/Arzt (2018) [32], Staben (2017) [62].

[8] Vgl. jüngst Arzt/Fährmann/Schuster (2020) [18].

[9] Vgl. Belina (2016) [22].

[10] Vgl. schon BVerfGE 65, 1 (42 ff.); ebenso bspw. BVerfGE 115, 320 (341 f.).

Nutzung dieses Raumes zu erschweren oder sie sogar zu vertreiben, etwa obdachlose oder drogenabhängige Menschen, auch wenn sie nichts Unzulässiges tun. Der Technikeinsatz ist somit auch ein Mittel sozialer Kontrolle, mit dem die Polizei die Nutzung des öffentlichen Raums steuern kann. Wenn sich Menschen zu Unrecht beobachtet fühlen, können auch Konflikte mit der Polizei entstehen.

Unsicherheiten und Sorgen werden auch dadurch verstärkt, dass Bürger:innen regelmäßig nicht nachvollziehen können, welche Daten erhoben werden und welche Zwecke die Polizei mit der von ihr eingesetzten Technik verfolgt. Die technischen Modalitäten und Möglichkeiten eingesetzter Geräte sind für Außenstehende kaum erkennbar. Unklar bleibt zumeist auch, was mit den erhobenen Daten geschieht. Selbst wenn Verhalten der Betroffenen von der Polizei tatsächlich nicht erfasst und dokumentiert wird (beispielsweise bei ausgeschalteten Geräten) oder der polizeiliche Technikeinsatz datenschutzkonform und rechtmäßig abläuft, wird das für viele Betroffene nicht ersichtlich. Insofern kann Transparenz ein Schlüsselkonzept zur Vermeidung von Einschüchterungseffekten polizeilicher Maßnahmen sein.[11] Umgekehrt kann indes auch gerade die offene Durchführung polizeilicher Maßnahmen Einschüchterungseffekte bewirken.[12]

Dieser Beitrag untersucht aus einer rechts- und verwaltungswissenschaftlichen Perspektive, inwiefern Transparenzdefizite bei der Ausgestaltung der polizeilichen Datenerhebung und weiteren Datenverarbeitung bestehen. Anschließend werden mögliche Instrumente zur Steigerung von Transparenz analysiert. Der Fokus liegt in diesem Beitrag auf der offenen polizeilichen Datenverarbeitung und klammert insofern spezifische, weiterreichende Probleme der verdeckten Datenverarbeitung aus, die bereits von ihrer Grundausrichtung her intransparent konzipiert ist.[13] „Verdeckt“ ist eine Datenverarbeitung dann, wenn die Polizei diese gezielt heimlich durchführt (wie etwa bei einer Telekommunikationsüberwachung oder Online-Durchsuchung) oder sie für die Betroffenen unter üblichen Umständen nicht erkennbar ist. „Offen“ ist daher zum Beispiel eine Ausweiskontrolle oder Befragung, von der die Betroffenen bereits durch ihre notwendige Mitwirkung erfahren. Der Beitrag zeigt, dass auch die offene Datenverarbeitung trotz rechtlicher Vorgaben für eine transparente Gestaltung an erheblichen Transparenzdefiziten leidet.

[11] Vgl. Held (2014) [33, S. 83].

[12] Vgl. Neskovic/Uhlig (2014) [44, S. 338].

[13] Näher hierzu Schwabenbauer (2018) [2], Aden (2018) [58, Rn. G 73 ff.].

2 Transparentes Verwaltungshandeln – Funktionen und rechtliche Anforderungen

Die Polizei kann Transparenz auf unterschiedlichen Ebenen herstellen. Interne Transparenz ermöglicht die Überprüfung staatlichen Handelns z. B. durch Innenrevisionen oder behördliche Datenschutzbeauftragte. Externe Transparenz umfasst beispielsweise Berichtspflichten ohne Personenbezug gegenüber der Öffentlichkeit oder die richterliche Vorabkontrolle für polizeiliche Eingriffsmaßnahmen. Schließlich kann auch gegenüber Betroffenen von polizeilichen Maßnahmen Transparenz hergestellt werden. Hier geht es nach der traditionellen Rechtskonzeption vornehmlich um (datenschutzrechtliche) Auskunfts- und Benachrichtigungspflichten gegenüber den Verfahrensbeteiligten[14] und um Rechte im Verwaltungsverfahren, insbesondere das Akteneinsichtsrecht.[15]

2.1 Funktionen und Wirkungen von Transparenz öffentlicher Verwaltungen

Die Wirkungen von Transparenz[16] und einer transparenten öffentlichen Verwaltung werden kontrovers diskutiert,[17] besonders in Deutschland, wo Verwaltungen traditionell weitgehend intransparent agierten (Verwaltungsarkanum).[18] Manche Akteure prognostizieren einen Verlust von Legitimität, wenn Verwaltungen gegen Regeln verstoßen und daher in der öffentlichen Debatte der Fokus primär auf diese Fehler gelegt wird und anderes Verwaltungshandeln außen vor bleibt.[19] Auch wird gelegentlich die Sorge geäußert, Menschen könnten bei der mit Transparenz einhergehenden Fülle von Informationen relevante Inhalte übersehen.[20] Sicherheitsbehörden betonen oft die Geheimhaltungsbedürftigkeit der von ihnen verarbeiteten Informationen, was Transparenz entgegenstehe.[21] Informationsfreiheit im Sinne eines Right to Information ist daher noch immer kein Allgemeingut in Deutschland.

---

[14] Gropp (1999) [30, S. 118].

[15] Kugelmann (2001) [39, S. 231 ff.].

[16] Hierzu Stehr/Wallner (2010) [63, S. 9].

[17] Zur Übersicht Richter (2017) [49, S. 236 ff.].

[18] Näher Aden (2004) [1, S. 66 ff.].

[19] Vgl. Fine Licht/Naurin/Esaiasson/Gilljam (2014) [29, S. 116–117].

[20] O'Neil (2006) [45, S. 86].

[21] Hierzu Aden (2018) [2], Riese (2019) [50], Velten (1996) [69, S. 17].

In der internationalen Verwaltungsforschung wird Transparenz dagegen ganz überwiegend die Funktion zugeschrieben, Vertrauen in behördliche Entscheidungsprozesse zu stärken[22] und dadurch deren Glaubwürdigkeit zu erhöhen.[23] Damit ist Transparenz ein zentraler Aspekt verantwortlichen Behördenhandelns im Sinne von *Accountability*.[24] Die Verfügungsgewalt über Informationen, die andere Akteur:innen nicht haben, führt ferner zu asymmetrischen Machtbeziehungen.[25] Bei der Polizei ist diese Asymmetrie besonders ausgeprägt, da sie über erhebliche Macht in Form von Eingriffsbefugnissen verfügt, die sie als Repräsentantin des staatlichen Gewaltmonopols nötigenfalls mit unmittelbarem Zwang durchsetzen kann. Polizeibeamt:innen handeln im Streifendienst und bei Notrufeinsätzen weitgehend eigenständig, sodass unangemessenes oder gar rechtswidriges Handeln regelmäßig der Leitungsebene gar nicht bekannt wird, wenn Beschwerden von außen oder innen ausbleiben. In solchen Fällen versagen innerbehördliche Kontrollmechanismen. Ob im Falle eines Bekanntwerdens eingeschritten oder im Sinne der *Cop Culture*[26] nichts unternommen wird, ist eine weitere Problematik. Deshalb ist es notwendig, möglichen Missbräuchen durch *Accountability-Foren* entgegenzuwirken.[27] Ein unabhängiges Monitoring, etwa durch Polizei- oder Datenschutzbeauftragte, trägt dazu bei, dass die Polizei eine Fehlerkultur entwickeln kann, um erkannte Fehler und Fehlverhalten durch verbesserte Konzepte zukünftig so weit wie möglich zu vermeiden.[28]

Die Polizei ist als Repräsentantin des staatlichen Gewaltmonopols stärker noch als andere Behörden auf Akzeptanz ihres Handelns in der Bevölkerung angewiesen. Nach der *Procedural Justice*-Theorie stoßen Entscheidungen von Institutionen wie der Polizei vor Allem dann auf Akzeptanz, wenn die Betroffenen sowohl den Entscheidungsprozess als auch das Ergebnis als fair empfinden.[29] Dies ist vielfach nur bei einer transparenten Gestaltung polizeilicher Maßnahmen denkbar. So bestätigen Forschungen zu Polizeieinsätzen, dass Transparenz in unterschiedlichen Einsatzsituationen zu einer Deeskalation von (potenziellen)

[22] Schaar (2015) [52, S. 15].

[23] Gropp (1999) [30, S. 104].

[24] Vgl. Bovens (2007) [23, S. 450].

[25] Zu den Herrschaftsaspekten von Wissensvorsprüngen: Aden (2004) [1].

[26] Grundlegend hierzu Behr (2000) [21].

[27] Töpfer/Normann (2014) [66, S. 5 ff.].

[28] Näher hierzu Aden (2019) [3].

[29] Tyler/Blader (2000) [68, S. 74–75], Tyler (2017) [67].

Konflikten beitragen kann.[30] Im Rahmen der Deeskalation kommt einer kontinuierlichen und fairen Kommunikation eine entscheidende Bedeutung zu, wobei vorrangig ist, die Beweggründe der jeweils anderen Seite zu verstehen[31] und das polizeiliche Handeln darauf auszurichten. Mit Fairness ist in diesem Kontext vor Allem eine nachvollziehbare Begründung der Maßnahme gemeint;[32] auch hier ist Transparenz gegenüber den Betroffenen ein zentrales Element. Intransparentes Vorgehen steigert nicht nur Einschüchterungseffekte, sondern auch das Misstrauen gegenüber dem polizeilichen Vorgehen und beschädigt damit die Akzeptanz polizeilicher Maßnahmen.

2.2 Verfassungsrechtliche Anforderungen

Transparentes staatliches Handeln ist eine verfassungsrechtliche Verpflichtung, die sich auf das Demokratie- und das Rechtsstaatsprinzip stützen kann. Das BVerfG hat die Bedeutung von Transparenz als Element des Demokratieprinzips (Art. 20 Abs. 2 GG) wiederholt betont.[33] In einer Demokratie muss staatliches Handeln für die Bürger:innen nachvollziehbar sein. Dies gilt für das Handeln der Sicherheitsbehörden auch deshalb, weil Intransparenz dazu führen kann, dass die Parlamente als demokratisch legitimierte Gesetzgeber das behördliche Handeln nicht nachvollziehen und kontrollieren können.[34]

Aus rechtsstaatlich-grundrechtlicher Perspektive ist auch relevant, dass intransparente polizeiliche Datenverarbeitung Bürger:innen davon abhalten kann, ihre Grundrechte wahrzunehmen, wenn für sie unklar ist, ob sie dabei von staatlicher Seite überwacht werden. Informationelle Selbstbestimmung setzt nach der ständigen Rechtsprechung des BVerfG voraus, dass die Einzelnen grundsätzlich frei entscheiden können, wer Informationen über sie hat. Jede Datenerhebung und -verarbeitung bedarf daher gerade im polizeilichen Handlungsfeld einer hinreichend bestimmten und verhältnismäßigen gesetzlichen Grundlage.[35] Daraus folgt eine staatliche Verpflichtung sicherzustellen, dass Abschreckungseffekte durch staatliche Eingriffe in das Grundrecht auf informationelle Selbstbestimmung so weit wie möglich vermieden werden, was durch offenes und nachvollziehbares

[30] z. B. Lorei/Kocab/Ellrich/Sohnemann (2017) [35, S. 114], Hücker (2017) [41, S. 26–27].
[31] Schmalzl/Hermanutz/Bodamer (2012) [55, S. 66].
[32] Lorei/Kocab/Ellrich/Sohnemann (2017) [41, S. 27].
[33] BVerfGE 40, 296 (327).
[34] Ausführlich dazu Grunwald (2010) [31, S. 85], Fährmann/Aden/Bosch (2020b) [28, S. 144].
[35] BVerfGE 65, 1 ff.

staatliches Handelns ermöglicht wird.[36] Auskunfts- und Aufklärungsansprüche der von staatlichen Eingriffen Betroffenen folgen daher unmittelbar aus dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.[37] Auch aus dem in der Vergangenheit wenig beachteten Grundrecht auf Informationsfreiheit (Art. 5 Abs. 1 Satz 1, 2. Halbsatz GG) lässt sich unter den Rahmenbedingungen von Digitalisierung und *Open Government* eine Verpflichtung des Staates ableiten, sein Handeln durch Veröffentlichung seiner vielfältigen Informationsbestände *transparent* zu machen.[38]

Auch aus der Versammlungsfreiheit folgen Transparenzanforderungen. In seinem Beschluss zum polizeilichen Umgang mit Demonstrationen am seinerzeit im Bau befindlichen Atomkraftwerk Brokdorf verwendete das BVerfG 1985 den Begriff *Transparenz* zwar nicht. Es etablierte in dieser Entscheidung aber das Kooperationsgebot, das Versammlungsbehörden und Polizei zu einer rechtzeitigen Kontaktaufnahme mit den Veranstalter:innen verpflichtet, „bei der beide Seiten sich kennenlernen, Informationen austauschen und möglicherweise zu einer vertrauensvollen Kooperation finden, welche die Bewältigung auch unvorhergesehener Konfliktsituationen erleichtert".[39] Eine Grundlage vertrauensvoller Kooperation besteht darin, dass beide Seiten die Beweggründe des Gegenübers nachvollziehen können. Bedenken der Versammlungsbehörde können nur dann ausgeräumt werden, wenn sie Anmelder:innen bzw. Veranstalter:innen der Versammlung bekannt sind.

Transparenz staatlichen Handelns ist zudem eine essenzielle Voraussetzung für die Wahrnehmung der grundrechtlichen Rechtsweggarantie (Art. 19 Abs. 4 GG). Nur wenn Betroffene von Grundrechtseingriffen erfahren, können sie dagegen rechtlich vorgehen. Mithin gehört zu den Anforderungen an eine verhältnismäßige Ausgestaltung von polizeilichen Überwachungsmaßnahmen die gesetzliche Anordnung von Benachrichtigungspflichten, um bei verdeckt durchgeführten Maßnahmen subjektiven Rechtsschutz im Sinne des Artikel 19 Abs. 4 GG gewährleisten zu können, soweit Personen bei oder im Gefolge der Maßnahme identifiziert wurden.[40] Für informationsbezogene Eingriffe, deren Vornahme oder Umfang die Betroffenen nicht sicher abschätzen können, sind Auskunftsrechte

[36] Vgl. Held (2014) [33, S. 83].

[37] BVerfGE 65, 1 ff.; Schmidt (2018) [56], 310 m. w. N.

[38] Ausführlich zur Begründung Lederer (2015) [40, S. 439 ff.].

[39] BVerfGE 69, 315 (355); zu den verfassungsrechtlichen Anforderungen s. a. Arzt (2009) [12].

[40] BVerfGE 109, 279 (295 f.); Schenke (2018) [53, Rn. 194].

vorzusehen, von denen allenfalls bei gegenläufigen Interessen von hinreichendem Gewicht Ausnahmen zugelassen werden können.[41]

2.3 Europarechtliche Anforderungen

Im Primärrecht der Europäischen Union hat Transparenz einen hohen Stellenwert. Ähnlich wie das BVerfG seit seiner Volkszählungsentscheidung aus dem Jahr 1983 definiert die EU-Grundrechtecharta Transparenz gegenüber den Betroffenen als essenzielles Element des Datenschutzgrundrechts. Nach Art. 8 Abs. 2 Satz 2 GRCh hat jede Person „das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken." Art. 42 GRCh gewährt darüber hinaus Zugang zu Dokumenten der EU-Organe.

Art. 5 Abs. 1 lit. a der EU-Datenschutzgrundverordnung 2016/679 erwähnt *Transparenz* folgerichtig als Datenschutzgrundsatz. In den Grundsätzen, die Art. 4 der Richtlinie (EU) 2016/680 für den Datenschutz im Polizei- und Strafjustizbereich („JI-Richtlinie") auflistet, fehlt hingegen eine explizite Erwähnung des Transparenzprinzips. Dennoch gilt dieses auch hier, nicht nur im Hinblick auf den Vorrang des Art. 8 GRCh in der Normenhierarchie des Unionsrechts, sondern auch weil Transparenz ein zentraler Bestandteil des Fairnessgebots aus Art. 4 Abs. 1 lit. a der JI-Richtlinie ist, das in der offiziellen deutschen Fassung etwas unglücklich mit „Treu und Glauben" übersetzt wurde.[42] Art. 13 der JI-Richtlinie etabliert zudem für das Polizeihandeln allgemeine Pflichten zur Transparenz. Betroffene sind demnach unter anderem über die Zwecke der Datenverarbeitung und über ihre Rechte zu informieren. Soweit Polizeitätigkeit nicht unter die JI-Richtlinie fällt, gelten die parallelen Vorschriften in Art. 13 DSGVO.

2.4 Einfachgesetzliche Ausgestaltung

Trotz der klaren verfassungs- und unionsrechtlichen Vorgaben[43] ist die einfachgesetzliche Ausgestaltung der Transparenz polizeilichen Handelns in den

[41] BVerfGE 141, 220 (283).

[42] So auch Johannes/Weinhold (2018) [36, S. 65] (= § 1 Rn. 128).

[43] Vgl. nur Schwichtenberg (2016) [58], Schwichtenberg (2020) [60], Weinhold/Johannes (2016) [70].

Landespolizei- und -datenschutzgesetzen bisher sehr allgemein gehalten.[44] Die Landesversammlungsgesetze blenden die Problematik der Datenverarbeitung bisher vollständig aus oder treffen allenfalls rudimentäre Regelungen zur Datenerhebung und -verarbeitung auch im Versammlungskontext. Die Umsetzung der JI-Richtlinie beschränkt sich zumeist auf eine weitgehend wörtliche Wiedergabe des Richtlinientextes. In Deutschland wurde Art. 13 der JI-Richtlinie in allgemeiner Form in den §§ 55 und 56 BDSG und den Landesdatenschutzgesetzen ohne inhaltliche Substantiierung umgesetzt (z. B. §§ 50 HDSIG oder 44 DSG NRW). Nach § 55 BDSG ist die Polizei nur verpflichtet, allgemeine Informationen über die polizeiliche Datenverarbeitung in leicht verständlicher Form öffentlich zur Verfügung zu stellen – beispielsweise auf einer Website.[45] Dazu gehören die grundsätzlichen Abläufe der Datenverarbeitung – vor allem in polizeilichen Datenbanken – und ihre Folgen und Konsequenzen für die Betroffenen (z. B. Verwendung der Daten und Speicherdauer) sowie Hinweise auf Rechtsmittel und Beschwerdeinstanzen, etwa Datenschutzbeauftragte oder ggf. polizeiliche Beschwerdestellen. Auch die Informationspflichten gegenüber den Betroffenen (§ 56 BDSG) orientieren sich an dem in der JI-Richtlinie vorgegebenen Minimalstandard.[46] Vor dem Hintergrund dieser sehr allgemein gehaltenen Regelungen verwundert es kaum, dass deutsche Polizeibehörden bisher wenig Anstrengungen unternommen haben, ihre Öffentlichkeitsarbeit den Transparenzanforderungen der JI-Richtlinie anzupassen.

Auskunftsrechte und Benachrichtigungspflichten sind einfachgesetzlich vorgesehen; sie haben sich allerdings als wenig effektiv erwiesen. Die Intransparenz polizeilicher Datenverarbeitung fördert auch Vollzugsdefizite, da Betroffene ihre Rechte nicht einfordern können, solange sie von der Datenverarbeitung nichts ahnen. Die allgemeinen Informationsfreiheitsgesetze sehen zudem weitreichende Ausnahmen für den Sicherheitsbereich vor, so beispielsweise § 3 des IFG des Bundes.

Nach dem Verwaltungsverfahrensgesetz des Bundes (VwVfG) sind regelmäßig nur schriftliche Verwaltungsakte zu begründen (§ 39). Bei mündlich angeordneten Verwaltungsakten – die bei polizeilichem Handeln im öffentlichen Raum der Regelfall sind – haben Betroffene aber nur einen Anspruch auf eine schriftliche Bestätigung, wenn sie hieran ein berechtigtes Interesse haben und dies unverzüglich verlangen (§ 37 Abs. 2 Satz 2). In der Praxis dürfte dies aber vielfach

[44] Vgl. etwa Arzt (2017) [13], Arzt (2019a) [14], Arzt (2019b) [15], Arzt (2019c) [16], Arzt (2020) [17].

[45] Schild (Stand 2019) [54], § 55 Rn. 4.

[46] Schwichtenberg (2018) [59], § 55 Rn. 1 f.

bereits daran scheitern, dass Betroffene dieses Recht nicht kennen und es daher nicht geltend machen. Zudem kommt es vor, dass Polizeibeamt:innen sich weigern, eine solche Bestätigung auszustellen. Mündliche Pflichten, das Vorgehen zu begründen, fehlen weitgehend.[47]

3 Ursachen für Transparenzdefizite polizeilichen Handelns

Im Folgenden werden strukturelle Ursachen für Transparenzdefizite polizeilichen Handelns im Allgemeinen (3.1) und für die polizeiliche Datenverarbeitung (3.2) untersucht.

3.1 Strukturelle Ursachen von Intransparenz polizeilichen Handelns

Mehrere Faktoren tragen dazu bei, dass Polizeiarbeit zu Intransparenz tendiert. Datenschutz genießt bei manchen Polizist:innen einen schlechten Ruf und wird oft fälschlicherweise als „Täterschutz“ oder als Gegensatz zum „Opferschutz“ verstanden.[48] Pflichten zu Transparenz in Form von Aufklärungs- und Benachrichtigungspflichten können aus einer polizeilichen Perspektive zudem als lästig und arbeitsintensiv empfunden werden.

Dabei haben verdeckte und damit *per definitionem* intransparente Eingriffsbefugnisse in den letzten Jahren stark an Bedeutung gewonnen, was schon vor Jahren, was schon vor 20 Jahren zutreffend als „Vernachrichtendienstlichung“ polizeilicher Tätigkeit bezeichnet wurde.[49] Zugleich ist die Bindung der Polizeiarbeit an klare und transparent nachvollziehbare Eingriffsvoraussetzungen durch neue Befugnisse im Vorfeld von konkreten Gefahren und Straftaten schwächer geworden.[50]

Auch die offene Datenverarbeitung ist für die Betroffenen oft wenig transparent, was aus der Perspektive der Polizeipraxis von Vorteil sein kann. Wissen

[47] Ausführlich dazu Aden/Fährmann/Bosch (2020) [10].

[48] z. B. https://www.gdp.de/gdp/gdpmp.nsf/id/74CC45DCEA6EDDA9C12580B500391749?open&search. So wird suggeriert, dass das Interesse am Schutz der eigenen Daten nicht schützenswert sei und auch, dass es nicht möglich sei, Opfer eines datenschutzwidrigen Verhaltens zu werden.

[49] So schon Paeffgen (2002) [46].

[50] Ausführlicher hierzu Albers/Weinzierl (2010) [11], Velten (1996) [69, S. 15].

die Adressat:innen polizeilicher Maßnahmen nicht, was die Polizei über sie weiß, so können sich hieraus für die Polizei taktische Vorteile ergeben, etwa bei der Vernehmung von Beschuldigten. Jeder Wissensvorsprung ist zugleich mit Macht gegenüber den Betroffenen verbunden,[51] die situationsbedingt genutzt werden kann. Dies gilt auch, wenn sich Betroffene über ihre Rechte und den rechtmäßigen Handlungsrahmen der Polizei nicht bewusst sind und daher rechtlich zweifelhafte oder gar rechtswidrige Eingriffsmaßnahmen über sich ergehen lassen. Dies kann insbesondere bei Menschen mit eingeschränktem Bildungshintergrund oder mangelnden Sprachkenntnissen der Fall sein, die erheblich in ihrer Beschwerdemacht beschränkt sind. In solchen Fällen kann Intransparenz dazu führen, dass Fehlverhalten nicht bemerkt oder ignoriert wird und daher ohne Konsequenzen bleibt.[52] Bei der Polizei kommt noch hinzu, dass sie selbst bei polizeilichem Fehlverhalten nicht nur für die disziplinarrechtlichen, sondern auch für die strafrechtlichen Ermittlungen zuständig ist. Die staatsanwaltschaftliche Verfahrensleitung funktioniert hier als Korrektiv nur unzulänglich. Externe *Accountability*-Foren wie Polizeibeauftragte, die zu mehr Transparenz polizeilichen Handelns beitragen könnten, gibt es bislang nur in einigen Bundesländern.[53]

Kontroverse Debatten über die polizeiliche Kennzeichnungspflicht oder die Ausstellung von Nachweisen über polizeiliche Kontrollen zeigen außerdem, dass manche Polizist:innen und Vertreter:innen ihrer Gewerkschaften transparenteres polizeiliches Handeln mit der Behauptung abwehren, Polizist:innen würden durch solche Vorschläge unter einen „Generalverdacht“ gestellt.[54] Insofern bewerten einige Polizist:innen intransparente Strukturen offenbar positiv, wobei die akzeptanzfördernden und deeskalierenden Effekte von Transparenz übersehen werden.

Intransparenz muss allerdings in Einsatzsituationen nicht immer machtorientiert und intentional sein. So können etwa die handelnden Polizist:innen die Rahmenbedingungen ihres Handelns so stark verinnerlicht haben, dass sie die Intransparenz ihrer Maßnahmen für die Betroffenen gar nicht wahrnehmen, während ihr Agieren für die Adressat:innen ungewohnt, intransparent oder belastend sein kann.

---

[51] Vgl. Aden (2004) [1], Roßnagel (2020) [51, 222 ff.].

[52] Velten (1996) [69, S. 16], zu potenziellen negativen Beispielen vgl. Singelnstein (2014) [61, S. 17], Witte (2012) [71, S. 62].

[53] Zur Übersicht Aden (2019) [3] m. w. N., in Berlin und in Bremen stehen entsprechende Stellen kurz vor der Einführung.

[54] Vgl. ausführlich zur Rolle der Polizeigewerkschaften Fährmann/Aden/Bosch (2020a) [27].

3.2 Spezielle Ursachen der Intransparenz polizeilicher Datenverarbeitung – Beispiele aus den Forschungsprojekten MEDIAN und AMBOS

Bei der polizeilichen Datenverarbeitung kommen weitere Ursachen für eine verbreitete Intransparenz hinzu. Vielfach fehlt es bereits an ausreichenden gesetzlichen Rahmenbedingungen für eine transparente Datenverarbeitung, da gesetzliche Regelungen aufgrund der Geschwindigkeit des technischen Fortschritts schnell obsolet werden. Neue technische Entwicklungen ermöglichen oftmals Eingriffsmaßnahmen, die faktisch schwerer wiegen als es die Gesetzgebung bei Erlass der Eingriffsbefugnisse absehen konnte.[55] Zudem tendiert die Gesetzgebung bereits seit Beginn der Umsetzung der BVerfG-Anforderungen aus der Volkszählungsentscheidung aus dem Jahr 1983 zur Schaffung abstrakter, weitgehend unbestimmter Normen für polizeiliche Informationseingriffe.[56] Dies führt dazu, dass (potenziell) Betroffene anhand des Gesetzestextes nicht ohne Weiteres nachvollziehen können, welche Befugnisse die Polizei in der konkreten Situation hat. Dies beginnt bereits bei „einfachen" und niedrigschwelligen Kontrollmaßnahmen.

Polizeiliche Personenkontrollen umfassen regelmäßig die Identitätsfeststellung und Befragungen. Im Rahmen des Forschungsprojekts MEDIAN zeigte sich, dass der Abgleich der Personendaten mit polizeilichen Datenbanken eine regelmäßig durchgeführte Folgemaßnahme ist. Die rechtlichen Voraussetzungen für einen solchen Datenbankabgleich sind dabei sehr allgemein formuliert – in der Regel reicht die Erforderlichkeit für die polizeiliche Aufgabenerfüllung aus –, sodass die rechtlichen Zugangshürden für Polizist:innen bei dieser Maßnahme sehr niedrig sind.[57] Für Betroffene ist in der Regel nicht ersichtlich, dass und mit welchen Datenbanken ihre Daten abgeglichen werden, ob die erhobenen Daten gespeichert werden und welche langfristigen Konsequenzen dieser Abgleich für sie hat,[58] obwohl Transparenz nach der hier vertretenen Rechtsauffassung bereits aufgrund der Vorgaben des EU-Rechts und des Verfassungsrechts (s. o., Abschn. 2) geboten wäre. Auch die handelnden Polizist:innen dürften indes kaum in der Lage sein, die Abläufe in den Hintergrundsystemen beim Datenabgleich präzise zu erläutern. Zudem werden Betroffene über den Zweck und die Konsequenzen des Datenabgleichs folglich regelmäßig nicht aufgeklärt. Durch die Nutzung mobiler Geräte, wie sie im MEDIAN-Projekt für polizeiliche Kontrollen erforscht werden, könnte

[55] Ausführlich hierzu Fährmann/Aden/Bosch (2020b) [28].

[56] Ausführlich Aden/Fährmann (2019a) [7], Aden/Fährmann (2019b) [8], Arzt (2019b) [15].

[57] Ausführlich dazu Aden/Fährmann (2019a) [7, S. 178.]

[58] Vgl. Aden/Bosch/Fährmann (2020) [5, S. 98–99].

die Intransparenz dessen, was mit den Daten der Betroffenen geschieht, noch weiter steigen, wenn hiergegen keine besonderen Vorkehrungen getroffen werden.

Auch für den gesamten Ablauf von Personenkontrollen gibt es in Deutschland weder klare gesetzliche Vorgaben noch einheitliche professionelle Standards, nicht zuletzt, weil die Maßnahme in Literatur und Rechtsprechung über Jahrzehnte hinweg als wenig grundrechtseingriffsintensiv eingeordnet wurde, was rechtlich und faktisch in vielen Konstellationen nicht zutreffend ist.[59] Die Aufklärung über Rechtsgrundlagen, Sinn und Zweck der Personenkontrolle und die damit verbundenen Maßnahmen bleibt somit den Polizist:innen vor Ort überlassen.[60] *De facto* unterbleibt diese Information oftmals. Die Betroffenen erfahren in diesen Fällen nicht, warum sie kontrolliert werden. Aufgrund der unklaren Vorgaben erfolgen Personenkontrollen in Deutschland zumeist aufgrund von Intuition, Gespür oder Erfahrungswissen der Polizist:innen,[61] wodurch das Risiko besteht, dass Vorurteile oder sogar Rassismus in die Auswahlentscheidung einfließen.[62]

Transparenzprobleme werden auch bei der polizeilichen Drohnenabwehr ersichtlich. Die zunehmende Nutzung von Drohnen durch Private birgt neue Gefährdungspotenziale für die öffentliche Sicherheit. Drohnen können durch unberechtigte Videoaufnahmen, die Nutzung eines hierfür gesperrten Luftraums oder unbeabsichtigte oder gezielte Abstürze einen Rechtsverstoß oder sogar eine Gefahr für Leben und Gesundheit der hiervon Betroffenen darstellen. Die im Projekt AMBOS entwickelte Technik zur Detektion von Drohnen und zur Intervention wird primär bei größeren Veranstaltungen, etwa den durch Art. 8 GG geschützten Versammlungen, bei Staatsbesuchen oder zum Schutz kritischer Infrastruktur eingesetzt werden. Damit eine solche Detektion und ggf. eine Intervention stattfinden kann, werden die hierfür notwendigen Detektionstechniken im öffentlichen Raum aufgebaut oder vorgehalten.[63] Die Detektion kann beispielsweise mittels Funk-, Akustik-, Elektro-Optik- (EO-), Infrarot- (IR) und Radarsensoren erfolgen. Als Interventionsmittel können beispielsweise Anwendungen zum Stören der Funkfernsteuerung oder Satellitennavigation *(Jamming),* hochpotente

[59] Hierzu instruktiv OVG Hamburg, NVwZ-RR 2015, 695; Burkhardt/Barskanmaz (2019) [24], Payandeh (2013) [47], Tomerius (2017) [64], Tomerius (2019) [65].

[60] Näher hierzu Aden/Fährmann/Bosch (2020) [10].

[61] Cremer (2013) [25, S. 31], Herrnkind (2014) [34, S. 45 ff.].

[62] Aden/Fährmann (2018) [6, S. 18], Keller (2018) [37, S. 21 ff.], Tomerius (2017) [64, S. 1400 ff.]

[63] Ausführlich Arzt/Fährmann/Schuster (2020) [18].

elektromagnetische Wellen (HPEM-Wellen) zum Stören der Elektronik oder Netzwerfer eingesetzt werden, die eine Drohne mittels eines verschossenen Fangnetzes unschädlich machen.

Für Versammlungsteilnehmer:innen und Menschen, die an anderen Veranstaltungen teilnehmen oder zufällig in Kontakt mit solchen Detektionsmitteln kommen, ist regelmäßig nicht ohne weitere Hinweise erkennbar, wofür die von der Polizei aufgestellten Kameras, Mikrofon- und Funkantennen oder Radarsensoren genutzt werden.[64] So kann der Eindruck entstehen, dass diese Technik der Überwachung anwesender Personen dient.[65] Gerade die Ungewissheit ob, wozu und in welcher Weise die mittels der Detektionstechnik gewonnenen Informationen später verwendet werden können, kann die Betroffenen in ihrem Recht hemmen, sich frei zu entfalten oder ungehindert zu versammeln. Wer unsicher ist, ob bestimmte Verhaltensweisen jederzeit notiert und als Informationen ggf. dauerhaft gespeichert, verwendet oder weitergegeben werden, wird mit einiger Wahrscheinlichkeit versuchen, nicht durch solche Verhaltensweisen aufzufallen.[66]

Zusätzlich wirken Interventionsmittel wie etwas ein Netzwerfer oder ein Gerät, das HPEM-Wellen aussendet, martialisch und einschüchternd. Diese Geräte erinnern eher an militärische Gegenstände und können leicht mit Waffen verwechselt werden. Da diese zusätzlich zu den Mitteln der Detektion vor Ort sein müssen, kann der Eindruck entstehen, dass es sich um eine Veranstaltung handelt, die im höchsten Maße dem Risiko von Angriffen ausgesetzt oder die besonders gefährlich ist, zum Beispiel mit Blick auf die Teilnehmenden.

Zusammenfassend kann daher festgehalten werden, dass Funktionsweise und Nutzung neuartiger technischer Geräte zur Bild- und Tonaufzeichnung, zum Datenabgleich oder zur Gefahrendetektion für die Betroffenen weitgehend intransparent sind und den Grundrechtsgebrauch qua Einschüchterung beeinträchtigen können. Daher ist es überaus wichtig, dass das Einsatzziel solcher Technik für die Menschen im öffentlichen Raum problemlos erkennbar ist.

4 Wege zu einer transparenteren polizeilichen Datenverarbeitung

Aufgrund der weiterhin hochdynamischen Technikentwicklung kann Gesetzgebung allein kaum eine transparentere polizeiliche Datenverarbeitung erzwingen.

[64] Ebd.

[65] Vertiefend Arzt/Fährmann/Schuster (2020) [18].

[66] So schon BVerfGE 65, 1, 43; VG Berlin, NVwZ 2010, 1442.

Besonderer Aufmerksamkeit bedarf daher die Konzeption der eingesetzten Technik wie auch deren Nutzung. Chancen hierfür bieten sich im Rahmen der interdisziplinären Zusammenarbeit zwischen Jurist:innen und Techniker:innen in interdisziplinären Projekten der Sicherheitsforschung, wie beispielsweise AMBOS und MEDIAN.

Rechtliche Anknüpfungspunkte für eine transparente Ausgestaltung polizeilicher Technik sind die Datenschutzfolgenabschätzung sowie datenschutzfreundliche Technikgestaltung und Voreinstellungen technischer Geräte *(privacy by design and by default;* Art. 20 JI-Richtlinie; Art. 25 DSGVO). Hinzu kommen geeignete technisch-organisatorische Maßnahmen. Eine Datenschutzfolgenabschätzung (Art. 27 JI-Richtlinie, Art. 35 DSGVO) soll die Wirkungen der Anwendung unter Berücksichtigung der Perspektive der Betroffenen analysieren. Externe Expert:innen und Betroffene sind daher – entgegen der bisher überwiegenden Praxis – auch bei der polizeilichen Datenschutzfolgenabschätzung maßgeblich zu beteiligen.[67] *Privacy by design* ist ein Schlüsselkonzept zur Verbesserung von Datenschutzstandards und zur Herstellung von Transparenz an der Schnittstelle zwischen Technik und Recht. Nach diesem Grundsatz darf die datenschutzkonforme Techniknutzung nicht dem Verhalten der Nutzer:innen überlassen bleiben, sondern sie muss durch geeignete technische und organisatorische Maßnahmen bereits während der Technikentwicklung sichergestellt werden.[68] Das Datenschutzrecht soll nämlich nicht nur negative Technikfolgen verringern, sondern bereits während der Technikentwicklung dafür sorgen, dass Grundrechtseingriffe bei der Anwendung der Technik so gering und transparent wie möglich ausgestaltet werden.[69] Noch besser wäre indes ein Konzept, das bereits vor der Technikentwicklung fragt, ob eine bestimmte Überwachungstechnik überhaupt gesellschaftlich gewollt ist,[70] ggf. in welchen Grenzen und unter welchen Voraussetzungen. Auf dieser Basis sollte der parlamentarische Gesetzgeber über die Techniknutzung entscheiden.[71]

Gerade Transparenzmechanismen müssen bereits bei der Technikgestaltung mitgedacht werden. Technische Anwendungen und Systeme sind von vornherein so zu gestalten, dass Intransparenz entweder ausgeschlossen ist oder Mechanismen zur Sicherstellung eines transparenten Vorgehens in die Anwendungen integriert werden. So kann etwa eine Statistikfunktion vorgesehen werden, die

[67] Ausführlich zur polizeilichen Datenschutzfolgenabschätzung Aden/Fährmann (2020) [9].

[68] Baumgartner/Gausling (2017) [20, S. 310].

[69] Baumgartner/Gausling (2017) [20, S. 310], Johannes/Weinhold (2018) [36, S. 113].

[70] Vertiefend Arzt/Rappold (2019) [19].

[71] Vgl. LVerfG Sachsen-Anhalt, Urt. v. 11.11.2014 – LVG 9/13, S. 35 f.

für die Öffentlichkeit nachvollziehbar macht, wie oft und zu welchen Zwecken polizeiliche Technik genutzt wird. Dabei können auch Schutzmechanismen gegen eine Verfälschung integriert werden, etwa dergestalt, dass die Daten auf einem externen Server gespeichert werden, zum Beispiel bei den Polizeibeauftragten. Diskutiert wurde dies zum Beispiel für Bodycam-Aufnahmen und deren Speicherung bei einer Treuhandstelle.[72] Monitoring-Instanzen wie zum Beispiel Datenschutz- oder Polizeibeauftragte hätten so bei Bedarf unmittelbaren Zugriff auf die Datenauswertung.

Ferner kann abhängig von der Maßnahme auch eine Nachweisfunktion („Quittung“) in technische Anwendungen integriert werden und zu mehr Transparenz beitragen. Für Maßnahmen, die im Zuge einer Personenkontrolle erfolgen, sollte die gesetzliche Verpflichtung etabliert werden, den Betroffenen eine „Quittung“ auszustellen, in der die Zwecke der Maßnahme, Ort und Zeit, das Ergebnis und die Identität der kontrollierenden Beamt:innen festgehalten sind (ggf. in Form eines Pseudonyms oder der polizeilichen Kennzeichnung). Sofern die Quittungsdaten nur für die Betroffenen einsehbar sind, bedarf es dafür keiner Ermächtigungsgrundlage. Jedoch ist davon auszugehen, dass polizeiliche Transparenzmaßnahmen nur aufgrund einer gesetzlichen Verpflichtung flächendeckend umgesetzt werden. Eine solche „Quittung“ könnte dazu dienen, dass Betroffene nachweisen können, dass, weshalb und wie oft sie kontrolliert worden sind. Sie könnte auch Rechtschutzhinweise enthalten bzw. darauf hinweisen, wo hierzu weiterführende Informationen zu finden sind. Die Inhalte könnten unmittelbar aus der jeweiligen polizeilichen Anwendung generiert werden. Beispielsweise könnte bei mobilen Geräten, die bei Kontrollen eingesetzt werden, die Menüführung so gestaltet werden, dass sich aus dieser und den Zugangsdaten automatisch der Inhalt der „Quittung“ ergibt, wodurch der Arbeitsaufwand für die Polizist:innen äußerst gering wäre. Im Projekt MEDIAN wurde gezeigt, dass solche Nachweise mit sehr geringem Arbeitsaufwand elektronisch generiert und ausgestellt werden können.[73]

Des Weiteren können (mobile) technische Anwendungen dazu beitragen, dass das Handeln der Beamt:innen für die jeweiligen Vorgesetzten transparent ist, indem das polizeiliche Handeln statistisch erfasst wird, wobei auch die datenschutzrechtlichen Belange der Polizist:innen angemessen berücksichtigt werden müssen. Transparenz kann in einigen Fällen auch im Eigeninteresse der Beamt:innen liegen, etwa wenn ihr Aufenthaltsort bei einem Notfall mithilfe mobiler Geräte geortet werden kann.

[72] Kipker/Gärtner (2015) [38, S. 299].

[73] Vgl. dazu Aden/Bosch/Fährmann (2020) [5], Aden/Fährmann/Bosch (2020) [10].

Eine effektive externe Kontrolle setzt eine mit wirksamen Befugnissen ausgestattete Stelle voraus; dies gilt sowohl für Datenschutz- als auch für Polizeibeauftragte. Hierfür ist erforderlich, dass die gesamte Datenverarbeitung vollständig protokolliert und durch technische und organisatorische Maßnahmen sichergestellt wird, dass die Protokolldaten im Bedarfsfall zur Verfügung stehen und hinreichende und konsistente Angaben zu dem jeweiligen Vorgang enthalten.[74] Den Interessen der Polizist:innen und externen Betroffenen am Schutz ihrer personenbezogenen Daten ist dabei durch technisch-organisatorische Maßnahmen wie frühzeitige Sperrung, klare Löschfristen und Zugriffsberechtigungen Rechnung zu tragen. Solche technisch-organisatorischen Maßnahmen können indes nicht allein der Polizei überlassen werden, sondern sind gesetzlich hinreichend detailliert zu regeln.[75]

Der Gesetzgeber sollte klar festlegen, wann die Polizei welche Transparenzmechanismen anzuwenden hat. Hier könnten in einem allgemeinen Teil generelle Transparenzvorschriften festgehalten werden. Daraus kann etwa folgen, dass die Polizei den Zweck einer öffentlichen Datenerhebung für alle Betroffenen erkennbar und nachvollziehbar begründen muss. Die Polizei sollte verpflichtet werden, Datenverarbeitungsabläufe zu erklären, etwa beim Kontakt mit Betroffenen, sofern dies in der Einsatzsituation ohne Eigengefährdung möglich ist. Mittel zur Datenerhebung wie etwa Kameras könnten mit Hinweisen auf eine Website versehen werden, etwa mittels eines *Quick Response* (QR)-Codes, der die Betroffenen bei Interesse zu den notwendigen Informationen führt.[76]

5 Schlussfolgerungen und Ausblick

Dieser Beitrag hat gezeigt, dass die polizeiliche Datenverarbeitung an erheblichen Transparenzdefiziten leidet und die rechtlichen Vorgaben für transparentes Behördenhandeln im Polizeibereich bisher kaum angekommen sind. Die Vorgaben des EU-Datenschutzrechts wurden in Deutschland auf Minimalniveau umgesetzt und haben bisher kaum zu mehr Transparenz polizeilicher Datenverarbeitung beigetragen. Hier bleibt abzuwarten, inwieweit die Europäische Kommission und die Rechtsprechung des Gerichtshofs der EU Deutschland zu höheren Standards zwingen. Der Grundsatz des Datenschutzes durch Technikgestaltung sollte

[74] Vgl. BVerfGE 141, 220, Rn. 140 f.; Petri (2018) [48, Rn. G 60 f.].

[75] Vgl. etwa Arzt (2020) [17, § 23 PolG NRW Rn. 47 ff.], Schmidt (2018) [56, 303] m.w.N

[76] Vgl. Arzt/Fährmann/Schuster (2020) [18].

gesetzlich weiter konkretisiert werden. Das Verfahren der Datenschutzfolgenabschätzung und die zu beteiligenden Akteure sollten darüber hinaus gesetzlich klarer festgelegt werden.[77] Eine konsequente datenschutzfreundliche Technikgestaltung kann zu einer wesentlich transparenteren polizeilichen Datenverarbeitung beitragen. Interdisziplinäre Projekte der Sicherheitsforschung wie AMBOS und MEDIAN können hierfür gangbare Wege aufzeigen.

Literatur

1. Aden, H.: Herrschaft und Wissen. In: Aden, H. (Hrsg.) Herrschaftstheorien und Herrschaftsphänomene, S. 55–70. VS Verlag, Wiesbaden (2004)
2. Aden, H.: Information Sharing, Secrecy and Trust among Law Enforcement and Secret Service Institutions in the European Union. West Eur. Polit. (WEP) **2018**, 981–1002 (2018)
3. Aden, H.: Unabhängige Polizei-Beschwerdestellen und Polizeibeauftragte. In: Kugelmann, D. (Hrsg.) Polizei und Menschenrechte, S. 171–185. Bundeszentrale für politische Bildung, Bonn (2019)
4. Aden, H.: Interoperability between EU Policing and Migration Databases: Risks for Privacy. Eur. Public Law **2020**, 93–108 (2020)
5. Aden, H., Bosch, A., Fährmann, J.: Kontrollieren – aber wie? Können technische Innovationen die Akzeptanz für polizeiliche Personenkontrollen verbessern. In: Groß, H., Schmidt, P. (Hrsg.) Polizei und Migration. Empirische Polizeiforschung XXIII, S. 90–108. Verlag für Polizeiwissenschaft, Frankfurt a. M. (2020)
6. Aden, H., Fährmann, J.: Polizeirecht vereinheitlichen? Kriterien für Muster- Polizeigesetze aus rechtsstaatlicher und bürgerrechtlicher Perspektive. (2018) https://www.boell.de/sites/default/files/endf_e-paper_polizeirecht_vereinheitlichen.pdf. Zugegriffen: 20. Okt. 2020
7. Aden, H., Fährmann, J.: Defizite der Polizeirechtsentwicklung und Techniknutzung. ZRP **2019**, 175–178 (2019a)
8. Aden, H., Fährmann, J.: Wie lassen sich Informationseingriffe der Polizei wirksam gesetzlich begrenzen? Vorgänge **227**, 95–106 (2019b)
9. Aden, H., Fährmann, J.: Datenschutz-Folgenabschätzung und Transparenzdefizite der Techniknutzung. Eine Untersuchung am Beispiel der polizeilichen Datenverarbeitungstechnologie, TATuP **3**, 24–28 (2020)
10. Aden, H., Fährmann, J., Bosch, A. Intransparente Polizeikontrollen – rechtliche Pflichten und technische Möglichkeiten für mehr Transparenz. In: Hunold, D., Ruch, A. (Hrsg.) Polizeiarbeit zwischen Praxishandeln und Rechtsordnung. Empirische Polizeiforschungen zur polizeipraktischen Ausgestaltung des Rechts, S. 3–22. Springer VS, Wiesbaden (2020)

[77] Ausführlich dazu Aden/Fährmann (2020) [9].

11. Albers, M., Weinzierl, R.: Wandel der Sicherheitspolitik. Menschenrechtsorientierte Evaluierung als Kontrollinstrument. In: Albers, M., Weinzierl, R. (Hrsg.): Menschenrechtliche Standards in der Sicherheitspolitik. Beiträge zur rechtsstaatsorientierten Evaluierung von Sicherheitsgesetzen, S. 9–12. Nomos, Baden-Baden (2010)
12. Arzt, C.: Das Bayerische Versammlungsgesetz von 2008. DÖV **2009**, 381–388 (2009)
13. Arzt, C.: Das neue Gesetz zur Fluggastdatenspeicherung. Einladung zur anlasslosen Rasterfahndung durch das BKA, DÖV **2017**, 1023–1030 (2017)
14. Arzt, C.: Neues Polizeirecht in NRW – Von Gefährdern und anderen drohenden Gefahren für den Rechtsstaat. Die Polizei **2019**, 353–359 (2019a)
15. Arzt, C.: Neues Polizeirecht in Brandenburg – Rot-Rot kein Garant für die Bürgerrechte, Vorgänge 2019. Nr. **224**, 171–182 (2019b)
16. Arzt, C.: Umsetzung des europäischen Datenschutzrechts in Sachsen – SächsPVDG und SächsDSUG: eine kritische Bestandsaufnahme. SächsVBl. **2019**, 345–352 (2019c)
17. Arzt, C.: Kommentierung § 23 PolG NRW. In: Möstl, M., Kugelmann, D. (Hrsg.) Polizei- und Ordnungsrecht Nordrhein-Westfalen, 15. Aufl. C.H. Beck, München (2020)
18. Arzt, C., Fährmann, J., Schuster, S.: Polizeiliche Drohnenabwehr. Detektion, Verifikation und Intervention – Grundrechtseingriffe und Eingriffsbefugnisse. DÖV **2020**, 866–877 (2020)
19. Arzt, C., Rappold, V.: Rechtliche Einhegung neuer polizeilicher Maßnahmen als Herausforderung. Überlegungen zu Chancen und Risiken der Beteiligung an der zivilen Sicherheitsforschung. In: Draude, C., Lange, M., Sick, M. (Hrsg.) INFORMATIK 2019 Workshops, Lecture Notes in Informatics (LNI), S. 403–419. Bonn (2019)
20. Baumgartner, U., Gausling, T.: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Was Unternehmen jetzt nach der DS-GVO beachten müssen, ZD **2017**, 308–313 (2017)
21. Behr, R.: Cop Culture – der Alltag des Gewaltmonopols. Männlichkeit, Handlungsmuster und Kultur in der Polizei. Leske + Budrich, Opladen (2000)
22. Belina, B.: Der Alltag der Anderen: Racial Profiling in Deutschland. In: Dollinger, B., Schmidt-Semisch, H. (Hrsg.) Sicherer Alltag? Politiken und Mechanismen der Sicherheitskonstruktion im Alltag, S. 125–146. Springer VS, Wiesbaden (2016)
23. Bovens, M.: Analysing and Assessing Accountability. A Conceptual Framework, Eur. Law J. **2007**, 447–468 (2007)
24. Burkhardt, M., Barskanmaz, C.: Verfassungsrechtliche Bewertung der Vorschrift des § 21 Abs.2 Nr. 1 des Allgemeinen Gesetzes zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin – das Konzept der kriminalitätsbelasteten Orte. Berlin (2019). https://kop-berlin.de/files/175. Zugegriffen: 2. Dez. 2020
25. Cremer, H.: Studie „Racial Profiling" – Menschenrechtswidrige Personenkontrollen nach § 22 Abs. 1 a Bundespolizeigesetz. Empfehlungen an den Gesetzgeber, Gerichte und Polizei. Deutsches Institut für Menschenrechte, Berlin (2013)
26. Fährmann, J.: Digitale Beweismittel und Datenmengen im Strafprozess. MMR **2020**, 228–233 (2020)
27. Fährmann, J., Aden, H., Bosch, A.: Polizeigewerkschaften und innenpolitische Gesetzgebung – politische Einflussnahme zwischen Symbolpolitik und Interessenvertretung. Der Moderne Staat **2020**, 363–383 (2020a)

28. Fährmann, J., Aden, H., Bosch, A.: Technologieentwicklung und Polizei: intensivere Grundrechtseingriffe auch ohne Gesetzesänderung. Kriminologisches J. **2020**, 135–148 (2020b)
29. de Fine Licht, J., Naurin, D., Esaiasson, P., Gilljam, M.: When Does Transparency Generate Legitimacy? Experimenting on a Context-Bound Relationship, Governance **2014**, 111–134 (2014)
30. Gropp, W.: Transparenz der polizeilichen Befugnisanwendung. In: Bäumler, H., Arens, H.-W. (Hrsg.) Polizei und Datenschutz. Neupositionierung im Zeichen der Informationsgesellschaft, S. 104–120. Luchterhand, Neuwied (1999)
31. Grunwald, A.: Parlamentarische Technikfolgenabschätzung als Beitrag zur Technology Governance. In: Aichholzer, G., Bora, A., Bröchler, S., Decker, M., Latzer, M. (Hrsg.): Technology Governance. Der Beitrag der Technikfolgenabschätzung, S. 85–92. Edition Sigma, Berlin (2010)
32. Heesen, J., Schuster, S., Arzt, C.: Ethische und rechtliche Bewertung von Projekten zur zivilen Drohnenabwehr. TATuP **2018**, 32–37 (2018)
33. Held, C.: Intelligente Videoüberwachung. Verfassungsrechtliche Vorgaben für den polizeilichen Einsatz. Duncker & Humblot, Berlin (2014)
34. Herrnkind, M.: Filzen Sie die üblichen Verdächtigen, oder: Racial Profiling in Deutschland. Polizei & Wissenschaft **2014**, 35–58 (2014)
35. Hücker, F.: Rhetorische Deeskalation. Deeskalatives Einsatzmanagement. 4. Aufl. Boorberg, Stuttgart (2017)
36. Johannes, P.C., Weinhold, R.: Das neue Datenschutzrecht bei Polizei und Justiz. Europäisches Datenschutzrecht und deutsche Datenschutzgesetze. Nomos, Baden-Baden (2018)
37. Keller, N.: Wer hat Angst vorm Kottbusser Tor? Zur Konstruktion „gefährlicher Orte“, CILIP, **115**, 18–24 (2018)
38. Kipker, D.K., Gärtner, H.: Verfassungsrechtliche Anforderungen an den Einsatz polizeilicher „Body-Cams“, NJW, 296–301 (2015)
39. Kugelmann, D.: Die informatorische Rechtsstellung des Bürgers. Mohr Siebeck, Tübingen (2001)
40. Lederer, B.: Open Data. Informationsöffentlichkeit unter dem Grundgesetz. Duncker & Humblot, Berlin (2015)
41. Lorei, C., Kocab, K., Ellrich, K., Sohnemann, J.: Kommunikation statt Gewalt. Verlag für Polizeiwissenschaft, Frankfurt a. M. (2017)
42. Marosi, J., Skobel, E.: Drohnende Gefahr? – Drohnendetektion de lege lata und de lege ferenda. DVBl. **2019**, 678–684 (2019a)
43. Marosi, J., Skobel, E.: Mit „Kanonen“ auf Drohnen schießen? Computer und Recht **2019**, 65–72 (2019b)
44. Neskovic, W., Uhlig, D.: Übersichtsaufnahmen von Versammlungen. NVwZ **2014**, 335 (2014)
45. O‘Neil, O.: Transparency and the Ethics of Communication. In: Hood, C., Heald, D. (Hrsg.) Transparency. The key to better governance? S. 75–90. Oxford Univ. Press, Oxford (2006)
46. Paeffgen, H.-U.: Vernachrichtendienstlichung von Strafprozess- (und Polizei-)Recht. StV **2002**, 336 (2002)
47. Payandeh, M.: Gefahrenabwehr gegen Bildaufnahmen von Polizeikräften. NVwZ **2013**, 1458–1461 (2013)

48. Petri, T.: G, Informationsverarbeitung im Polizei- und Strafverfahrensrecht. In: Lisken, H., Denninger, E. (Hrsg./Begründer) Handbuch des Polizeirechts. Gefahrenabwehr – Strafverfolgung – Rechtsschutz. 6. Aufl., S. 763–1108. C.H. Beck, München (2018)
49. Richter, P.: Es werde Licht! Und es ward Licht? – Zur Wirkung von Transparenz auf die Legitimität öffentlicher Verwaltung. Politische Vierteljahresschrift **2017**, 234–257 (2017)
50. Riese, D.: Grenzen der Transparenz – Geheimhaltung in demokratischen Systemen. In: August, V., Osrecki, F. (Hrsg.) Der Transparenzimperativ. Normen-Praktiken-Strukturen, S. 95–122. Springer Fachmedien Wiesbaden GmbH & Springer VS, Wiesbaden (2019)
51. Roßnagel, A.: Technik, Recht und Macht. Aufgabe des Freiheitsschutzes in Rechtsetzung und -anwendung im Technikrecht, MMR **2020**, 222–228 (2020)
52. Schaar, P.: Zwischen Öffentlichkeit und Datenschutz. In: Arnim, H. H. von (Hrsg.): Transparenz contra Geheimhaltung in Staat, Verwaltung und Wirtschaft. Beiträge auf der 16. Speyerer Demokratietagung vom 23. bis 24. Oktober 2014 an der Deutschen Universität für Verwaltungswissenschaften Speyer, S. 27–34. Duncker & Humblot, Berlin (2015)
53. Schenke, W.-R.: Polizei- und Ordnungsrecht, 10. Aufl. C.F. Müller, Heidelberg (2018)
54. Schild, H. H.: § 55. In: Wolff, H. A., Brink, S. (Hrsg.) BeckOK Datenschutzrecht. 29. Aufl. C.H. Beck, München (Stand 2019)
55. Schmalzl, H.-P., Hermanutz, M., Bodamer, L.: Moderne Polizeipsychologie in Schlüsselbegriffen, 3. Aufl. Boorberg, Stuttgart (2012)
56. Schmidt, F.: Polizeiliche Videoüberwachung durch den Einsatz von Bodycams. Nomos, Baden-Baden (2018)
57. Schwabenbauer, T.: Informationsverarbeitung im Polizei- und Strafverfahrensrecht. In: Lisken, H., Denninger, E. (Hrsg./Begründer) Handbuch des Polizeirechts. Gefahrenabwehr – Strafverfolgung – Rechtsschutz. 6. Aufl., S. 763–1108. C.H. Beck, München (2018)
58. Schwichtenberg, S.: Die „kleine Schwester" der DSGVO: Die Richtlinie zur Datenverarbeitung bei Polizei und Justiz. DuD **2016**, 605–609 (2016)
59. Schwichtenberg, S.: § 55 DS-GVO. In: Kühling, J., Buchner, B. (Hrsg): Datenschutz-Grundverordnung/BDSG. Kommentar. 2. Aufl. C.H. Beck, München (2018)
60. Schwichtenberg, S.: Das neue BDSG und die StPO: zwei, die bislang noch nicht zusammengefunden haben, NK 2020, S 91–105 (2020)
61. Singelnstein, T.: Körperverletzung im Amt durch Polizisten und die Erledigungspraxis der Staatsanwaltschaften – aus empirischer und strafprozessualer Sicht, JK 2014, S. 15–27 (2014)
62. Staben, J.: Der Abschreckungseffekt auf die Grundrechtsausübung. Strukturen eines verfassungsrechtlichen Arguments. Mohr Siebeck, Tübingen (2017)
63. Stehr, N., Wallner, C.: Transparenz: Einleitung. In: Jansen, S. A., Schröter, E., Stehr, N., Wallner, C. (Hrsg.) Transparenz. Multidisziplinäre Durchsichten durch Phänomene und Theorien des Undurchsichtigen, S. 9–19. Wiesbaden, VS Verlag (2010)
64. Tomerius, C.: „Gefährliche Orte" im Polizeirecht – Straftatenverhütung als Freibrief für polizeiliche Kontrollen? Eine Beurteilung aus verfassungs- und polizeirechtlicher Perspektive, DVBl **2017**, 1399–1406 (2017)
65. Tomerius, C.: Die Identitätsfeststellung im Licht der neueren Rechtsprechung. DVBl. **2019**, 1581–1588 (2019)

66. Töpfer, E., von Normann, J.: Unabhängige Polizei-Beschwerdestellen. Eckpunkte für ihre Ausgestaltung. Dt. Inst. für Menschenrechte, Berlin (2014)
67. Tyler, T.: Procedural Justice and Policing: A Rush to Judgment? Ann. Rev. Law Soc. Sci. **2017**, 29–53 (2017)
68. Tyler, T. R., Blader, S. L.: Cooperation in Groups. Procedural Justice, Social Identity, and Behavioral Engagement. Psychology Press, Philadelphia (2000)
69. Velten, P.: Transparenz staatlichen Handelns und Demokratie. Zur Zulässigkeit verdeckter Polizeitätigkeit. Centaurus, Pfaffenweiler (1996)
70. Weinhold, R., Johannes, P.C.: Europäischer Datenschutz in Strafverfolgung und Gefahrenabwehr (…). DVBl. **2016**, 1501–1506 (2016)
71. Witte, A.: Grauzonen. Funktionsweisen der Beniner Polizei und ihr Verhältnis zur Bevölkerung, Arbeitspapiere des Instituts für Ethnologie und Afrikastudien der Johannes Gutenberg-Universität Mainz (2012). https://www.ifeas.uni-mainz.de/files/2019/07/AP133.pdf. Zugegriffen: 20. Okt. 2020

Datenübertragbarkeit – Zwischen Abwarten und Umsetzen

Özlem Karasoy, Gülcan Turgut und Martin Degeling

Zusammenfassung

Mit der europäischen Datenschutzgrundverordnung wurde das Recht auf Datenübertragbarkeit eingeführt. Die Erwartungen an dieses neue Betroffenenrecht waren, dass es die informationelle Selbstbestimmung der Einzelnen stärken und Netzwerk-Effekte verringern kann. Basierend auf zwei qualitativen Studien mit Betroffenen und Unternehmen ziehen wir eine erste Bilanz. Unsere Ergebnisse zeigen, dass das Recht bisher in der Praxis kaum Relevanz hat. Aufgrund der geringen Nachfrage zögern Unternehmen, Schnittstellen bereitzustellen und Anfragen werden häufig per Hand beantwortet. Die Betroffenen wiederum sehen zwar theoretische Vorteile, aber Dienste, die den Import von Daten von Plattformen erlauben, sind rar und es besteht Skepsis gegenüber der Weitergabe umfangreicher Datensätze. Beide Gruppen sehen große Überschneidungen zwischen dem Recht auf Datenübertragbarkeit und dem Recht auf Auskunft. Für die Praxis scheint es daher sinnvoll, Hybridmodelle zu entwickeln, bei denen sowohl eine erklärende Auskunft als auch eine konfigurierbare Abrufmöglichkeit für die Daten bereitgestellt werden. Um in Zukunft die gewünschte Übertragung zwischen zwei Verantwortlichen zu ermöglichen,

Ö. Karasoy (✉) · G. Turgut · M. Degeling
Ruhr-Universität Bochum, Bochum, Deutschland
E-Mail: Oezlem.Guedel@rub.de

G. Turgut
E-Mail: guelcan.kilci@rub.de

M. Degeling
E-Mail: martin.degeling@rub.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_16

braucht es darüber hinaus Anreize zur Entwicklung von Schnittstellen sowie Vorgaben zu Formaten und Umfang.

Schlüsselwörter

Datenübertragbarkeit • Betroffenenrechte • Datenportabilität

1 Das Recht auf Datenübertragbarkeit

In der Öffentlichkeit wird mit Datenschutzgesetzen vor allem auf der Schutz personenbezogener Daten vor Missbrauch assoziiert. Der europäische Gesetzgeber verband aber sowohl mit der früheren Richtlinie 95/46/EG als auch mit der Datenschutzgrundverordnung (DSGVO) das Ziel, den Datenaustausch im europäischen Binnenmarkt zu erleichtern. Die DSGVO sieht dazu unter anderem das Recht auf Datenübertragbarkeit oder „data portability" vor, das Betroffenen mehr Kontrolle über die sie betreffenden personenbezogenen Daten geben und gleichzeitig den Datenaustauch zwischen (datenschutzkonformen) Dienstleistern fördern soll. Eines der Ziele dieser Förderung war es, Datenmonopole zu verhindern.

Im Vergleich zum Recht auf Auskunft, das die DSGVO ebenfalls vorsieht und das sich mit dem Recht auf Datenübertragbarkeit überschneidet, liegt der Fokus darauf, dass die Daten direkt – entweder durch die Betroffenen selbst oder durch einen anderen Verantwortlichen – weiterverarbeitet werden können.

Konkret haben Betroffene nach Art. 20 DSGVO das Recht, ihre personenbezogenen Daten auf Verlangen in einem „strukturierten, gängigen und maschinenlesbaren Format" zu erhalten oder direkt zu einem neuen Verantwortlichen übertragen zu lassen. Voraussetzung dafür ist, dass die Daten von den Betroffenen selbst direkt oder indirekt zur Verarbeitung bereitgestellt wurden. Unter direkt bereitgestellte Daten fallen personenbeziehbare Informationen wie Name, Geburtsdatum oder auch Status-Postings auf Social Media Webseiten. Indirekt bereitgestellte Daten sind solche, die durch die Nutzung eines Dienstes von den Betroffenen erzeugt und vom Anbieter beobachtet werden [1].[1] Das Recht auf Datenübertragbarkeit ermöglicht es also, eine Kopie (eines Teils) der gesammelten Daten anzufordern [4]. Eine Löschung oder Sperrung geht mit dem Abruf nicht automatisch einher. Die Datenübertragbarkeit dient, so ist es in Erwägungsgrund 68 DSGVO beschrieben, somit nicht der Datenminimierung, sondern allein dem Erleichtern des Kopierens und Verschiebens von Daten. Das Auskunftsrecht

[1] Eine ausführliche Diskussion über die Abgrenzung und Anwendungsbereiche von Artikel 15 und 20 findet sich in Roßnagel und Geminn (2020) [7].

nach Art. 15 wiederum zielt im Kern auf die Information der Betroffenen, nicht nur über die verarbeiteten Daten, sondern auch über die Zwecke und Wege der Weiterverarbeitung. Das Recht auf Datenübertragbarkeit wird entsprechend in der Leitlinie der Artikel-29-Datenschutzgruppe als Ergänzung des Auskunftsrechts beschrieben.

Für die Datenübertragbarkeit gelten darüber hinaus auch die Anforderungen, die in anderen Artikeln festgelegt sind. Alle Informationen sollen in präziser, transparenter, verständlicher und leicht zugänglicher Form verfügbar gemacht werden. Hierfür soll eine klare und einfache Sprache gewählt werden, um Missverständnissen vorzubeugen (Art. 12 Abs. 1 DSGVO). Während der Datenübertragung muss die Sicherheit der Daten gewährleistet sein und diese müssen vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust sowie unbeabsichtigter Zerstörung oder Schädigung geschützt werden. Zusätzlich ist eine Authentifizierung der betroffenen Person vorgesehen, um zu verhindern, dass Dritte unberechtigt eine Kopie anfordern. Studien haben gezeigt, dass die Verantwortlichen zuletzt Auskunftsanfragen nach Artikel 15 nicht sorgfältig genug prüften und ein Missbrauch möglich ist [6]. Eine Authentifizierung kann gemäß Art. 12 Abs. 6 DSGVO bei begründetem Zweifel an der Identität des Betroffenen auch erfordern, dass zusätzliche Informationen angefragt werden. In Bezug auf die Umsetzung der Datenübertragbarkeit ist kein genaues Ablaufschema vorgegeben. Technische Vorgaben zur Bereitstellung der Daten sind nicht Teil der Verordnung.

Mit der Einführung des neuen Rechts soll die Position der Nutzer:innen gegenüber den Plattformen gestärkt werden. Durch die Möglichkeit, Daten und Profile von einem Anbieter zu einem anderen zu übertragen, sollen Lock-in-Effekte reduziert werden, worunter das Abhängigkeitsverhältnis von Kund:innen von einem Anbieter verstanden wird [10]. Die direkte Weitergabe der Daten soll den Kund:innen die mühselige Wiedereingabe der Daten bei einem Dienstleister-Wechsel, z. B. zwischen zwei Sozialen Netzwerken, erleichtern [4]. De Hert et al. (2018) [3] weisen darauf hin, dass dieses Recht eher ökonomische als datenschutzrechtliche Ziele verfolgt, betonen aber das damit einhergehende Potential für die informationelle Selbstbestimmung.

Das Recht auf Datenübertragbarkeit soll sicherstellen, dass eine Person die sie betreffenden personenbezogenen Daten erhalten und selbstbestimmt weiterverarbeiten oder weitergeben kann [1]. Auch wenn kein festes Format vorgegeben ist, sind die Verantwortlichen dazu aufgefordert, technisch interoperable Systeme zu entwickeln. Das heißt, es sollen gemeinsame Standards und einheitliche Systeme geschaffen werden, um die Weiterverarbeitung und Wiederverwendung von personenbezogenen Daten zu ermöglichen [2]. Für die Datenübertragung werden von

technischen Expert:innen XML, JSON und CSV-Formate empfohlen. Der Vorteil dieser Datenformate ist, dass sie mit Standardsoftware gelesen werden können und somit nicht nur für Verantwortliche, sondern auch für Betroffene einsehbar sind. Das CSV-Format wird hierbei als eine Art Minimallösung angesehen. Es wird empfohlen, eine einfache Beschreibung hinzuzufügen, welche erklärt, wie die Daten strukturiert sind. Bei umfangreichen Daten wird geraten, XML oder JSON einzusetzen, da diese sowohl Inhaltsdaten als auch beschreibende Metadaten enthalten. Außerdem reicht deren Leistungsumfang für die Abbildung von komplexen Datenstrukturen aus. Um eine effektive Weiterverwendung zu gewährleisten, sollte das Datenformat PDF nicht zum Einsatz kommen [4].

Zuletzt sieht Art. 20 DSGVO vor, dass Verantwortliche innerhalb der Frist eines Monats einer Anfrage auf Datenübertragbarkeit nachkommen. Sollten Verzögerungen auftreten, sind diese der betroffenen Person mit einer entsprechenden Begründung zu melden. Die Frist kann in solchen Fällen um bis zu zwei weitere Monate verlängert werden. Sollte der Verantwortliche eine Umsetzung verweigern, muss er dies ebenfalls begründen.

2 Problemstellung

Die Herausforderungen des Rechts auf Datenübertragbarkeit liegen in der technischen wie organisatorischen Umsetzung der gesetzlichen Pflicht in die unternehmerische Praxis. Vier Jahre nach dem Inkrafttreten der DSGVO und zwei Jahre nach deren Anwendbarkeit ist unklar, inwieweit Verantwortliche ihrer Pflicht bereits nachkommen und Prozesse etabliert haben, um auf Anfragen zur Datenübertragung zu antworten. Wenig untersucht ist zudem, ob und wie viele Betroffene bereits von ihrem Recht Gebrauch machen und inwiefern die gesetzten Ziele der besseren Kontrolle und Reduzierung von Lock-in-Effekten erreicht werden können.

Die Vorgabe, dass die zu übermittelnden Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden müssen, setzt keine einheitliche Umsetzung voraus. Aus Sicht der Betroffenen ist klar, dass komplexere Datenformate eine Herausforderung darstellen. Für Unternehmen steht dagegen im Vordergrund, dass der Import und Export von Daten möglichst kompatibel zur intern genutzten Softwarelösung ist.

Aus Sicht der bereitstellenden Unternehmen stellt sich die Frage wie Daten exportiert werden können, ohne bei einer Offenlegung die Rechte und Freiheiten anderer Personen zu beeinträchtigen. Die Verantwortlichen haben die Pflicht, ausschließlich Daten der Betroffenen sowohl bei einer einfachen Auskunft als auch

bei der Weitergabe an andere Verantwortliche zu übertragen. In der Praxis sind allerdings häufig in einem Datensatz Bezüge zu mehreren Personen enthalten. Beispielsweise ist es bei einer Datenübertragung von einem Bankkonto unvermeidlich, dass die Transaktionen sowohl Informationen über die Kontoinhaber als auch über die Transaktionspartner enthält. Während in diesem Fall die Rechte und Freiheiten der anderen Personen nicht wesentlich beeinträchtigt werden, ist die Abwägung bei komplexeren und umfangreicheren Daten, wie etwa in Social Networks, schwieriger. In die Entscheidung muss auch einfließen, wie der neue Verantwortliche diese Daten nutzt: Eine Zweckänderung ist nicht möglich [1].

Offen ist auch der Umfang der zu übertragenden Daten. Beispielsweise können interne und ohne weiteres nicht nachvollziehbare Kennungen und andere für die Betroffenen unverständliche Angaben vorhanden sein, die von den Verantwortlichen offenbart werden. Urban et al. (2019) [8] haben gezeigt, dass im Fall von Online Tracking unnötige und teilweise falsch gekennzeichnete Daten an die Betroffenen weitergegeben wurden. Somit stellt sich die Frage, welche Daten die Kund:innen als personenbezogen einstufen und welche sie als überflüssig empfinden [4].

3 Empirische Untersuchungen

Um einen Einblick in den Umgang mit und die Umsetzung des Gesetzes zu erhalten, wurde eine Studie mit Betroffenen sowie mit Expert:innen in Unternehmen durchgeführt.

3.1 Unternehmensperspektive

Die Perspektive der Unternehmen auf das Ab- und Annehmen von Daten wurde mit Hilfe von Expert:inneninterviews untersucht. Das Ziel dieser Befragung war es zu erheben, inwieweit die Datenübertragbarkeit nach Art. 20 DSGVO in Unternehmen praktisch umgesetzt wird. Dabei wurden die Vorgehensweise, die Relevanz und das Ziel der Datenportabilität überprüft. Bei der Befragung lag der Fokus auf Unternehmen, die eine Vielzahl personenbezogener Daten von Kund:innen verarbeiten.

Insgesamt wurden 102 Unternehmen per E-Mail angeschrieben und um eine Interviewteilnahme gebeten. Die E-Mail-Adressen der Kontaktpersonen wurden den jeweiligen Datenschutzerklärungen entnommen. Es erklärten sich schließlich zwölf Unternehmensvertreter:innen für ein Interview bereit. Die Unternehmen, bei

denen diese beschäftigt sind, gehören zu unterschiedlichen Branchen und variieren in ihrer Größe. Von den zwölf interviewten Unternehmen befinden sich elf in Deutschland und eines in Österreich: Fünf haben die Größe eines Konzerns, drei sind Großunternehmen. Hinzu kommen ein mittelständisches Unternehmen, ein Kleinunternehmen, ein Verkehrsverbund und eine Krankenkasse. Alle Interviewpartner:innen sind Datenschutzbeauftragte im jeweiligen Unternehmen und damit für die Einhaltung der datenschutzrechtlichen Vorschriften zuständig.

Die Interviews wurden telefonisch durchgeführt und die Dauer der Gespräche betrug durchschnittlich 22 min. Alle Interviews wurden zwischen dem 05.04. und dem 17.05. des Jahres 2019 durchgeführt. Auf Wunsch wurden die Namen der interviewten Unternehmen anonymisiert (vgl. Tab. 1 im Anhang).

Die Interviewfragen wurden vorher in einem Interviewleitfaden festgelegt, der die Vergleichbarkeit der Interviewergebnisse gewährleistet. Der Leitfaden orientierte sich an den übergeordneten Fragen: Wie wird die Datenübertragbarkeit in der Praxis umgesetzt? Besteht ein Bedarf der Betroffenen für dieses Recht? Wie kann man die bereitgestellten Daten wiederverwenden? Welches Format wird eingesetzt, um die Anforderungen eines strukturierten, gängigen und maschinenlesbaren Formats zu erfüllen? Können durch die Datenübertragbarkeit Betriebsgeheimnisse preisgegeben werden?

3.1.1 Ergebnisse der Unternehmensbefragung

Zu Beginn des Interviews wurden die Datenschutzbeauftragen gefragt, inwieweit die Datenübertragbarkeit von den Unternehmen umgesetzt wird. Von den zwölf Befragten gaben zwei an, Anfragen auf Datenübertragbarkeit nicht zu beantworten. Es handelte sich dabei einmal um einen großen Zeitungsverlag, der dies damit begründete, dass personenbezogene Daten immer im Zusammenhang mit einem Abonnement stünden und damit ein Vertrag als Rechtsgrundlage vorläge. Dies steht allerdings im Widerspruch zu Art. 20 Abs. 1 lit. a DSGVO, der Verarbeitung auf Basis von Verträgen explizit nennt. So fand die Datenübertragbarkeit bei der Krankenversicherung ebenfalls keine Anwendung, da dort personenbezogene Daten nicht auf Basis der Einwilligung der Betroffenen verarbeitet werden und Datenübertragbarkeit nicht auf Verarbeitungen anzuwenden ist, die im öffentlichen Interesse liegen (Art. 20 Abs. 3 DSGVO). Die genannten Unternehmen wurden daher bei der weiteren Auswertung der Interviews nicht betrachtet.

Den übrigen zehn Interviewpartner:innen wurde die Frage gestellt, wie viele Anfragen auf Datenportabilität sie bisher erhalten hatten. Acht Unternehmen erhielten bisher keine Anfragen. Fünf der Befragten rechneten auch in Zukunft nicht mit Anfragen, zwei hielten es für unwahrscheinlich. Nur der Datenschutzbeauftragte des Verkehrsverbundes ging davon aus, dass Anfragen eingehen werden.

Vier Interviewpartner:innen begründeten ihre Erwartung damit, dass das Recht auf Datenübertragbarkeit sehr eingeschränkt sei, da es nur die Daten umfasse, die Betroffene selbst zur Verfügung gestellt haben. Bei einer Portierung der Daten wären nach Ansicht der Befragten nur wesentliche Kontaktangaben und Vertragsangaben von der Übertragbarkeit betroffen. Zwei Interviewte waren der Meinung, dass der Aufwand der Datenübertragung größer sei als die erneute Eingabe der Daten durch die Betroffenen bei einem neuen Anbieter. Zwei weitere Interviewpartner:innen berichteten, dass sie Kontakt zu anderen Datenschutzbeauftragten in ähnlichen Bereichen hätten und auch dort die Anzahl der Anfragen niedrig sei. Eine der Interviewten erwähnte, als Datenschutzbeauftragte in mehreren Unternehmen tätig zu sein und dass auch bei diesen das Recht noch nicht geltend gemacht worden sei.

Nur zwei der Interviewten gaben an, bereits Anfragen im einstelligen Bereich erhalten zu haben. Dabei handele es sich um Anfragen, bei denen die Betroffenen die Daten als Kopie erhalten wollten. Fälle von tatsächlichen Datenübertragungen zu einem anderen Verantwortlichen gab es bisher bei keinem der interviewten Unternehmen.

Bezüglich der Umsetzung gaben sieben Unternehmen an, die Daten gegebenenfalls manuell bereit zu stellen. Das bedeutet, dass die personenbezogenen Daten im Falle einer Anfrage durch einen Datenbankexport erzeugt würden. Der aus der Datenbank exportierte Auszug werde der betroffenen Person anschließend durch eine verschlüsselte Mail bzw. auf einer CD oder einem USB-Stick übermittelt.

Die strukturierteste Umsetzung beschrieb der Interviewte eines Softwareunternehmens, das für die Umsetzung die eigene Software zum Personalmanagement einsetzt, die im selben Unternehmen entwickelt und vermarktet wird. Teil der Software sei ein Auswertungstool, mit dem ein Bericht erstellt werden könne. Eine dieser Berichtsarten sei die Auswertung mit dem Fokus auf Datenportabilität. Dabei könne festgelegt werden, in welchem Format die Daten zur Verfügung gestellt werden sollen, bevor sie aus der Datenbank exportiert würden.

Der Datenschutzbeauftragte eines Logistikunternehmens erklärte, dass ein Tool für die Personalverwaltung bei einem Drittanbieter verwendet werde und auf Wunsch eine komplette Personalakte generiert werden könne. Bei den Kund:innen setze das Unternehmen die Datenportabilität manuell um. Den Nutzer:innen wird zudem ein Portal bereitgestellt, das verschiedene Betroffenenrechte bündelt, sodass die eigenen Daten kontrolliert, korrigiert oder gelöscht werden können. Auch bei einem interviewten Kreditinstitut können personenbezogene Daten im Onlinebanking-Portal von Betroffenen selbst bearbeitet werden und Daueraufträge sowie Überweisungen heruntergeladen werden. Bei einem Fitness-App-Hersteller

haben Nutzer:innen über die Webseite jederzeit die Möglichkeit, eine Kopie ihrer Daten herunterzuladen – dabei wird zwischen einer Kopie nach Art. 15 Abs. 3 DSGVO und Art. 20 DSGVO nicht unterschieden. Nach Bestätigung der E-Mail-Adresse können die eigenen Daten über einen bereitgestellten Link als ZIP-Datei heruntergeladen werden.

Die unmittelbare Übertragung der Daten zu einem anderen Verantwortlichen ist in keinem der befragten Unternehmen automatisiert möglich. Der Interviewpartner eines Kreditinstituts erklärte, dass Daten anderer Unternehmen aus technischen Gründen nicht importiert werden könnten. Zwei Interviewpartner:innen gaben an, dass die Ausgabe der Daten keine Probleme darstelle, jedoch die Übernahme der Daten von anderen Anbietern fast unmöglich sei. Sie waren der Meinung, dass alle Unternehmen unterschiedliche Daten speichern und somit unterschiedliche Systeme verwendet würden, sodass die Datenformate eine Barriere darstellten. Ein Import sei sehr aufwändig, da die Daten zuerst zeitintensiv bearbeitet werden müssten. Der Interviewpartner beim Fitness-App-Hersteller sprach sich daher für gesetzliche Vorgaben bezüglich des Formats aus.

Bei der Übertragung der personenbezogenen Daten kommen bei den untersuchten Unternehmen ausschließlich die Formate PDF, CSV, XML und JSON zum Einsatz. Zwei Unternehmen stellen die personenbezogenen Daten als PDF-Datei zur Verfügung. Drei Interviewpartner:innen gaben an, die Daten in mehreren Formaten zur Verfügung stellen zu können. Möglich seien PDF, CSV oder XML. Der Datenschutzbeauftragte des Kreditinstituts teilte mit, dass die Daten, die dokumentenhaft verfügbar seien, als PDF-Datei und listenartige Daten als CSV-Datei aus der Datenbank exportiert würden. Der Datenschutzbeauftragte der Fitnessstudio-Kette gab an, dass die Daten in XML-Format übermittelt würden. Zwei weitere teilten mit, dass die Übertragung als JSON-Datei stattfände.

3.1.2 Ergebnisse

Die Expert:inneninterviews haben gezeigt, dass noch viele Unsicherheiten und technische Schwierigkeiten bei der Umsetzung des Art. 20 DSGVO vorhanden sind. Es wird versucht, durch individuelle Lösungsansätze der Pflicht nachzukommen. Konkret konnten wir folgende Probleme feststellen:

- *Die überwiegende Mehrheit der Unternehmen exportiert Daten manuell:* Der Export der Daten erfolgt in sieben der Unternehmen manuell. Bei zwei Unternehmen wird ein Tool zum Exportieren der personenbezogenen Daten genutzt. In einem Unternehmen wird nur für die Mitarbeitenden ein Tool zur Umsetzung verwendet, für die Kund:innen hingegen erfolgt die Zusammenstellung

der Daten manuell. Nur eines der befragten Unternehmen stellt ein Download-Tool für Betroffene zur Verfügung, mit dem personenbezogene Daten jederzeit selbst angefordert und heruntergeladen werden können.

- *Keines der interviewten Unternehmen stellt eine automatisierte Lösung für die Datenübermittlung zu einem anderen Verantwortlichen zur Verfügung:* Die Übermittlung der Daten zu einem anderen Verantwortlichen ist in jedem der interviewten Unternehmen nur über Datenträger oder eine E-Mail möglich.
- *Eine Wiederverwendung der bereitgestellten Daten ist aus Betroffenenperspektive nicht möglich:* Verbraucher:innen können zwar ihre bereitgestellten Daten erhalten, jedoch ist durch die fehlenden interoperablen Systeme die effektive Wiederverwendung dieser Daten nicht möglich.
- *Die interviewten Unternehmen verwenden bei der Übermittlung der Daten unterschiedliche Formate:* Die Formate variieren zwischen den Unternehmen, was den Import der Daten zu einem anderen Verantwortlichen erschwert.
- *Von der Datenübertragbarkeit wird so gut wie nie Gebrauch gemacht:* In den Interviews konnten wir feststellen, dass es von zehn der Unternehmen nur in zwei Unternehmen einzelne Anfragen innerhalb eines Jahres gegeben hat. Dabei wird auch zukünftig keine Steigerung von Anfragen erwartet.

3.2 Betroffenenperspektive

In einer zweiten Studie lag der Fokus auf den Erwartungen und Perspektiven der Betroffenen in Bezug auf den Export und die Weitergabe ihrer personenbezogenen Daten. Die Analyse gibt daher keinen Aufschluss über die Korrektheit des Verfahrens entsprechend der juristischen Vorgaben, sondern gibt Hinweise auf das Verständnis und die Erwartung von Laien. Dazu wurden zuerst Leitfadeninterviews durchgeführt, im Anschluss Anfragen an verschiedene Unternehmen gestellt und die beauskunfteten Daten diskutiert.

Insgesamt wurden 14 Interviews durchgeführt. Bei der Auswahl der Befragten wurde darauf geachtet, Personen unterschiedlicher Altersgruppen und Lebensumstände zu befragen. Bei den ausgewählten Befragten handelte es sich um neun weibliche und fünf männliche Personen zwischen 19 und 44 Jahren mit unterschiedlichen Bildungsabschlüssen und beruflichen Tätigkeiten.

Vorab wurde das Vorwissen der Interviewten erhoben. Im Anschluss erhielten die Teilnehmer:innen die Aufgabe, bei häufig genutzten Dienstleistern eine Anfrage auf Datenportabilität nach Art. 20 DSGVO zu stellen. Dazu wurde ein Ablaufprotokoll erstellt, das schrittweise erklärte, wie eine solche Anfrage zu stellen ist. Nach Erhalt der Daten wurden die Teilnehmer:innen aufgefordert, im

Rahmen von Thinking-Aloud-Protokollen die Daten und Formate zu bewerten. Thinking-Aloud-Protokolle dienen zur Erfassung von bewussten handlungsbegleitenden Kognitionen [5]. Insgesamt wurden 33 Anfragen begleitet, die an 17 unterschiedliche Dienstleister gestellt wurden. Die Unternehmen wurden über eine separate Vorstudie ausgewählt. Hierbei sollten die 14 Teilnehmer:innen angeben, welche Dienste sie in Anspruch nehmen. Zur Vereinfachung wurden die am häufigsten genutzten Dienste als Antwortmöglichkeit angegeben. Hieraus ergaben sich folgende Kategorien: Bargeldloser Zahlungsverkehr, Musik- bzw. Video-Streamingdienste, Soziale Medien, Online-Kommunikationsmethoden, Onlinehandel, E-Mail-Provider, Fitnessstudios und Filehosting-Dienste. Darunter sind bekannte Unternehmen wie Sparkasse, YouTube, WhatsApp, McFit und Google Mail.

3.2.1 Datenauswertung Vorab-Interviews

Die Befragung der Datenschutzbeauftragen in Abschn. 3.1 hat bereits gezeigt, dass Betroffene das Recht auf Datenübertragbarkeit so gut wie nicht Anspruch nehmen. Den Teilnehmer:innen wurde deshalb die Frage gestellt, ob ihnen das Recht bereits bekannt sei. Die meisten Teilnehmer:innen verneinten diese Frage. Nur eine:r der Teilnehmer:innen hat bisher eine Anfrage aus Neugier gestellt. Bei der Befragung wurde schnell klar, dass die Teilnehmenden – die keine juristischen Vorkenntnisse hatten – nicht zwischen Auskunftsanfragen nach Art. 15 DSGVO und Anfragen zur Datenübertragung nach Art. 20 DSGVO unterscheiden.

Die im Rahmen der Anfrage bereitgestellten Daten müssen nach Art. 20 DSGVO nur solche Informationen enthalten, die aktiv und wissentlich von der Person bereitgestellt und solche, die von dem Verantwortlichen beobachtet wurden. Den Teilnehmer:innen unserer Studie wurde deshalb die Frage gestellt, welche Daten und Informationen über ihre Person sie als personenbezogen einstufen würden. Aus Sicht der Betroffenen fallen unter personenbezogene Daten fast ausschließlich solche, die aktiv und wissentlich bereitgestellt wurden. Nur vier Teilnehmer:innen zählten auch beobachtete Daten dazu und erwarteten diese in der Antwort.

Danach wurden die Teilnehmer:innen darüber befragt, was sie unter einem „strukturierten, gängigen und maschinenlesbaren“ Format verstehen. Die eher breite Definition im Recht über das Dateiformat wurde von den Interviewten überwiegend so interpretiert, dass es ein Format ist, das auf allen Endgeräten genutzt werden kann. Bezüglich der individuellen Präferenz gaben 93 % der Befragten an, das PDF-Format zu bevorzugen. Auch wurde den Teilnehmenden die Frage

gestellt, welche Assoziationen sie mit Datenportabilität verbinden. Die Antworten waren dabei sehr positiv und wurden mit den Begriffen „nützlich“, „hilfreich“, „zeitgemäß“ und „wichtig“ beschrieben.

Ein Ziel des Rechts auf Datenübertragbarkeit ist es, den Lock-in-Effekt zu verringern und Nutzer:innen den Wechsel zwischen Dienstanbietern zu erleichtern. Aus diesem Grund wurden die Teilnehmenden gefragt, ob sie in der Vergangenheit bereits einen Dienstwechsel angestrebt, diesen jedoch aufgrund des hohen Aufwandes nicht unternommen haben. Die Mehrheit der Befragten bestätigte diese Erfahrung des Lock-in-Effekts, gaben aber an, dass sie nicht davon überzeugt seien, dass die Datenübertragbarkeit hier Abhilfe schaffen könne.

Grundsätzlich zu ihren Erwartungen befragt, erklärten die Teilnehmenden, dass sie sich durch die Anfrage einen besseren Überblick über die eigenen Daten erhofften und gegebenenfalls einen erleichterten Anbieterwechsel durchführen könnten. Ersteres Ziel entspricht dabei eher einem Auskunftsersuchen nach Art. 15 DSGVO.

3.2.2 Auswertung der Anfragen

Zusätzlich zur Befragung über die Erwartungen wurden die Teilnehmer:innen aufgefordert, Daten anzufordern. Vierzehn Teilnehmende haben dazu Anfragen an bis zu drei Unternehmen gestellt, insgesamt waren es 33 Anfragen. Bei zehn Dienstleistern war die Kontaktaufnahme auf Deutsch möglich, bei sieben wurden die entsprechenden Formulare nur auf Englisch bereitgestellt, was für einige Teilnehmende eine Hürde darstellte.

Wie bereits aus der Befragung der Unternehmen bekannt, übermittelten die Verantwortlichen die Daten in einer Vielzahl von Formaten. Einige Dienstleister wie Snapchat, YouTube, H&M oder WhatsApp stellten die Daten in jeweils zwei unterschiedlichen Datenformaten bereit. Das am häufigsten eingesetzte Format war das Format JSON. Acht von vierzehn Teilnehmer:innen konnten mit diesem Datenformat nicht umgehen. Weitere acht Teilnehmer:innen erhielten ihre Daten (zusätzlich) im HTML-Format, welches sich im Browser öffnen ließ und damit leichter zugänglich war. Der Einsatz von PDF und passwortgeschützten PDFs wurde von den Teilnehmer:innen positiv aufgenommen. Drei Verantwortliche (zwei Fitnessstudioketten und ein Kreditinstitut) sendeten die Daten postalisch auf Papier, wobei nur eines der Unternehmen zusätzlich eine Online-Version anbot. Eine Bekleidungskette setzte auf das XML-Format, womit die zwei Teilnehmenden, die die Daten angefragt hatten, große Schwierigkeiten hatten. Unsere Daten bestätigen die Ergebnisse einer Studie von Wong und Henderson (2018) [9], die bei Anfragen an 230 Unternehmen eine ähnliche Vielfalt an Dateiformaten und Zustellwegen festgestellt haben. Bei 20 Protokollen gaben die Teilnehmer:innen

an, dass die Gliederung der Daten angemessen war und das Verständnis gefördert hat. Die Sortierung von Daten mit Hilfe von Ordnern erleichterte ebenfalls das Verständnis. Unnötige Verschachtelung von Daten in eine Vielzahl von Ordnern wurde jedoch als nicht hilfreich für das Verständnis empfunden.

Der Datenumfang der personenbezogenen Daten variierte je nach Unternehmen. Die Menge der Daten wurde bei 17 Protokollen als angemessen empfunden. Sie erfüllte also die Erwartungen, die im Vorabinterview geäußert wurden. Bei den von YouTube bereitgestellten Daten wurde die Möglichkeit, die Daten vorab zu selektieren, als positiv beurteilt. Bei zehn Auskünften waren die Teilnehmer:innen der Meinung, dass die Daten zu umfangreich seien. Dies lag unter anderem daran, dass Dienstleister wie Snapchat, Amazon und Twitter leere Ordner oder einzelne Daten wie Emojis einfügten oder Dateien aufgezeigt wurden, die Tags und Informationen von anderen Personen enthielten und daher nicht vollständig integriert werden konnten.

Insgesamt zeigte sich, dass die Teilnehmer:innen bei der Mehrzahl der Protokolle den Inhalt der Daten verstanden haben. Dies wurde hauptsächlich durch die Benennung der Daten und Ordner unterstützt. Die meisten der bereitgestellten Daten boten nach Selbsteinschätzung einen Mehrwert für die Betroffenen, in fünfzehn Protokollen wurde dies konkret benannt. YouTube ermöglichte seinen Nutzer:innen nach Erhalt der Daten, diese zu löschen oder die weitere Speicherung zu pausieren und vereint somit verschiedene Betroffenenrechte in einer Funktion. Die Teilnehmer:innen, die Daten bei Fitnessstudios, Kundenbindungsprogrammen oder Finanzdienstleistern (insgesamt vier Unternehmen) angefragt hatten, konnten mit Hilfe dieser Daten ihr vergangenes Verhalten nachvollziehen. Zu sechs weiteren Anfragen wurde der Mehrwert als neutral eingestuft. Dies betraf solche Daten, bei denen die Dateien nicht verstanden wurden oder die Betroffenen nur ihre eigenen Daten (Bilder, Videos, Dokumente) erhielten, wie etwa bei Instagram oder Google Drive.

Nachdem die Teilnehmer:innen einen Einblick in ihre personenbezogenen Daten erhielten, wurden sie gefragt, ob sie einen Anbieterwechsel mit Hilfe des Rechts ausführen würden. Achtzehn Teilnehmer:innen entschieden sich gegen einen Anbieterwechsel. Ihre Entscheidung begründeten sie überwiegend damit, dass zu viele Daten über sie weitergegeben würden.

3.2.3 Ergebnisse

Die Befragung der Nutzer:innen hat ergeben, dass die Mehrheit das Recht auf Datenübertragbarkeit nicht kennt. Nur ein Teilnehmer hat bisher eine Anfrage gestellt. Zusammenfassend können wir die folgenden Ergebnisse und Empfehlungen festhalten:

- *Die Betroffenen sehen einen Mehrwert in dem Recht auf Datenübertragbarkeit, vermischen die Ziele aber mit dem Auskunftsrecht:* Aus Sicht der Betroffenen ist der Zweck des Rechts, einen erleichterten Anbieterwechsel durchzuführen und gleichzeitig einen besseren Überblick über die eigenen Daten zu erhalten. Die Erwartung schließt also die Ziele des Rechts auf Auskunft mit ein.
- *Nur eine Minderheit der Befragten erwartet, dass beobachtete Daten mit übertragen werden:* Die große Mehrheit erwartet als Antwort auf eine Anfrage nach Datenübertragbarkeit nur die von ihnen selbst bereitgestellten Informationen. Die erweiterten Informationen, die etwa Teil einer Antwort auf eine Auskunftsanfrage wären, vermissen die Befragten nicht. Der bereitgestellte Datenumfang wird von der Mehrheit als angemessen empfunden.
- *Rund 93 % der Befragten bevorzugen das PDF-Format. Nur vier der 14 Teilnehmer konnten Daten im JSON-Format nachvollziehen:* Bezüglich des Formats wünschen sich die Betroffenen vor allem, dass es auf allen Endgeräten genutzt werden kann. Dieser Wunsch zeigt, dass Erwartungen an die Datenübertragbarkeit unabhängig von der juristischen Grundlage der gestellten Anfrage sind und generell auf Transparenz und Nachvollziehbarkeit abzielen. Das PDF-Format wird bevorzugt, da es weit verbreitet ist. Mit technischen Formaten wie JSON können die Betroffenen häufig wenig anfangen. Anbieter, die ein PDF zur Übersicht und eine technischeres Format für die Übertragung anbieten, unterstützen das Verständnis bei den Betroffenen. Um den Anforderungen der Datenportabilität gerecht zu werden, sollten weitere Formate zusätzlich bereitgestellt werden.
- *Drei Anfragen wurden nur postalisch beantwortet:* Drei Dienstleister stellten die Daten der Betroffenen auf Papier zur Verfügung, was eine Weiternutzung deutlich erschwert, sodass diese Verantwortlichen einer wesentlichen Vorgabe von Art. 20 nicht nachkommen.
- *Die Hälfte der Verantwortlichen bieten ein eigenes Download-Tool an:* In diesen Tools findet die Authentifizierung durch einen Login statt. Für die übrigen Anbieter erfolgt die Authentifizierung auf Anfrage der Verantwortlichen. Zur Authentifizierung werden Kundennummer, Anschrift und Geburtsdatum abgeglichen oder eine Kopie des Personalausweises oder der Mitgliedskarte angefordert. Die Daten werden entweder auf Deutsch oder Englisch bereitgestellt.
- *Vorabauswahl zur Bestimmung der Datenmenge erleichtert die Nutzung:* Die Kontrolle über die eigenen Daten und die Möglichkeit, die eigenen beobachteten Daten anzuzeigen, bietet Benutzer:innen einen Mehrwert. Wenn die bereitgestellten Daten jedoch verwirrend oder redundant sind, sehen die Befragten keinen Nutzen.

- *Transparenz über die vorhandenen Daten verringert den Wunsch, die Daten zu übertragen:* Auf einen Anbieterwechsel verzichten die meisten Teilnehmenden. Interessanterweise hat die Einsicht in die Daten bei den Nutzer:innen zu einer Reflexion über den Umfang der Datenmenge geführt, sodass sie von einer Übertragung aller Daten an einen anderen Anbieter Abstand genommen haben.

4 Zusammenfassung

Im Rahmen unserer Studien wurden sowohl die Umsetzungsstrategien als auch die Tauglichkeit der Datenübertragbarkeit nach Art. 20 DSGVO untersucht. Die Studien waren überwiegend qualitativ und explorativ angelegt. Die Auswahl der Teilnehmenden und der befragten Unternehmen ist nicht repräsentativ, die Ergebnisse sind aber dennoch verallgemeinerbar, insofern viele Erkenntnisse auch auf andere Fälle anwendbar scheinen.

In der Expert:innenbefragung konnten wir feststellen, dass die überwiegende Mehrheit der interviewten Unternehmen bisher keine Anfragen auf Datenportabilität erhielten. Diese Aussage wurde durch die Interviews mit Nutzer:innen bestätigt. Die Betroffenen kannten das Recht nicht und haben es daher noch nie genutzt. Beide Befragungen haben außerdem gezeigt, dass das ursprüngliche Ziel, Lock-in Effekte zu verringern und einen Anbieterwechsel zu erleichtern, bisher weder ein Bedürfnis der Nutzer:innen ist, noch umsetzbar wäre, da die Unternehmen keine entsprechenden Schnittstellen zur Verfügung stellen. Durch die geringe Zahl der Anfragen entsteht keine praktische Notwendigkeit, gemeinsame Standards zu erarbeiten. In den befragten Unternehmen werden in den seltenen Fällen einer Anfrage die Daten manuell zusammengetragen bzw. aus Datenbanken exportiert. Durch die Vielfalt der Datenformate wird die Wiederverwendung und Weiterverarbeitung der bereitgestellten Daten erschwert.

Unsere Studie mit Nutzer:innen zeigt zudem die Skepsis der Betroffenen gegenüber einer direkten Übertragung. Zwar ist es das eigentliche Ziel von Art. 20 DSGVO einen direkten Anbieterwechsel auch ohne Einsicht der Betroffenen zu ermöglichen, in der Praxis bevorzugen die Teilnehmenden aber, die Daten vorab in einem angemessenen Format zu erhalten, um einschätzen zu können, welche Daten weitergegeben werden.

Hier entsteht ein Zielkonflikt zwischen Transparenz für die Betroffenen (ähnlich des Auskunftsrechts) und Nützlichkeit des Datenformates für die (empfangenden) Verantwortlichen. Es scheint daher sinnvoll, beide Rechte als eines

zu behandeln und auf Anfragen von Betroffenen mit einer erklärenden Zusammenfassung im Sinne des Auskunftsrechts zu antworten sowie zusätzlich den Datenexport mit Konfigurationsmöglichkeiten für den Umfang und das Format des Exports anzubieten.

Anhang

Tab. 1 Liste der Interviewpartner, sowie Zeitpunkt und Dauer der Interviews

Unternehmen	Datum	Dauer
Kleines Werbeunternehmen	05.04.2019	32 min
Großes global agierendes Logistikunternehmen	08.04.2019	36 min
Große Fitnessstudio-Kette	10.04.2019	26 min
Krankenkasse	12.04.2019	12 min
Großes Handelsunternehmen	17.04.2019	17 min
Großer Zeitungsverlag	17.04.2019	5 min
Mittelständisches Software-Unternehmen	17.04.2019	16 min
Großes Kreditinstitut	23.04.2019	28 min
Großer Postdienstleister	30.04.2019	17 min
Verkehrsverbund	02.05.2019	17 min
Große Hilfsorganisation	08.04.2019	27 min
Großer Fitness-App Hersteller	17.05.2019	27 min

Literatur

1. Artikel 29-Datenschutzgruppe: Leitlinien zum Recht auf Datenübertragbarkeit. Brüssel, 13.12.2016. https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2017/07/WP242de_Art_29-Gruppe_Datenubertragbarkeit.pdf (2016). Zugegriffen: 20. Dez. 2020
2. Brandner, R., Dörge, O., Isele, C., Kaufmann, P., Oemig, F., Schütze, B., Spyra, G., Stahmann, A.: Hinweise/Stellungnahme zum „Recht auf Datenübertragbarkeit“ gemäß Art. 20 DS-GVO. Köln, 04.12.2016. https://ds-gvo.gesundheitsdatenschutz.org/download/recht_datenuebertragbarkeit.pdf (2016). Zugegriffen: 20. Dez. 2020
3. De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., Sanchez, I.: The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services. Comput. Law Secur. Rev. **34**(2), 193–203 (2018) https://doi.org/10.1016/j.clsr.2017.10.003

4. Horn, N., Riechert, A.: Praktische Umsetzung des Rechts auf Datenübertragbarkeit. Stiftung Datenschutz, Leipzig, 04.10.2017. https://stiftung-datenschutz.org/fileadmin/Redaktion/Datenportabilitaet/studie-datenportabilitaet.pdf (2017). Zugegriffen: 20. Dez. 2020
5. Konrad, K.: "Lautes Denken." In: Handbuch Qualitative Forschung in der Psychologie: Bd. 2: Designs und Verfahren, S. 373–393. Springer Fachmedien, Wiesbaden (2020) https://doi.org/10.1007/978-3-658-26887-9_41.
6. Martino, M.D., Robyns, P., Weyts, W., Quax, P., Lamotte, W., Andries, K.: "Personal Information Leakage by Abusing the GDPR 'Right of Access.'" In: Symposium on Usable Privacy and Security 2019. https://www.usenix.org/conference/soups2019/presentation/dimartino (2019). Zugegriffen: 20. Dez. 2020
7. Roßnagel, A., Geminn, C.: Datenschutz-Grundverordnung verbessern: Änderungsvorschläge aus Verbrauchersicht. Nomos Verlagsgesellschaft mbH & Co. KG. (2020). https://doi.org/10.5771/9783748920991
8. Urban, T., Degeling, M., Holz, T., Pohlmann, N.: 'Your Hashed IP Address: Ubuntu.' – Perspectives on Transparency Tools for Online Advertising. In: Proceedings ACSAC 2019 (2019). https://doi.org/10.1145/3359789.3359798
9. Wong, J., Henderson, T.: How Portable Is Portable?: Exercising the GDPR's Right to Data Portability. In: Proceedings UbiComp 2018 (2018). https://doi.org/10.1145/3267305.3274152.
10. Zanfir, G.: The Right to Data Portability in the Context of the EU Data Protection Reform. International Data Privacy Law **2**(3), 149–162 (2012). https://doi.org/10.1093/idpl/ips009

Datenschutz durch Technikgestaltung

Digitale Selbstermächtigung. Hürden für Privatheit und Autonomie in einer algorithmisch konstruierten Wirklichkeit

Peter Biniok

Zusammenfassung

Digitalisierung und algorithmische Konstruktion der Gesellschaft orientieren sich (derzeit) einseitig vor allem an techno-ökonomischen und machtpolitischen Kriterien. Algorithmisierung und damit verbundene digitale Dynamiken verändern grundsätzliche Handlungs- und Strukturmuster, womit sich Fragen nach Privatheit und Autonomie der Nutzer:innen im Umgang mit Technik neu stellen. Im Beitrag werden Herausforderungen und Chancen digitaler Selbstermächtigung anhand von drei Dimensionen algorithmischer Konstruktion diskutiert: Algorithmen als Besitztümer, Algorithmen als Akteure und Algorithmen als Kontrollmittel. Sozial konstruierte Algorithmen agieren autonom, interagieren mit Nutzer:innen, sortieren und filtern für sie die Wirklichkeit, übernehmen gesellschaftliche Kontrollfunktionen. Selbstermächtigung im Bereich des Digitalen steht diesbezüglich nicht nur für eine Form der praktischen Befähigung, sondern schließt auch Reflexion und Bewertung des eigenen Handelns ein. Selbstermächtigung ist gleichzeitig an fremde Unterstützung gekoppelt und konstituiert sich in einem kollektiven Prozess.

Schlüsselwörter

Algorithmisierung • Souveränität • Digitale Bildung

P. Biniok (✉)
Kompetenzzentrum Innung SHK Berlin, Berlin, Deutschland
E-Mail: peter.biniok@freenet.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_17

1 Einleitung: Soziale Ordnung und Digitalisierung

Gesellschaft befindet sich in einem kontinuierlichen Wandlungsprozess, Technisierung und Digitalisierung eingeschlossen. Die fortwährende Dynamik zieht immer neue Ordnungsleistungen nach sich, damit gesellschaftliches Leben stabil bleibt.

1.1 Gesellschaftliche und technische Konstruktion der Wirklichkeit

Wie Gesellschaft möglich ist und *soziale Ordnung* entsteht und aufrechterhalten bleibt, durch wen und welche Mechanismen also welche Ordnungsleistungen auf welche Weise erbracht werden, wird in der Soziologie vielfältig diskutiert. In diesem Beitrag wird die Prämisse zugrunde gelegt, dass in erster Linie Individuen selbst die soziale Ordnung herstellen und gesellschaftliche Wirklichkeit konstruieren [1, 2]. Durch Interaktion und Kommunikation, d. h. vielfältige Kooperationen, Koordinationsaktivitäten, Aushandlungen usw. bringen Individuen in einem kollektiven Prozess die Gesellschaft in Form von Normen, Prozeduren und Organisationen hervor, die den Individuen als objektive Strukturen und Tatsachen gegenüberstehen und handlungsleitend wirken. Gesellschaft ist so gesehen eine Art *Handlungsstrom,* aus dem spezifische Handlungen in überdauernde Strukturen sedimentieren, die sich weniger langsam verändern als andere. Gemeinsam geteilte und für legitim erachtete Handlungsabläufe, Denkmuster und Wertvorstellungen werden zu Institutionen und bilden einen gesellschaftlichen Handlungsrahmen. Durch Sozialisation erwerben neue Gesellschaftsmitglieder das notwendige Wissen und integrieren sich anhand gesellschaftlicher Vorgaben. Zugleich wird die bestehende soziale Ordnung kontinuierlich hinterfragt und angesichts neuer Entwicklungen, auch technischer Art, reflektiert und verändert. Soziale und technische Veränderungen sind dabei eng miteinander verwoben und bedingen sich wechselseitig.

Neben der Institutionalisierung sozialer Strukturen erfolgt stets auch eine technische Institutionalisierung, also eine technische Konstruktion der Wirklichkeit [3]. Technische Abläufe und Verfahren verfestigen sich ebenso wie Handlungen und Interaktionsbeziehungen in gesellschaftlichen Strukturen, genauer in *‚Technostrukturen‘,* und stehen den Individuen als objektivierte Gegebenheiten gegenüber. Technikaneignung und Umgang mit Technik wird entsprechend erlernt und folgt technostrukturellen Regulativen. Solche handlungsleitenden Institutionalisierungen sind DIN-und ISO-Normen, technologische Paradigmen (wie der

Verbrennungsmotor), oder dominante Designs (bspw. die QWERTY-Tastatur). Technische Institutionen begrenzen und regeln menschliches Handeln (so als Bestandteil der Verkehrstechnik: Ampeln, Schranken, Schilder) und eröffnen neue Handlungsoptionen, z. B. in Form von Experimentalsystemen (wie das CERN, die Europäische Organisation für Kernforschung). Der Beitrag fokussiert mithin, dem ‚Technopragmatismus' folgend, sich stetig wandelnde *soziotechnische* Konstellationen, bestehend aus Mensch und Technik. Insbesondere mit fortschreitender Technisierung kommen den technischen Instanzen immer mehr Handlungsträgerschaft und ein wachsender Anteil am Handlungsstrom zu.

1.2 Digitalisierung und algorithmische Konstruktion der Wirklichkeit

Digitalisierung ist eine *besondere* Form der Technisierung. Der symbolhafte Charakter der Technik bedingt eine neue Qualität im Unterschied zu analogen Werkzeugen und Maschinen. Digitale Technik ist größtenteils nicht sicht- oder fassbar, oft nur indirekt zugänglich (Reaktionen und Auswirkungen sind vermittelt) und permanent existent mit zahlreichen Rückwirkungen und (unbeabsichtigten) Nebenfolgen. Der Bereich des Digitalen erschließt sich nicht wie bei anderen Techniken materiell-sinnlich. Stattdessen sind Nutzer:innen über Interfaces mit einer schwer nachvollziehbaren Welt aus Bits und Bytes verbunden. Der Zugriff auf diese ‚Blackbox(es)' [4, 5] ermöglicht neue Interaktions- und Kommunikationsweisen, die auf einem komplexen Geflecht von Algorithmen und Daten aufbauen. In der digitalen ‚Echtzeitgesellschaft' ergänzen sich die Handlungsströme von Mensch und Technik mit *Datenströmen* aus ständig aktualisierten Daten [6, 7]. Die mannigfaltigen Daten sind verknüpfbar und verfolgbar, sie hinterlassen „Spuren" und bilden im Zeitverlauf ein für die Nutzer:innen intransparentes Referenzsystem.

Im Zuge von Digitalisierung entfalten sich neue Formen der Institutionalisierung, die im Anschluss an die vorstehenden Gedanken als *algorithmische Konstruktion* der Wirklichkeit gefasst werden. Neben gesellschaftliche Sozial- und Technostrukturen treten immer häufiger Algorithmenstrukturen, d. h. durch metrische Prozesse und kalkulatorisches Handeln etablierte und objektivierte Rahmenbedingungen sowie softwarebasierte Interaktions- und Kommunikationsformen. Dabei wird Technik immer stärker als mithandelnde Akteurin relevant. Software und *Algorithmen* bestimmen mehr und mehr soziales Miteinander. Die Herstellung sozialer Ordnung basiert somit zunehmend auf den Ergebnissen algorithmischer Prozesse und sich herausbildender digitaler Institutionen in

Form von Softwareanwendungen, aber auch als Hardware (Smartphone) und als digitale Praxen [8, 9]. Es bildet sich bspw. ein Kontext „des Surfens“, also der Aneignung und Nutzung digitaler Internettechniken heraus. Dieser konstituiert sich durch Technologiefirmen, deren Geräte und Applikationen sowie durch Regeln des digitalen Umgangs miteinander („Netiquette“). Normen und Werte menschlicher Kommunikation verändern sich (von E-Mail über Messenger-Dienste zu Instagram und TikTok), Gesetze werden angepasst und/oder erlassen (Datenschutz-Grundverordnung und ePrivacy-Verordnung), manche wirtschaftliche Organisationen verlieren an Bedeutung und Einfluss (etwa Netscape Communications und MySpace), während andere neu entstehen und den Markt dominieren, wie die sog. „Big Five“ Apple, Google, Microsoft, Facebook und Amazon.

Der institutionelle Kontext algorithmischer Strukturierung ist (noch) *fragil* und befindet sich in Aushandlung, da vielfältige Fragen bis heute nicht geklärt sind. Sind der Einsatz von Algorithmen und das Ergebnis algorithmischer Kalkulationen zu kennzeichnen? Bedarf es einer Kontrolle sozialer Plattformen und wie kann diese aussehen? Inwiefern hat Auskunft über die Verarbeitung personenbezogener Daten zu erfolgen? Wer trägt die Verantwortung in der algorithmischen Entscheidungsfindung? Es deutet sich an: Die algorithmische Konstruktion der Gesellschaft ist stark fragmentiert und schließt bislang nicht an die frühen Demokratieversprechen an [10, 11]. Digitales Leben vollzieht sich partiell (Onliner und Offliner), zensiert (gesperrte Webseiten, Unternehmens-Richtlinien), gefiltert (sowohl durch Algorithmen als auch durch Webseiten- und Profil-Inhaber:innen) und beschränkt bzw. vorstrukturiert (Vorgabe von Zeichenzahlen oder Umfang eines Anhangs). Auf diese Weise entstehen und/oder verstärken sich soziale Unterschiede, Exklusion und Intransparenz. Die Nutzung digitaler Technik birgt die Gefahr, emanzipatorische Potenziale zu verlieren. Die Macht des Digitalen, so die kritische Einstellung, symbolisiere einen ‚technologischen Totalitarismus‘ [12, 13].

1.3 Privatheit und Autonomie auf dem Prüfstand

Daraus leitet sich die These der folgenden Argumentation ab. Digitalisierung und algorithmische Konstruktion der Gesellschaft orientieren sich (derzeit) *einseitig* vor allem an techno-ökonomischen und machtpolitischen Kriterien. Gleichwohl finden sich auch Digitalisierungs- und Algorithmisierungsprozesse, die am Gemeinwohl orientiert sind und sich an den Belangen der Individuen und der Solidargemeinschaft ausrichten. Allerdings verlaufen diese Bemühungen eher im

Hintergrund und sind nicht die dominanten Strukturierungsmomente der digitalen Gesellschaft. Im Folgenden wird insofern eine *kritische* Perspektive auf die algorithmische Konstruktion der Wirklichkeit eingenommen. Damit ist keine immanent technikkritische Positionierung verbunden, die jeglichen Einsatz von Algorithmen und Künstlicher Intelligenz negativ beurteilt. Im Gegenteil sind zahlreiche Digitalisierungs- und Algorithmisierungsprozesse mit positiven Effekten, individuellem Empowerment und der Förderung von Gemeinschaft verbunden.

Allerdings ist es Ziel des Beitrags, auf gesellschaftliche Schieflagen hinzuweisen, die durch vorwiegend positiv konnotierten – auch im öffentlichen Diskurs – und unzureichend reflektierten Technikeinsatz hervorgerufen werden. Algorithmische Medien sind nicht neutral und Daten nicht objektiv. Algorithmisierung und damit verbundene digitale Dynamiken verändern grundsätzliche Handlungs- und Strukturmuster und ziehen problematische Verantwortungsverschiebungen in der Gesellschaft nach sich. Es stellt sich die Frage, wie Privatheit und Autonomie in einer algorithmisch konstruierten Welt gewährleistet und gefördert werden können. Hierzu wird insbesondere der mediale und forschungswissenschaftliche Diskurs aufgearbeitet und die Gefährdungen individueller Privatheit anhand ausgewählter Literatur belegt. *Privatheit* gilt in der eingenommenen Perspektive als, in Auseinandersetzung mit Gesellschaft, herzustellender Zustand und *Selbstermächtigung* folglich als Prozess, durch den dieser Zustand erreicht wird.

In diesem Beitrag geht es weniger um die konkrete Benennung von Instrumenten und Maßnahmen als vielmehr um die differenzierte Betrachtung von Herausforderungen und die Identifikation von möglichen Handlungsfeldern bzgl. Privatheit und Autonomie. Im Folgenden werden zunächst die algorithmische Konstruktion der Wirklichkeit und der Bedarf an Selbstermächtigung der Nutzer:innen und Verbraucher:innen näher erörtert (Abschn. 2). Anschließend werden drei Dimensionen der algorithmischen Konstruktion und mögliche Formen der Selbstermächtigung diskutiert: Algorithmen als Besitztümer (Abschn. 3), als Akteure (Abschn. 4) und als Kontrollmittel (Abschn. 5). Im Resümee wird abschließend auf die Notwendigkeit einer kollektiven Selbstermächtigung hingewiesen (Abschn. 6).[1]

[1] Mein Dank gilt an dieser Stelle den drei Reviewer:innen für die konstruktiven Hinweise zum ursprünglichen Manuskript.

2 Algorithmische Konstruktion und Selbstermächtigung

Aus informatischer Perspektive ist ein Algorithmus eine wohl-definierte Berechnungsprozedur, die ausgehend von einem gegebenen Input an Daten einen bestimmten Output an Daten erzeugt. Mit anderen Worten: Algorithmen sind Werkzeuge, mit denen konkrete Berechnungsprobleme in einer Sequenz von Einzeloperationen gelöst werden. In diesem Sinne handelt es sich um eine Art Handlungsanweisung. Dazu muss die soziale Welt kalkulierbar werden: Der Gegenstand oder Prozess wird zum semiotischen Zeichen, dann zum Signal, das jede Bedeutung verliert, und schließlich berechenbar.

2.1 Algorithmische Konstruktion und digitale Vulnerabilitäten

Soziale Phänomene werden durch *Verdatung und Algorithmisierung* in binäre Kategorien überführt – Analoges wird digital. Vice versa werden von Technik Daten als Aussagen über die soziale Welt zur Interpretation durch Menschen rückgemeldet – digitale Werte werden analog. Mit diesem doppelseitigen Transformationsprozess sind spezifische Charakteristika und Herausforderungen verbunden [14]. Drei *Dimensionen* algorithmischer Konstruktion von Wirklichkeit erscheinen für diesen Beitrag zentral.

Erstens werden Algorithmen von Menschen entwickelt. Es existieren Konstrukteure und Konstrukteurinnen, die den Arbeitsbereich und die Funktionalität der Algorithmen festlegen. Insofern fließen spezifische Weltsichten und Deutungen sowie Problemlösungsstrategien in die Softwareentwicklung ein. Darüber hinaus ist der „Arbeitsbereich" von Algorithmen eingeschränkt, sie funktionieren unter spezifischen Bedingungen für konkrete Fragestellungen. *Zweitens* nehmen Algorithmen an menschlichen Handlungen und Interaktionen teil, indem sie komplexe Kommunikations-, Regelungs- und Entscheidungsprozesse unterstützen und beeinflussen [15, 16]. Algorithmen besitzen Handlungsträgerschaft (‚Agency'), handeln mit und prägen nicht nur individuelles Verhalten, sondern auch gesellschaftliche Strukturen. *Drittens* erzeugen digitale Techniken Datenspuren. Daten werden erhoben, verarbeitet, weitergeleitet, ausgetauscht und gespeichert. Im Zeitverlauf bildet sich ein komplexes datenbasiertes Referenzsystem in der digitalen Welt heraus. Wer über diese Daten verfügt und bestimmt, ist in der Lage, Machtansprüche geltend zu machen und/oder Macht auszuüben.

Gesamtgesellschaftlich bilden sich eigenständige, digitale Infrastrukturen und Institutionen als neue Basis sozialen Zusammenlebens heraus [17, 18]. Das

bedeutet auch, dass durch Nutzung digitaler Technologien neue *digitale Vulnerabilitäten* entstehen. Neue Angriffsflächen bei Nutzer:innen bieten sowohl die Sorglosigkeit und/oder Überschätzung der eigenen Fähigkeiten im Umgang mit Computertechnik als auch potenzielle Sicherheitsrisiken. Durch ‚Trivialisierung' der digitalen Werkzeuge werden die mit der Nutzung verbundenen Gefahren und Risiken ausgeblendet [19]. Eine mögliche Besorgtheit der Nutzer:innen geht dennoch einher mit einem unbesorgten Umgang mit ihren Daten (‚Privacy-Paradox'). Hinzu kommt, dass gerade beim Einsatz von Digitaltechnik oftmals noch institutionalisierte, sicherheitsfördernde Maßnahmen fehlen [20]. So besteht neben verschiedenen Formen der Cyberkriminalität (Cyber-Grooming, Phishing-Betrug, Identitätsdiebstahl, etc.) die Gefahr, dass Menschen im Rahmen von Datenökonomie und Plattformkapitalismus zu „gläsernen" Verbraucher:innen werden, wenn Technologiefirmen ihre Netzwerkmacht missbrauchen, um etwa Konsum anzuregen. Ebenso kritisch ist die Möglichkeit einzuschätzen, „gläserne" Bürger:innen zu erzeugen, etwa im Zuge einer stärkeren Überwachung durch staatliche Organisationen und Geheimdienste, die Computer infiltrieren und Funkzellen abfragen (Stichworte: Bundestrojaner und Vorratsdatenspeicherung).

Digitale Angriffsflächen sind wenig offensichtlich und nur vermittelt erfahrbar. Angriffe erfolgen mittels Algorithmen, Softwareagenten und neuronalen Netzen und basieren auf der Zirkulation von, seien es durch „freiwillige" Angaben oder durch nicht sichtbare Protokollierung erhobene, Daten der Nutzer:innen und Verbraucher:innen durch die Gesellschaft. Der Einsatz von Algorithmen und deren Funktionsweise sind weitestgehend intransparent und die – wenn auch bedienrichtige – Nutzung von Computertechnik ist oft durch Nicht-Wissen über die zugrunde liegenden Infrastrukturen, Eigentumsrechte und regulativen Hoheitsansprüche gekennzeichnet.

2.2 Digitale Selbstermächtigung entlang dreier Dimensionen

Während die Gewährleistung von Privatheit und Autonomie zum einen seitens wirtschaftlicher Unternehmen oftmals untergraben wird und zum anderen durch staatliche bzw. politische Regulierung lange Umsetzungsphasen durchläuft, sehen sich Nutzer:innen und Akteure und Akteurinnen in eigener Verantwortung, aktiv zu werden und sich zu schützen. Es bedarf einer *digitalen Selbstermächtigung* im Rahmen der Nutzung von digitalen Techniken, um zu einem gewissen Grad digital souverän handeln zu können. Digitale Souveränität umfasst Datenschutz, Privatheitsschutz (Privacy) und Datensicherheit ebenso wie verschiedenste

soziale, technologische und regulative Aspekte, so den Erwerb digitaler Kompetenzen, Privacy-by-Design, Interoperabilität, und vieles mehr [21, 22]. Für digitale Selbstermächtigung sind insbesondere Einblick und Kontrolle in die Arbeit von Algorithmen, in Datenbewegungen und in zugrunde liegende Infrastrukturen wichtig [23]. Selbstermächtigung im Bereich des Digitalen ist nicht nur eine Form der praktischen Befähigung, sondern auch der Reflexion und Bewertung des eigenen Handelns mit Computertechnik, also Aneignung und Distanzierung mit dem Ziel der Hervorbringung, Veränderung und Aufrechterhaltung autonomer digitaler Handlungsweisen. Digitale Selbstermächtigung stellt die Nutzer:innen und Verbraucher:innen in den Mittelpunkt und nicht techno-ökonomische Interessen oder politische Überwachungsmaßnahmen.

Die vorgenommene Identifizierung eines Bedarfs an digitaler Selbstermächtigung ist keine neoliberalistische Forderung, die das Individuum einzig und allein selbstverpflichtet. Es geht um die Stärkung *einer* Facette der Sicherung von Privatheit und Autonomie, eine Facette, die von Nutzer:innen eigenständig bearbeitet werden kann. Darüber hinaus wären bspw. Infrastruktursysteme, die Privatheit fördern, zu schaffen – ganz im Sinne einer gesellschaftlichen Verantwortung für Privatheit (aller) [24]. Die Zuständigkeiten und Verantwortlichkeiten dafür sind weit gestreut, auch wenn es sich oft um ostentative Zuschreibungen handelt und keine konkret umgesetzten Handlungsprogramme. Selbstermächtigung bedeutet auch, von anderen ermächtigt, also durch fremdes Handeln in Autonomie und Souveränität gestärkt zu werden, wie im Falle eines holistischen Datenschutzes [19]. *Fremdermächtigung* und das Engagement staatlicher oder institutioneller Akteurinnen und Akteure haben einen Anteil am souveränen Handeln Einzelner. Das verweist auf die Relevanz eines umfassenden Konzepts von Privatheit, bei dem individuelle Nutzer:innen nur ein Teil der schützenden Figuration sein können. Darüber hinaus sind wirtschaftliche, politische und wissenschaftliche Akteurinnen und Akteure ebenso gefordert, die Privatheit und Autonomie von Nutzer:innen zu ermöglichen. In diesem Beitrag werden die temporären „Grauzonen“ hervorgehoben, in denen Verantwortung durch Andere nicht übernommen und/oder zugeteilt wird und Schutzmaßnahmen für die Individuen mindestens für einen beschränkten Zeitraum ausbleiben.

Im Folgenden werden die drei genannten Dimensionen algorithmischer Konstruktion der Wirklichkeit ausführlicher diskutiert und zugehörige gesellschaftlichen Auswirkungen sowie Ansätze digitaler Selbstermächtigung skizziert (vgl. Tab. 1). Selbstermächtigung erfolgt bestenfalls entlang aller Dimensionen, wobei deren Trennung analytischer Art ist, und die Dimensionen empirisch ineinander übergehen. Kapitel drei „Algorithmen als Besitztümer“ fokussiert Software und Code als Eigentum und stellt digitale Aufklärung und den Erwerb von Hintergrundwissen in den Vordergrund, bspw. über Sektoren, Firmenstrukturen

Tab. 1. Dimensionen algorithmischer Konstruktion

Algorithmen als…	Modus	Imagination und Repräsentation	Selbstermächtigung durch…
…Besitztümer	Geldquelle	Rationalität	…digitale Aufklärung: Hintergrundwissen
…Akteure	Interaktion	Objektivität	…digitale Bildung: Handlungswissen
…Kontrollmittel	Daten	Legitimität	…digitale Achtsamkeit: Folgenwissen

und Kooperationen. „Algorithmen als Akteure“ (Kapitel vier) nimmt die Interaktion mit Software in den Blick und fokussiert Kompetenzerwerb durch digitale Bildung, um den Output von Algorithmen einzuordnen, um also bspw. Suchergebnisse und mediale Öffentlichkeiten zu deuten. Das fünfte Kapitel „Algorithmen als Kontrollmittel“ stellt Daten in den Mittelpunkt und sieht digitale Achtsamkeit (etwa Datensparsamkeit) als zentralen Mechanismus der Selbstermächtigung.

In der vorliegenden Argumentation wird eine Akzentuierung der *Fähigkeiten und Kompetenzen* des Individuums vorgenommen – ganz im Sinne der Fragestellung: Was kann jede:r selbst auf einem niedrigschwelligen Niveau für die eigene Privatheit in der digitalen Sphäre tun? Demzufolge tritt auch die Diskussion der konkreten Verantwortung für Schutzmaßnahmen in den Hintergrund, etwa der staatliche Ausgestaltungsauftrag für Datenschutzregeln und Auffangverantwortung. Individuellen Praktiken der Selbstermächtigung wird ein eher geringer Durchdringungsgrad in der Gesellschaft konstatiert und genau darin liegt die Gestaltungsaufgabe. Diese Gestaltungsaufgabe erfordert allerdings die kollektiven Bemühungen verschiedener Akteurinnen und Akteure und die Institutionalisierung gesellschaftsweit verfügbarer Maßnahmen [20]. Die Zuständigkeiten für Privatheit sind multipel und bilden ein Netz *verteilter Verantwortung.* Dieses Phänomen wird bereits in den nachstehenden Ansätzen zu Selbstermächtigung tangiert und im abschließenden Kapitel aufgegriffen.

3 Algorithmen als Besitztümer: Geldquelle, Rationalität, Aufklärung

Algorithmen und Software sind Besitztümer, Eigentum und Geldquelle. Als Institutionen repräsentieren Algorithmen rationale Problemlösungen. Nutzer:innen

imaginieren eine auf sie selbst ausgerichtete Funktionalität. Diese paradigmatische Repräsentation liegt quer zur intransparenten Inwertsetzung von Nutzer:innen-Daten. Es scheint daher nötig, einen Blick in die Blackboxes der Algorithmen zu werfen und sich im Sinne digitaler Aufklärung mit Hintergrundwissen über digitale Technik auszustatten.

3.1 Geldquelle

Algorithmen sind durch Menschen geschaffene Produkte für wirtschaftliche Unternehmen, staatliche und andere Organisationen. Der Quellcode unterliegt daher in den meisten Fällen spezifischen *Eigentumsrechten* und gilt als Betriebsgeheimnis. Algorithmen haben eine konkrete Zielsetzung, die sich vorrangig über die offiziell artikulierte Funktion definiert. Über den Verkauf von Software generieren Unternehmen einen Gewinn. Ebenso wird mit kostenfrei angebotener Software *Geld* verdient, indem bspw. Werbung in der Software eingeblendet wird und/oder die Daten der Nutzer:innen verwertet werden. Die vordergründige Funktion der Nutzung, bspw. von sozialen Medien wie Facebook, wird so mit einem weitgehenderen Geschäftsmodell überlagert. In diesen Funktionschimären überwiegen die wirtschaftlichen Interessen der Privatunternehmen die sozialen Interessen der Nutzer:innen. Algorithmen und digitale Technik sind sozial konstruiert, beinhalten demzufolge eingeschriebene Handlungsanweisungen und verkörpern vorherrschende Paradigmen, insb. Visionen von Ingenieur:innen, Ideologien globaler Konzerne, und mögliche Stereotype und Rassismen [25, 26].

Dieses ökonomisierte und von datenbasierten Geschäftsmodellen geprägte Technikmilieu ist für Nutzer:innen weitgehend intransparent. *Verantwortung* für eine souveräne Computernutzung wird nicht von den Eigentümer:innen übernommen, sondern diffundiert in den soziotechnischen Konstellationen und verfestigt sich in unausgesprochenen Verhaltensmustern [27]. Einerseits wird die Verantwortung zum Umgang mit personenbezogenen Daten an die Nutzer:innen delegiert, indem überkomplexe Allgemeine Geschäftsbedingungen vorgelegt werden, obwohl Nutzer:innen oft nicht in der Lage sind, sich mit den zahlreichen Regelungen aller Dienstleistungsanbieter:innen auseinanderzusetzen. Andererseits muss Software von Nutzer:innen aufwendig konfiguriert werden, um in einem Privatsphäre-Modus zu arbeiten. Softwareentwickler:innen und Anbieter:innen digitaler Techniken entziehen sich so ihrer Verantwortung. Auch die neuen Regelungen über den Einsatz von Cookies werden mitunter durch schlechte Usability untergraben, sodass die Aus- bzw. Abwahl von Cookies vernachlässigt wird und die Firmen letztendlich doch Daten erheben können.

3.2 Rationalität

Darüber hinaus stellt sich eine weitere Form der Verantwortungsverschiebung ein, wenn Nutzer:innen die Algorithmen als die eigentlichen Handlungsträger ansehen [28]. Die Zuschreibung von Handlungsfähigkeit geht einher mit der Zuweisung von Verantwortung. Die Funktionsausführung der Algorithmen erscheint dann *rational* und die Ergebnisse objektiv. Die dahinterliegenden Strukturen und Eigentümer:innen der Software werden außer Acht gelassen und die multiple Fehleranfälligkeit der Software dürfte in den wenigsten Fällen reflektiert werden. So gelingt es Organisationen ihre Interessen zu technisieren und daraus Profit zu schlagen: das Suchergebnis einer Maschine ist, wie es ist, und gilt als zuverlässig. Die Google-Suchmaschine ist in dieser Hinsicht ein Paradebeispiel für eine algorithmische Institution.

Private Firmen erhalten durch Nutzer:innen einen Vertrauensvorschuss, trotzdem sie die Verantwortung für ihr Handeln auf Nutzer:innen und Technik übertragen. Oft scheint eine gewisse Gutgläubigkeit gegenüber digitalen Technologien zu überwiegen. Dabei kann bspw. bei Suchmaschinen nicht von Suchneutralität ausgegangen werden [16]. Es ist in der Regel kaum möglich, etwas über Prozeduren zur Generierung von Trefferlisten oder Empfehlungen in Erfahrung zu bringen. Die Nutzer:innen sind daher geleitet von einem kurzfristigen Pragmatismus [17]. Sie lassen sich Daten vorsortieren und schauen, ob das Ergebnis in der jeweiligen Situation passt und Gültigkeit besitzt. Ein Urteil über die Qualität der Daten können sie sich kaum bilden. Alle Prozesse der Modellbildung, der Datenauswahl usw. sind ebenso ausgeblendet, wie die eingangs erwähnten Geschäftsmodelle.

3.3 Digitale Aufklärung

Selbstermächtigung der Nutzer:innen wird durch den Erwerb von *Hintergrund- bzw. Kontextwissen* über das Technikmilieu, nicht nur der „Big Five“, möglich. Bislang ist vor allem zu beobachten, dass sich Nutzer:innen proaktiv und auf vielfältige Weise Bedienwissen aneignen. Die Schnittstelle zum digitalen Endgerät scheint jedoch eine „Trennwand“ zu markieren und den Erwerb von Hintergrundwissen zu hemmen. Selbstermächtigung bedeutet das Hinterfragen von digitalen Strukturen und Prozessen.

Hintergrundwissen ist zwar nicht zwingend notwendig, um Techniken zu handhaben. Im Gegenteil: es ist ein grundlegendes Charakteristikum von Technik, als Blackbox zu funktionieren, um die Nutzung zu erleichtern. In Bezug auf die besonderen Merkmale von Digitalisierung (intransparente Referenzsysteme,

Datenprotokollierung, algorithmische Induzierung), wird es jedoch immer wichtiger, die Blackbox der Algorithmen zumindest in Teilen zu verstehen. Welche Firma besitzt welche Software und verdient damit auf welche Weise Geld? Auf welchen Servern werden Bilder und Dokumente gespeichert und welche Verantwortungsprinzipien sind damit verbunden? Nach welchen Regeln arbeiten Filter- und Bewertungsalgorithmen und wie erfolgt Personalisierung?

Letztlich entscheiden Nutzer:innen, welchen Dienst sie zu welchen Konditionen „einkaufen". Diese Konditionen könnten jedoch transparenter gemacht werden. Insbesondere Klarheit über die hinter den Algorithmen liegenden Wissensmodelle und deren Ausrichtung auf Profit oder Gemeinwohl wäre wichtig. Initiativen und Vereine klären diesbezüglich über Digitaltechnik und spezifische Herausforderungen auf. So wurde bspw. das „kritische Lexikon der Digitalisierung" [29] herausgegeben und es existiert ein „Deutschland Dialog für digitale Aufklärung".[2] Der Staat sieht sich ebenso in der Verantwortung und die „Bundeszentrale für digitale Aufklärung"[3] kann u. a. bei Themen wie Fake News und Hassrede zu wichtigen Einsichten und möglichen Handlungsstrategien verhelfen. In der Analyse algorithmischer Entscheidungsfindung ist zudem die Nichtregierungsorganisation „AlgorithmWatch" sehr aktiv und informiert über die Arbeitsweise von Algorithmen, zuletzt bei „Instagram".[4]

4 Algorithmen als Akteure: Interaktion, Objektivität, Bildung

Nutzer:innen stehen in Interaktion mit Algorithmen und Software. Die Meldungen und Benachrichtigungen der digitalen Technik werden als objektive Ergebnisse wahrgenommen. Diese Repräsentationen von realer Welt werden kaum hinterfragt und für gültig befunden. Algorithmen beeinflussen so menschliches Handeln. Der Umgang und Dialog mit Technik sollte reflektiert werden, besonders vor dem Hintergrund der begrenzten Arbeitsgebiete von Algorithmen. Digitale Bildung fördert hier den Erwerb von Bedien- und Nutzungswissen.

[2] Vgl. https://www.sicher-im-netz.de/deutschland-dialog-für-digitale-aufklärung (10.10.2020).

[3] Vgl. https://www.bundesregierung.de/breg-de/bundesregierung/staatsministerin-fuer-digitalisierung/bundeszentrale-fuer-digitale-aufklaerung (06.12.2020).

[4] Vgl. https://algorithmwatch.org (10.10.2020).

4.1 Interaktion

Digitale Technik handelt mit, beeinflusst soziales Handeln und bringt soziale Wirklichkeit hervor [30]. Algorithmen entscheiden, welche Ausschnitte von der Welt auf „Twitter“ in den Meldungen oder bei „Amazon“ in den Kaufempfehlungen zu sehen sind. Grundsätzlich erlaubt Personalisierung, sich zielgerichtet mit relevanten Optionen zu beschäftigen. Gleichzeitig fehlt Nutzer:innen der Zugriff auf derartige Algorithmen, um eben jene Personalisierung zutreffend zu definieren. Soziales wird also nicht dargestellt, sondern vorgefiltert und sortiert. Algorithmen agieren in und für einen kleinen Ausschnitt der Welt. Der Output von Algorithmen wird mitunter jedoch als universell gültig angesehen. In der Konsequenz besteht die Gefahr, diese für jeden User eigens generierten, modellbasierten Konstruktionen als realweltliche *Repräsentationen* misszuverstehen [17]. „Facebook“ als primäre Nachrichtenquelle für Nutzer:innen und damit digitale Institution ist insofern kritisch zu sehen.

Das eher „passive“ Zuschneiden der Welt der Nutzer:innen wird ergänzt durch immer häufigere Handlungsinitiierungen von technischen Agenten. Durch ‚Nudging‘ werden Handlungen von Anwender:innen unbemerkt in vorgegebene Richtungen gelenkt. Update-Aufforderungen und Empfehlungen von Produkten oder Kontakten in sozialen Netzwerken nehmen die Aufmerksamkeit der Nutzer:innen in Anspruch und veranlassen oder erzwingen sogar eine Reaktion. Technologiefirmen werden zu ‚gierigen Institutionen‘ [31], die allumfassende „Besitzansprüche“, d. h. permanente Erreichbarkeit und Verantwortung zur Reaktion, an die Nutzer:innen stellen. Ausgehend von der Programmierung und implementierten Funktionalität beeinflussen Algorithmen unser Verhalten und sind darüber hinaus Teil von Entscheidungsketten und Entscheidungsfindung. ‚Scoring‘ durch Algorithmen regelt Sozialbeziehungen, bspw. in Einstellungsgesprächen oder bei der Bonitätsauskunft. Die Unantastbarkeit der Zahlen und berechneten Werte ist dabei zentrales Moment: eine SCHUFA-Bewertung ist korrekt, auch wenn unklar ist, wie sie entsteht [32].

4.2 Objektivität

Algorithmen werden zu Regelungsmechanismen sozialen Lebens, indem sie gesellschaftliche Komplexität reduzieren. Ihre Berechnungen und Ergebnisse besitzen eine inhärente *Objektivität.* Es scheint, als wäre der Algorithmus intelligent, wenn er Präferenzen identifiziert. Das erscheint bei Algorithmen als Handlungsgrundlage durchaus fragwürdig, da diese anhand der vergangenen

Handlungen (Selektionen) der Nutzer:innen und früheren Referenzen (Webseitenaufrufen, Likes, Einkäufen, etc.) funktionieren. So werden Dysfunktionalitäten diskutiert, etwa in Form von ‚filter bubbles' und ‚echo chambers', in denen Nutzer:innen durch automatisierte Personalisierung „gefangen" seien [33].

Algorithmen und deren Ergebnisse sind sehr dynamisch, weil sie von den Entwickler:innen ständig angepasst werden und weil Nutzer:innen durch ihre Aktionen und Handlungen (mitunter absichtsvoll und manipulativ) Daten generieren, die die Ergebnisse der Algorithmen verändern. Ein Kernmoment digitaler Technologien besteht also darin, dass sie sich zu jeder Zeit in Modifikation befinden (können) – auch wenn gerade darauf zugegriffen wird. Die immanente Dynamik der Technik resp. die permanente technische *Unabgeschlossenheit* [34] hat Konsequenzen. Nutzer:innen erlernen nicht einmalig den Umgang mit einer Technik, sondern müssen sich stets umorientieren, neu lernen, neu denken. Objektivität und Erwartungssicherheit, die mit Technik typischerweise verbunden ist, erodieren im digitalen Raum.

4.3 Digitale Bildung

Aus den vorstehenden Bemerkungen lässt sich eine technische *Selbstverantwortlichkeit* der Nutzer:innen ableiten. Selbstermächtigung bedeutet in dieser praktischen Hinsicht die kompetente Handhabung digitaler Technik zu erlenen. Dazu gehört primär die Aneignung des Bedienwissens von Smartphones, Computern, Peripheriegeräten (bspw. Routern). Es bedeutet gleichzeitig auch, eine (Kauf-)Auswahl für bestimmte Geräte treffen zu können, und zwar nach den für die Nutzer:innen wichtigen Kriterien. Dies sollte dem Trend entgegenwirken, dass Technologiefirmen Zwecke für vorhandene Techniken festlegen und deren Dienstbarkeit suggerieren, statt reale Bedarfe zu adressieren. Die souveräne Handhabbarkeit digitaler Technik umfasst zudem intuitive Designs, altersgerechte Menüstrukturen und individuelle Konfigurierbarkeit. Softwareentwickler:innen sind hier gefordert, nutzerzentrierte und subjektorientierte Produkte zu gestalten. In Bezug auf Konstruktion und Implementierung von Software stellen sich die Fragen der Verantwortung für eine nutzer:innenfreundliche Gestaltung. Entwickler:innen sind in Konzernstrukturen eingebunden und programmieren auftragsgemäß [35]. Vorgaben für Softwareprodukte werden insofern intern durch das Management oder extern durch staatliche Vorgaben gemacht. Auch wenn deren Einfluss aktuell gering erscheint, werden Forderungen nach ‚demokratischen Ingenieur:innen' laut, die Technikentwicklungen eine selbstermächtigende Richtung geben [36].

Bezüglich der Interaktion mit Algorithmen wäre es wünschenswert, diese und deren Arbeit zu kennzeichnen und sichtbar zu machen. So wären bspw. Suchergebnisse direkt adressierbar und bekämen weniger den Eindruck von Objektivität. Auch der Einsatz alternativer Algorithmen durch Nutzer:innen und die eigenverantwortliche Ent-Personalisierung von Software sollten gefördert werden. Dazu braucht es eine stete Erweiterung und Aktualisierung der Grundkompetenzen digitalen Handelns. Solch eine digitale Bildung kann bereits in der Schule beginnen [37],[5] wobei der dazu nötige Diskurs über Format und Inhalte eines entsprechenden Schulfachs aktuell eher parteilich aus Informatik-Perspektive geführt wird. Zudem darf ein „Digitalpakt" nicht lediglich zu einer Digitalisierung überholter Lehrpläne führen. Digitale Bildung ist Bestandteil lebenslangen Lernens und es scheint unerlässlich, Maßnahmen sowohl zielgruppenspezifisch zuzuschneiden, bspw. mit Comics für Kinder[6] oder Projekten für Senior:innen[7], also auch Angebote in Volkshochschulen und anderen Bildungseinrichtungen zur Verfügung zu stellen.

Selbstermächtigung wird zudem durch Verbraucher:innenschutzverbände gewährleistet. Die Cyberfibel[8] etwa vermittelt, wie sich Verbraucher:innen im Alltag vor Bedrohungen schützen können. Nutzer:innen sind darüber hinaus aufgefordert, proaktiv Erfahrungsberichte im Umgang mit Softwareprodukten zur Verfügung zu stellen und so strukturelle Problemlagen aufzudecken. Mit der „Marktbeobachtung Digitales" (früher Marktwächter „Digitale Welt") bspw. wird versucht, Verbraucher:innen bei Online-Einkäufen oder bei der Nutzung von Preisvergleichsportalen zu unterstützen und deren Interessen zu schützen.[9]

5 Algorithmen als Kontrollmittel: Daten, Legitimität, Achtsamkeit

Algorithmen produzieren Daten und arbeiten mit Daten, die nicht den Nutzer:innen zur Verfügung stehen, sondern von den Eigentümer:innen der Software in Wert gesetzt werden. Damit sind Tendenzen der Überwachung und Kontrolle verbunden. Über argumentative Legitimation werden von Privatunternehmen und

[5] Vgl. auch https://www.netzwerk-digitale-bildung.de (10.10.2020).

[6] Vgl. https://edri.org/our-work/privacy-for-kids-digital-defenders (10.10.2020).

[7] Vgl. https://www.silversurfer-rlp.de/ (10.10.2020).

[8] Vgl. https://www.cyberfibel.de (01.12.2020).

[9] Vgl. https://www.vzbv.de/themen/marktbeobachtung/marktbeobachtung-digitales (10.10.2020).

Regierungen Profile von Nutzer:innen und Bürger:innen angelegt und deren Aktivitäten verfolgt. Dieser informationelle Kapitalismus ist offenzulegen und Nutzer:innen ist mehr digitale Achtsamkeit zu vermitteln.

5.1 Daten

Zunehmend werden unter Einsatz von Algorithmen und aufgrund von Daten und deren Verknüpfungen algorithmenbasierte Entscheidungen getroffen, Scorings und Bewertungen vorgenommen und ‚Big Data'-Analysen durchgeführt, die die sozialen Ordnungsleistungen und die gesellschaftliche Dynamik tangieren. Ausgehend von der Hoffnung, dass mit dem Aufkommen des World Wide Web und digitaler Kommunikation (dezentrale Vernetzung, peer-to-peer-Kommunikation, eine wertfreie (d. h. ungefilterte und ungebremste) Informationsübertragung und freie Verlinkungen) sich demokratische bzw. demokratisierende Prozesse entfalten, wird nunmehr konstatiert, dass die digitale Welt zunehmend reguliert, hierarchisiert und zentralisiert wird [38].

Ausschlaggebend dafür sei die *Ökonomisierung* der digitalen Welt, die zugleich die infogene Grundversorgung und das Menschenrecht auf Informationszugang gefährde. Digitale Entwicklung scheint gekennzeichnet durch ubiquitäre Technisierung, infrastrukturelle Zentralisierung und scharf asymmetrische Inklusionsordnungen [27]. Nutzer:innen seien im sog. ‚informationellen' oder ‚kybernetischen' Kapitalismus lediglich Datenlieferanten und würden durch das (auch heimliche) Sammeln von Daten ausgebeutet und von den profitgenerierenden Bedingungen abgeschnitten [39–42]. Die Monopolisierung und Informationsmacht bei einer Handvoll Firmen wie Apple, Microsoft, Google, Amazon und Facebook führe zu rekursiven Steuerungsprozessen menschlichen Handelns, aufbauend auf den durch Nutzer:innen generierten Datenströmen.[10]

5.2 Legitimität

Algorithmen sind Kontrollinstanzen. In ihrer Kombination oder Gesamtheit unter zentraler Verwaltung lassen sich Daten kombinieren, Profile erstellen und Überwachungsstrukturen schaffen. Welche Daten der Individuen hierbei an welchen

[10] Ähnlich verhält es sich mit dem Social Credit System in China, bei dem die Daten allerdings aus staatlicher Protokollierung und Überwachung stammen und für die Bewertung der Bürger:innen (und Firmen) in Bezug auf Staatstreue genutzt werden.

Stellen der Gesellschaft verarbeitet werden, ist für Nutzer:innen wenig nachvollziehbar. Zu denken ist diesem Zusammenhang an Predictive Policing, Gesichtserkennung und die neueren Diskussionen über die Steuer-ID in Deutschland. Legitimität für unmittelbare algorithmengesteuerte Kontrolle und Überwachung wird hergestellt u. a. durch Begründung erhöhter *Sicherheit* und erhöhter Sicherheitsbedürfnisse der Bürger:innen.

Mittelbare, also indirekte, Kontrolle durch Technologiefirmen etwa legitimiert sich demgegenüber unter einer funktionsbedingten Argumentation. Ohne Daten wäre eine regelkonforme Nutzung von Software nicht möglich. Damit verbunden ist die stillschweigend Zustimmung der Nutzer:innen. Aufgrund fehlenden Widerspruchs, sei es weil ein Widerspruch nicht als Handlungsoption zur Auswahl steht oder nicht wahr- und/oder ernstgenommen wird, wird der Einsatz der Algorithmen toleriert und so legitimiert. Es sind über die Nutzung hinausgehende „Zwangsformen", denen sich die Nutzer:innen ausgesetzt sehen, wie die Einwilligung in Datenweitergabe oder Werbemails. Digitale Technik wird in ihrer jetzigen Form als Status Quo anerkannt und Nutzer:innen ordnen sich „freiwillig" dieser Netzwerkmacht unter [17].

5.3 Digitale Achtsamkeit

Die zentrale Herausforderung für Selbstermächtigung besteht zunächst darin, dass Nutzer:innen digital wachsam sind und die Chancen und Risiken der Nutzung digitaler Technologien vor allem mit Blick auf die Datenspuren und Referenzsysteme abschätzen, also *Folgenwissen* generieren und erwerben.

Daten sind bspw. immer seltener auf den Endgeräten der Nutzer:innen gespeichert, sondern in einer ‚Cloud' zentral verfügbar, also auf den Servern und Datenbanken der Dienstleister:innen. Mit Nutzung von Clouds geht die, mit einem Personal Computer gewonnen, Souveränität wieder verloren und es stellen sich Fragen der Sicherheit, des Zugriffs und der Überwachung – auch bereits bei der Übermittlung. Als Alternative gilt die unabhängige Vernetzung von Computern, wie bei der Initiative „Freifunk".[11] Auch der Einsatz von VPN-Servern und des „privaten Modus" bei Nutzung von Browsern bieten Möglichkeiten gegen Ausspähen, wenngleich diese Instrumente gegenüber professionellen Hackern und Geheimdiensten kaum Schutz bieten. Software und Plattformen sollten von Technologieunternehmen initial auf Privatheit ausgelegt sein, um personenbezogene Daten zu schützen. Nutzer:innen hätten dann später die Möglichkeit, Daten zu

[11] Vgl. https://freifunk.net (10.10.2020).

spezifischen Zwecken freizugeben. Auch hier zeigen sich Konvergenzen von Selbst- und Fremdermächtigung durch Privacy by Design und Default-Konzepte.

Datensicherheit ist auch Aufgabe des Staates. Öffentliche Rechenzentren könnten hier eine neue Rolle einnehmen [43, 44]. Neben dem Schutz der Privatsphäre der Bürger:innen könnten diese als Wissensbasen dienen und Informationen und Kurse anbieten. Dadurch ergäben sich für Bürger:innen Möglichkeiten, ihr Handeln an professionellem und lokal relevantem Wissen auszurichten. Dass digitale Medien auf solche Zielsetzungen ausgerichtet sein können, zeigt das Projekt „FragDenStaat“.[12] Bürger haben hier die Möglichkeit, Anfragen zu politischen Themen an staatliche Behörden zu stellen. Die Anfragen und Antworten werden gesammelt und stehen der digitalen Öffentlichkeit zur Verfügung. Auf europäischer Ebene gibt es ebenfalls Bemühungen, sich durch „GAIA-X“ eine regional begrenzte Cloud-Infrastruktur zu schaffen und so Datenhoheit aufrecht zu erhalten und Daten zu sichern.

6 Digitale Selbstermächtigung als kollektiver Prozess

Gesamtgesellschaftlich ist zu beobachten, dass sich Handlungen, Werte, Normen und Lebensweisen verstärkt an rationalistischen, ökonomischen und algorithmischen Grundmustern orientieren [32, 45]. Dabei werden eher kaum demokratisierende und emanzipatorische Prozesse angestoßen, sondern in digitalen Technologien werden die sozialen, bspw. milieu- und altersspezifischen, Verhältnisse gespiegelt und digitale Klüfte erzeugt [46]. Privatheit und Autonomie der Nutzer:innen stehen dabei auf dem Prüfstand und Fragen nach digitaler Selbstermächtigung werden aufgeworfen.

6.1 Algorithmische Konstruktion und Gesellschaft

Die algorithmische Konstruktion der Gesellschaft zeigt viele Manifestationen, von denen drei analytisch getrennte, jedoch empirisch eng miteinander verbundene Facetten erörtert wurden. Sozial konstruierte Algorithmen agieren autonom, interagieren mit Nutzer:innen, sortieren und filtern für sie die Wirklichkeit und übernehmen gesellschaftliche Kontrollfunktionen [47, 48]. Damit sind Chancen und Vorteilen verbunden. Algorithmen reduzieren durch Personalisierung Komplexität und ermöglichen bzw. unterstützen auf diese Weise Handeln. Dies erfolgt

[12] Vgl. https://fragdenstaat.de (10.10.2020).

jedoch völlig intransparent. Neben reinem Bedien- und z. T. Konstruktionswissen, das sich die Nutzer:innen selbst aneignen, bringen sie kaum etwas über die Grundlagen und Funktionsweisen der Algorithmen oder über den Verbleib der persönlichen Daten in Erfahrung. Algorithmisierung ermöglicht zwar Verschlüsselung und anonyme Kommunikation, es existieren Firewalls, um PCs zu schützen und der Einsatz von Track-Blockern vermindert die Sammlung von Daten. Nutzer:innen haben jedoch selten Wahlmöglichkeiten beim Einsatz digitaler Medien, es werden ihnen lediglich Entscheidungen überlassen. Diese Entscheidungen folgen nicht selten der Maxime, entweder den Bedingungen der privaten Firmen oder staatlichen Stellen zuzustimmen oder die Software oder den Dienst nicht zu nutzen.

Die algorithmische Konstruktion der Gesellschaft hat stark ökonomisch-rationale Züge. Statt zunehmender Kritik, genießen die Internet- und Technologiefirmen einen überraschenden Vertrauensvorschuss, obwohl Grundrechte der Nutzer:innen infrage gestellt werden. In öffentlichen Medien wird Digitalisierung mehrheitlich positiv konnotiert und die (möglichen) Vorteile immer wieder propagiert. Der Diskurs um Datenschutz und verwandte, mit Digitalisierung verbundene, Herausforderungen kommen nur zögerlich in der Öffentlichkeit an. Dabei besteht kein Wissens-, sondern ein Vollzugsdefizit. Das Problem liegt nicht in der wissenschaftlichen Erforschung und Kritik, sondern darin, die Ergebnisse auf der *tagtäglichen* Handlungsebene der Individuen zu artikulieren und zu nutzen.

Eine drängende Frage lautet weiterhin, wie Digitalisierung im Sinne von Bürger:innen und Nutzer:innen gestaltet wird. Es besteht grundsätzlich die Gefahr, dass sich die gesellschaftliche Konstruktion der Wirklichkeit immer weiter am Credo ökonomischer Algorithmisierung orientiert und ein schleichender Wandel einsetzt, der sich in kaum wahrnehmbaren inkrementellen Veränderungen von Normen und Werten äußert und digitale Souveränität erodiert. Es bedarf einer „Sozialisierung“ technischer Routinen statt einer zunehmenden Formalisierung sozialen Handelns. Statt den Lebensalltag der Menschen proaktiv zu informatisieren und digitale Hörigkeit zu forcieren, sollten Informatiker:innen Medien- und Systemgestalter für selbstbestimmte Lebenswelten sein [11].

6.2 Selbstermächtigung und verteilte Verantwortlichkeit

Da weniger auf die freiwillige Selbstkontrolle der Unternehmen und die zeitverzögerte Fremdkontrolle durch staatliche Gesetzgebung zu hoffen ist, stellt digitale Selbstermächtigung ein wichtiges Moment zur Herstellung und Festigung von

Privatheit dar. Dabei geht es nicht um eine neoliberalistische Verantwortungszuweisung, sondern um die Ermöglichung souveräner Entscheidungen, um die Entwicklung eines ‚digitalen Bauchgefühls' [49] und um Awareness der „menschlichen Firewall" – und zwar sowohl durch selbständige Aneignung als auch durch *externe* Unterstützung. Aufgrund asymmetrischer Machtverhältnisse in der Gesellschaft, speziell zwischen individuellen Nutzer:innen und Organisationen, deren Software und Plattformen genutzt werden, ist Selbstermächtigung stets auch gekoppelt an und abhängig von den organisationalen Handlungsparadigmen und Handlungsweisen [50]. Nutzer:innen sind scheinbar frei in ihrer Entscheidung, bspw. Facebook nicht zu nutzen. Andererseits wirken soziale Zwänge, die zur Nutzung „verpflichten". Verbote in Bezug auf den Betrieb solcher Plattformen sind wenig sinnvoll, da sie an Regulierungs- und Durchsetzungsdefiziten scheitern. Freilich könnte die Masse der Nutzer:innen Firmen unter Druck setzen, dafür scheinen die Gefahren jedoch zu wenig greifbar. Selbstermächtigung kann dann im Minimum bedeuten, soziale Plattformen zu nutzen und über die Folgen Bescheid zu wissen. Zugleich kann Selbstermächtigung bedeuten, freie Software als gleichwertige Alternative wählen zu können. Hierfür könnte der Staat in Verantwortung genommen werden.

Selbstermächtigung darf nicht professionellen Nutzer:innen vorbehalten und *Nischenkompetenz* sein. Selbstermächtigung bedeutet, bildungsferne Nutzer:innen zu berücksichtigen und zu überlegen, wie Mensch-Technik-Interaktionen plastischer gestaltet werden können, bspw. durch Visualisierungen (wie Verkehrsschilder), die beim Verständnis digitaler Prozesse helfen. Software ist für eine souveräne Nutzung zu entwickeln und mit Schutzfunktionen auszustatten. Digitale Bildung an den Schulen ist grundsätzlich sinnvoll, wenngleich auch hier über Formate und Inhalte bislang keine Einigkeit herrscht. Mögliche Schulfächer befreien jedoch nicht von der Notwendigkeit, breite Bevölkerungsschichten lebenslang weiterzubilden. Dazu gehören kompetenzbasierte Schulungsszenarien, bspw. Kurse an Volkshochschulen, und andere gruppenbasierte Formate bei denen auf Altershomogenität oder eben Altersmischungen geachtet wird, und Arbeitsplätze, an denen Awareness entwickelt und Selbstermächtigung gefördert wird. Nötig sind gesellschaftsweite Prozesse der Selbstermächtigung.

Digitale Selbstermächtigung ist ein kollektiver Prozess, der im Sinne einer ‚sozialen Innovation' die digitale Ordnung rekonfiguriert. Er erfordert die Bemühungen unterschiedlicher Akteure auf allen gesellschaftlichen Ebenen. Selbstermächtigung ist ein partizipativer Prozess, bei dem Konstruktion und Implementation von Technik an Bedarfen orientiert sind und das Subjekt im Mittelpunkt steht. Darüber hinaus ist die Partizipation weiterer Akteurinnen und Akteure

(aus Zivilgesellschaft, Politik, etc.) mitzudenken, um gemeinsam die soziotechnischen Rahmenbedingungen für souveräne Digitalität entlang der Maximen von Privatheit und Autonomie zu schaffen [51–53]. Wünschenswert sind eine bedarfsorientierte, zielgruppengerechte und gemeinwohlorientierte Konstruktion und ein entsprechender Einsatz digitaler Technik. Wichtig hierbei ist eine Kooperation mit den relevanten Zielgruppen, um Bedarfslagen *und* Dienstleistungen aufeinander abzustimmen. Algorithmen und algorithmenbasierte Entscheidungssysteme sind stets in gesellschaftliche Zusammenhänge eingebettet, die ebenfalls in den Blick zu nehmen sind [14]. So ist neben kompetenten Individuen ein starker Staat nötig, der seine Bürger:innen bspw. durch Gesetzgebung schützt. Digitale Selbstermächtigung konstituiert sich relational zwischen individuellen Voraussetzungen und personenexogenen Faktoren: Selbstermächtigung der Individuen ist nur in einer selbstermächtigenden Gesellschaft möglich. Dabei greifen Grade von Selbst- und Fremdermächtigung in einem Netz verteilter Verantwortung produktiv ineinander.

Literatur

1. Berger, P., Luckmann, T.: Die gesellschaftliche Konstruktion der Wirklichkeit, 19. Aufl. Fischer, Frankfurt a. M. (2003)
2. Strauss, A.L.: Continual Permutations of Action. Routledge, London (2008[1993]).
3. Rammert, W.: Technik – Handeln – Wissen. Springer VS, Wiesbaden (2016[2007]).
4. Passig, K.: Fünfzig Jahre Black Box (2017). https://www.merkur-zeitschrift.de/2017/11/23/fuenfzig-jahre-black-box. Zugegriffen: 6. Okt. 2020
5. Geitz, E., Vater, C., Zimmer-Merkle, S. (Hrsg.): Black Boxes – Versiegelungskontexte und Öffnungsversuche. De Gruyter, Berlin (2020)
6. Weyer, J.: Die Echtzeitgesellschaft. Campus, Frankfurt (2019)
7. Lobo, S.: Leben im Datenstrom. Bequemlichkeit schlägt Datensparsamkeit (2016). https://www.spiegel.de/netzwelt/web/zugriff-auf-daten-bequemlichkeit-schlaegt-sicherheit-kolumne-a-1114091.html. Zugegriffen: 6. Okt. 2020
8. Orwat, C., et al.: Software als Institution und ihre Gestaltbarkeit. Informatik Spektrum **33**(6), 626–633 (2010)
9. Just, N., Latzer, M.: Governance by algorithms: reality construction by algorithmic selection on the Internet. Media Cult. Soc. **39**(2), 238–258 (2017)
10. Enzensberger, H.M.: Das digitale Evangelium (2000). https://www.spiegel.de/spiegel/print/d-15376078.html. Zugegriffen: 6. Okt. 2020
11. Hellige, H.D.: Die Dialektik der informationellen Aufklärung. Ein Rückblick auf den Theoriediskurs von Informatik & Gesellschaft. In: Kühne, C. et. al. (Hrsg.) Per Anhalter durch die Turing-Galaxis, S. 55–60. Verlags-Haus Monsenstein und Vannerdat, Münster (2012)
12. Schirrmacher, F. (Hrsg.): Technologischer Totalitarismus. Suhrkamp, Berlin (2015)
13. Han, B.-C.: Psychopolitik. Neoliberalismus und die neuen Machttechniken. Fischer, Frankfurt a. M. (2014)

14. Zweig, K.A.: Algorithmische Entscheidungen: Transparenz und Kontrolle. In: Analysen und Argumente 338. Konrad-Adenauer-Stiftung e. V., Berlin (2019)
15. Schmidt, J.-H.: Social Media. Springer VS, Wiesbaden (2013)
16. Lewandowski, D.: Suchmaschinen verstehen. Springer, Berlin (2015)
17. Stalder, F.: Kultur der Digitalität. Suhrkamp, Berlin (2016)
18. Seyfert, R., Roberge, J. (Hrsg.): Algorithmuskulturen. Über die rechnerische Konstruktion der Wirklichkeit. Transcript, Bielefeld (2017)
19. Biniok, P.: Maschinenraum, Privatsphäre und Psychopolitik. Holistischer Datenschutz als Kombination von individueller Souveränität und kollektiver Gesetzgebung. Informatik Spektrum **43**(3), 220–226 (2020).
20. Karaboga, M., Masur, P., Matzner, T., Mothes, C., Nebel, M., Ochs, C., Schütz, P., Fhom, H.S.: Selbstdatenschutz. Fraunhofer ISI, Karlsruhe (2014)
21. SVRV: Digitale Souveränität. Gutachten des Sachverständigenrats für Verbraucherfragen. Sachverständigenrat für Verbraucherfragen beim Bundesministerium der Justiz und für Verbraucherschutz, Berlin (2017).
22. GI (Gesellschaft für Informatik): Schlüsselaspekte digitaler Souveränität (Arbeitspapier). Gesellschaft für Informatik e. V., Berlin (2020).
23. Biniok, P.: Emanzipierende Infrastrukturen. Wie digitale Teilhabe ausgebaut werden kann. Rosa-Luxemburg-Stiftung, Berlin (2017)
24. Matzner, T., Masur, P.K., Ochs, C., von Pape, T.: Do-It-Yourself Data Protection – Empowerment or Burden? In: Gutwirth, S., Leenes, R., de Hert, P. (Hrsg.): Data Protection on the Move, S. 277–305. Springer, Dordrecht (2016)
25. Akrich, M.: The De-Scription of Technical Objects. In: Bijker, W.E., Law, J. (Hrsg.) Shaping Technology/Building Society. Studies in Sociotechnical Change, S. 205–224. MIT Press, Cambridge/Mass. (1992)
26. Dosi, G.: Technological paradigms and technological trajectories: A suggested interpretation of the determinants and directions of technical change. Res. Policy **11**(3), 147–162 (1982)
27. Dickel, S.: Post-Technokratie. Prekäre Verantwortung in digitalen Kontexten. Soziale Systeme **19**(2), 282–303 (2014).
28. Bauman, Z., Lyon, D.: Daten, Drohnen. Disziplin. Ein Gespräch über flüchtige Überwachung. Suhrkamp, Berlin (2013)
29. RSL: Smarte Worte. Das kritische Lexikon der Digitalisierung. Rosa-Luxemburg-Stiftung, Berlin (2016)
30. Rammert, W., Schulz-Schaeffer, I. (Hrsg.): Können Maschinen handeln? Soziologische Beiträge zum Verhältnis von Mensch und Technik. Campus, Frankfurt a. M. (2002)
31. Coser, L.: Gierige Institutionen. Soziologische Studien über totales Engagement. Suhrkamp, Berlin (2015)
32. Mau, S.: Das metrische Wir: Über die Quantifizierung des Sozialen. Suhrkamp, Berlin (2017)
33. Pariser, E.: Filter Bubble: Wie wir im Internet entmündigt werden. Hanser, München (2012)
34. Grenz, T.: Mediatisierung als Handlungsproblem. Eine wissenssoziologische Studie zum Wandel materialer Kultur. Springer VS, Wiesbaden (2017)

35. Spiekermann, S., Korunovska, J., Langheinrich, M.: Inside the Organization: Why Privacy and Security Engineering Is a Challenge for Engineers. Proc. IEEE **107**(3), 600–615 (2019)
36. Nemitz, P., Pfeffer, M.: Prinzip Mensch. Freiheit und Demokratie im Zeitalter der Künstlichen Intelligenz. Dietz, Bonn, Macht (2020)
37. Müller-Lietzkow, J.: Quo Vadis Digitale Bildung? In: Friedrichsen, M., Bisa, P.-J. (Hrsg.): Digitale Souveränität Vertrauen in der Netzwerkgesellschaft, S. 305–323. Springer VS, Wiesbaden (2016)
38. Egloff, D.: Digitale Demokratie: Mythos oder Realität? Auf den Spuren der demokratischen Aspekte des Internets und der Computerkultur. Westdeutscher Verlag, Opladen (2002)
39. Castells, M.: Jahrtausendwende. Das Informationszeitalter, Bd. 3. Campus, Opladen (2003)
40. Sevignani, S.: Krise der Privatheit. In: Hahn, K., Langenohl, A. (Hrsg.): Kritische Öffentlichkeiten – Öffentlichkeiten in der Kritik, S. 237–254. Springer VS, Wiesbaden (2017)
41. Daniljuk, M.: Die neuen Gatekeeper. Google und Facebook in den kybernetischen Kapitalismus. Rosa-Luxemburg-Stiftung. Berlin, Mit Apple (2016)
42. Zuboff, S.: Das Zeitalter des Überwachungskapitalismus. Campus, Frankfurt a. M. (2018)
43. Jäger, W.: Neue Rolle öffentlicher Rechenzentren für Bürger-Datenschutz und Bürger-Befähigung. In: Friedrichsen, M., Bisa, P.-J. (Hrsg.) Digitale Souveränität Vertrauen in der Netzwerkgesellschaft, S. 23–34. Springer VS, Wiesbaden (2016)
44. Krenn, K., Tiemann, J., Hunt, S.S.: Datenachtsamkeit – ein neuer(licher) Blick auf den Selbstdatenschutz. Fraunhofer-Institut für Offene Kommunikationssysteme, Berlin (2019)
45. Selke, S.: Lifelogging. Digitale Selbstvermessung und Lebensprotokollierung zwischen disruptiver Technologie und kulturellem Wandel. Springer VS, Wiesbaden (2016)
46. Warschauer, M.: Technology and social inclusion. MIT Press, Cambridge/Mass, Rethinking the digital divide (2003)
47. Kurz, C., Rieger, F. Die Datenfresser. Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen. Fischer, Frankfurt a. M. (2011)
48. Lanier, J.: You are not a gadget. A manifesto. Alfred A. Knopf, New York (2010)
49. Müller, L.-S.: Das digitale Bauchgefühl. In: Friedrichsen, M., Bisa, P.-J. (Hrsg.) Digitale Souveränität Vertrauen in der Netzwerkgesellschaft, S. 267–285. Springer VS, Wiesbaden (2016)
50. Rost, M.: Zur Soziologie des Datenschutzes. DuD – Datenschutz und Datensicherheit **37**(2) 85–91 (2013).
51. Le Dantec, C., DiSalvo, C.: Infrastructuring and the formation of publics in participatory design. Soc. Stud. Sci. **43**(2), 241–264 (2013)
52. Pipek, V., Wulf, V.: Infrastructuring: Toward an Integrated Perspective on the Design and Use of Information Technology. Journal of the Association for Information Systems **10**, 447–473 (2009)
53. Hagendorff, T., Geminn, C., Lamla, J., Karaboga, M., Krämer, N., Nebel, M., Uhlmann, M.: Risiken künstlicher Intelligenz für die menschliche Selbstbestimmung. Fraunhofer ISI, Karlsruhe (2020)

Zum Datenschutz gestupst? Gestaltungsorientierte Entwicklung von Privacy Nudges vor dem Hintergrund ethischer und rechtlicher Leitlinien

Sofia Marlena Schöbel, Sabrina Schomberg, Torben Jan Barev, Thomas Grote, Andreas Janson, Gerrit Hornung und Jan Marco Leimeister

S. M. Schöbel (✉)
Juniorprofessur für Wirtschaftsinformatik, Universität Osnabrück, Osnabrück, Deutschland
E-Mail: sofia.schoebel@uni-osnabrueck.de

S. Schomberg · G. Hornung
Fachgebiet für Öffentliches Recht, IT-Recht und Umweltrecht, Universität Kassel, Kassel, Deutschland
E-Mail: sabrina.schomberg@uni-kassel.de

G. Hornung
E-Mail: gerrit.hornung@uni-kassel.de

T. Grote
Arbeitsgruppe Ethik und Philosophie der künstlichen Intelligenz, Universität Tübingen, Tübingen, Deutschland
E-Mail: thomas.grote@uni-tuebingen.de

A. Janson · J. M. Leimeister
Universität St. Gallen, Institut für Wirtschaftsinformatik (IWI-HSG), Gallen, Schweiz
E-Mail: andreas.janson@unisg.ch

J. M. Leimeister
E-Mail: janmarco.leimeister@unisg.ch

T. J. Barev · J. M. Leimeister
Fachgebiet für Wirtschaftsinformatik, Universität Kassel, Kassel, Deutschland
E-Mail: torben.barev@uni-kassel.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_18

Zusammenfassung

Die Digitalisierung verändert unsere Gesellschaft, die Art wie wir miteinander kommunizieren und wie wir arbeiten. Dabei birgt Digitalisierung nicht nur Vorteile, sondern führt auch dazu, dass jedes Individuum durch sein Agieren in der digitalen Welt Datenspuren hinterlässt. Diese Daten werden gesammelt, aggregiert und ausgewertet, und das vielfach, ohne dass sich Individuen dessen bewusst sind. Hier kann das sogenannte Privacy Nudging genutzt werden, durch das Nutzende „angestupst" werden, um ihr Verhalten so zu verändern, dass sie ihre eigenen Daten besser schützen. Bei der Gestaltung von Nudging Konzepten gibt es zahlreiche rechtliche, ethische und soziotechnische Hürden, die es zu berücksichtigen gilt. Hierzu existieren bisher keine einheitlichen Richtlinien und Empfehlungen. Entsprechend präsentiert der Beitrag eine integrative soziotechnische Gestaltungsperspektive für digitale privacy Nudges, indem Technik, Ethik und Recht nicht mehr nur isoliert betrachtet werden.

Schlüsselwörter

Privacy Nudging • Design von digitalen Benutzeroberflächen • Digitale Entscheidungsarchitekturen • Datenschutzrecht • Ethik • Soziotechnik

1 Einleitung und Motivation

Aktuellen Prognosen zufolge werden im Jahre 2022 60 % des weltweiten Bruttoinlandsprodukts mithilfe digitaler Technologien erbracht [1]. Die Digitalisierung birgt hierbei nicht nur Vorteile, sondern führt auch dazu, dass jedes Individuum durch sein Agieren in der digitalen Welt Datenspuren hinterlässt. Diese Daten werden gesammelt, aggregiert und ausgewertet, und das vielfach, ohne dass sich Individuen dessen bewusst sind [2]. Dementsprechend ergeben sich nicht nur für Individuen Risiken, sondern auch für Unternehmen. Für Individuen wird es vermehrt schwieriger, zu entscheiden und zu erkennen, welche Daten sie gefahrlos mit anderen teilen können. Gleichzeitig sind Unternehmen durch die neue Datenschutz-Grundverordnung stärker in der Pflicht, ihre Mitarbeitenden in Bezug auf einen sensiblen und nachhaltigen Umgang mit Daten zu schulen und aufmerksam zu machen. Auch durch die fließenden Grenzen zwischen Arbeit und Privatleben, die durch die Digitalisierung immer stärker verschwimmen, wächst die Notwendigkeit für Lösungen, die den sparsamen Umgang mit Daten unterstützen.

Es bedarf somit innovativer Konzepte, die sowohl die Chancen der Digitalisierung ausschöpfen als auch gleichzeitig gewährleisten, dass seitens der Individuen sorgsam mit Daten umgegangen wird. Um beides zu fördern, kann das sogenannten Privacy Nudging wertvolle Unterstützung bieten. Privacy Nudging beeinflusst das Verhalten in digitalen Umgebungen dahingehend, dass datenschutzfreundlichere Entscheidungen durch Individuen getroffen werden [3, 4]. Das Konzept des Privacy Nudgings hat sich bereits in vielen Kontexten als sinnvoll und effektiv erwiesen. Es kann beispielsweise eingesetzt werden, um Individuen vor versehentlicher Datenpreisgabe zu schützen [5] oder sie dazu zu bewegen, sorgsamer in sozialen Medien zu agieren [6]. Ein Nudge dient dazu, Individuen „anzustupsen", um sie durch den Einsatz von Steuerungselementen und ohne jegliche Einschränkung dazu zu bewegen, ihr Verhalten zu ändern [7]. Das Konzept des Privacy Nudgings ist besonders relevant, da Individuen sich oft gar nicht bewusst sind, in welcher Form die von ihnen preisgegebenen Daten verarbeitet und weiter genutzt werden.

Allerdings werden die dem Nudging zugrunde liegenden kognitiven Mechanismen nicht nur dazu verwendet, Individuen zu schützen. Durch den Einsatz von sogenannten „Dark Pattern" können Individuen besonders bei Online-Einkäufen dazu angeregt werden, gezielt Entscheidungen zu treffen, die zwar aus Sicht der Verkäufer vorteilhaft sind, jedoch ein Individuum zu einem eigentlich nicht beabsichtigten Vertragsschluss oder zum Akzeptieren eines überhöhten Preises manipulieren (beispielsweise [8]). Ein prominentes Beispiel hierfür ist das Framing von Entscheidungen bei der Annahme von Internet-Cookies. Dieses Framing kann auf zwei Arten erfolgen – zur Unterstützung der maximalen Sammlung von Nutzerdaten oder zur Minimierung dieser Sammlung, indem die rechtlich und ethisch konforme Alternative geframed wird. In der Praxis lässt sich oftmals beobachten, dass mittels des ersteren Vorgehens gesetzliche Anforderungen ausgehebelt werden. So werden zwar – entsprechend den rechtlichen Vorgaben – datenschutzfreundliche Defaults vorgegeben, allerdings framen vermehrt Internetplattformen die Entscheidung so, dass Individuen eher weiteren Cookies zustimmen als den eigentlichen Default beizubehalten.

Die alternative und manipulative Gestaltungsrichtung zu Ungunsten von Individuen verdeutlicht, dass bei der Gestaltung von digitalen Nudges Vielzahl von verschiedenen Aspekten eine Rolle spielen [9, 10]. So werden Nudges in ein Informationssystem integriert und an bestimmte Entscheidungsarchitekturen sowie einzelne Nutzende angepasst. Bei der Gestaltung von Nudges gilt es auch die rechtliche Perspektive zu berücksichtigen, die besonders im Hinblick auf die Gefahren, die beispielsweise durch „Dark Pattern" entstehen können, gewährleisten sollte, dass Individuen nicht entgegen gesetzlicher Bestimmungen negativ beeinflusst werden. Schlussendlich gilt es im Sinne von Individuen eine ethische

Perspektive bei der Gestaltung von Nudges zu berücksichtigen, damit diese nicht in ihrer Autonomie eingeschränkt werden. In der bisherigen Forschung und Praxis gibt es kaum Ansätze, die eine konsolidierte Betrachtungsweise aller drei Disziplinen realisieren. Darauf aufbauend fehlen oftmals Leitlinien die Forscher und Praktiker dabei unterstützen, das Wissen von mehreren Disziplinen bei der Gestaltung von digitalen Nudges zu vereinigen. Zwar gibt es methodische Ansätze [9], die bei der Gestaltung von Nudging Konzepten helfen, diese greifen jedoch die einzelnen Disziplinen nicht auf, die für die Gestaltung von Relevanz sind.

Dieser Beitrag präsentiert eine integrative soziotechnische Gestaltungsperspektive für Privacy Nudging, indem Technik, Ethik und Recht nicht mehr nur isoliert betrachtet werden. Dies dient einerseits dazu, Entwicklern eine Hilfestellung in Bezug auf den Einsatz und die Gestaltung von Privacy Nudges geben zu können. Andererseits soll aufgezeigt werden, welche Möglichkeiten und Grenzen bei der Gestaltung von Privacy Nudges bestehen. Hierdurch sind wir in der Lage, theoretische Empfehlungen zu geben, wie unter der Berücksichtigung von verschiedenen Perspektiven tiefergehende Analysen zum Einsatz von Privacy Nudges durchgeführt werden können. Aus einer praktischen Perspektive kann der Beitrag demonstrieren, welche Modifikationen von Privacy Nudges notwendig sind, damit nicht nur eine systemseitige, nutzerzentrierte Anpassung vorgenommen wird, sondern auch eine rechtlich unbedenkliche und ethisch angemessene Gestaltung von Privacy Nudges erfolgt.

2 Theoretischer Hintergrund

Nachfolgend widmet sich dieser Beitrag den theoretischen Hintergründen, die wichtig sind, um die verschiedenen Perspektiven, die verglichen werden, nachvollziehen zu können. Dazu wird in einem ersten Schritt der Begriff des digitalen Nudgings aufgegriffen. Darauf aufbauend wird eine soziotechnische, ethische und rechtliche Sichtweise auf die Gestaltung von Privacy Nudges erläutert.

2.1 Das Konzept des digitalen Nudgings

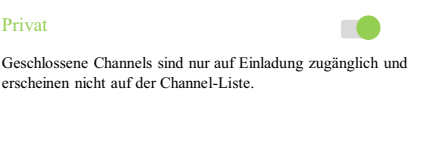
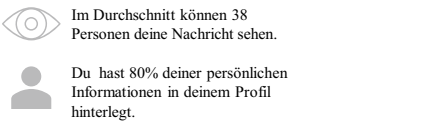
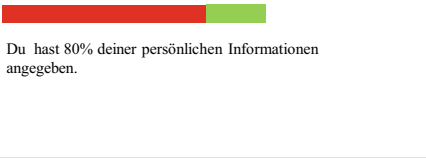
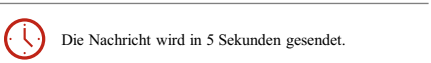
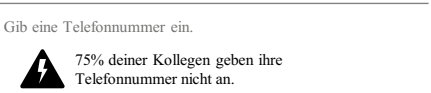
Die Gestaltung von digitalen Nudges verfolgt das Ziel, Individuen zu ihrem Vorteil in eine bestimmte Richtung zu „stupsen“ und zwar durch den Einsatz von Elementen, wie beispielsweise dem farblichen Hervorheben von datenschutzfreundlichen Optionen (sog. Framing). Nudges können dabei nicht nur offline (wie

durch den Einsatz einer Lebensmittelampel) sondern auch online (in Form derartiger farblicher Hervorhebungen, Voreinstellungen oder anderer Designelemente) verwendet werden. Nudges kommen vor allem dann zum Einsatz, wenn viele Entscheidungsalternativen verfügbar sind oder eine Entscheidung sehr komplex ist [11]. Digitale Nudges sind speziell für das Web entwickelt worden. Weinmann et al. [4] definieren digitale Nudges als Anwendung von Elementen für Benutzeroberflächen, um Wahlmöglichkeiten von Nutzenden in digitalen Umgebungen zu unterstützen [4]. Meske und Potthoff [12] erweitern diese Definition um die Aspekte der freien Entscheidung sowie der Nutzung von Informations- und Interaktionselementen. Interaktionselemente oder allgemein und fortan Nudge Elemente genannt, können unterschiedlich ausgeprägt sein (siehe Tab. 1).

Oftmals treffen Individuen, die in einer online Umgebung agieren, Entscheidungen unter Stress und Zeitdruck. Da Individuen in online Umgebungen zahlreiche Informationen gleichzeitig verarbeiten müssen [9], geben sie oft private Daten preis, die sie unter anderen Umständen nicht zwangsläufig weitergegeben hätten. Diesbezüglich können digitale Nudges einerseits Modifizierungen hinsichtlich des präsentierten Inhalts vornehmen. Andererseits können sie die Art und Weise der Visualisierung modifizieren bspw. das Ändern des Designs einer Benutzeroberfläche [13]. Digitale Nudges können Individuen unterstützen, indem sie ihnen relevante Informationen in kurzer Zeit übersichtlich darstellen und diese vor der Preisgabe von privaten Daten schützen.

Digitale Nudges sind in Entscheidungsarchitekturen integriert und werden immer dann relevant, wenn Individuen Entscheidungen treffen müssen. Entscheidungen werden dabei häufig nicht auf Basis von rationalen Überlegungen getroffen, sondern auf Basis von Heuristiken, welche den Entscheidungsprozess systematisieren [14]. Ein Erklärungsansatz dafür ist die Duale Prozesstheorie von Kahnemann, die besagt, dass Individuen zwei Denksysteme benutzen. System 1 repräsentiert unsere Intuition oder unseren unbewussten „Autopiloten“. System 2 hingegen drückt sich durch unsere bewusste Planung und Kontrolle aus. Beide Systeme sind gleichzeitig aktiv und arbeiten in der Regel reibungslos zusammen. Zwei Systeme sind notwendig, um die Informationsfülle in der heutigen (digitalen) Welt besser einschätzen und gezielte Entscheidungen treffen zu können [15]. Im Alltag hat der Einzelne jedoch selten genug Zeit und Informationen, um alle Alternativen vollständig zu bewerten. Aus der Anwendung von Heuristiken können daher Biases, sogenannte Verzerrungen der Entscheidung, resultieren. Nudges wiederum bauen auf vertraute Verhaltensmuster der Individuen, welche durch Heuristiken und Biases entstehen, auf. Diesen Aspekten folgend, wird nachfolgend zum Konzept des digitalen Nudgings aus drei Sichtweisen Bezug genommen.

Tab. 1 Nudge Elemente

Name	Beschreibung	Visualisierung
Voreinstellung	Standardeinstellungen, welche meist als voreingestellte Optionen bevorzugt und nur selten verändert werden	
Farbliche Elemente	Farbelemente können als Framing-Nudge verwendet werden, wobei farbliche Hinterlegungen die Aufmerksamkeit auf ausgewählte Elemente lenken	
Information	Informiert Nutzende darüber, was für Konsequenzen die Weitergabe von Daten haben kann	
Rückmeldung	Die Bereitstellung von Rückmeldungen als Privacy Nudge weist ein Individuum auf sein bisheriges Nutzungsverhalten hin	
Zeitverzögerung	Dem Nutzenden wird ein Zeitfenster eingeräumt, in dem er seine Entscheidung überdenken kann	
Soziale Normen	Auf diesem Prinzip der sozialen Normen basiert die Wirkung von sogenannten sozialen Nudges die zeigen, wie andere sich verhalten haben oder würden	

Eine genaue Einordnung und Einstufung aus rechtlicher Sicht kann der folgenden Publikation entnommen werden: Schomberg, S.; Barev, T. J.; Janson, A. & Hupfeld, F. (2019): Ansatz zur Umsetzung von Datenschutz nach der DSGVO im Arbeitsumfeld: Datenschutz durch Nudging. In: Datenschutz und Datensicherheit – DuD, 2019, 774–780.

2.2 Die ethische Sichtweise

Typischerweise werden Nudges als eine Art paternalistischer Akt verstanden. Paternalistische Handlungen sind Eingriffe, die darauf abzielen, die Interessen, die Werte oder das Wohlergehen einer bestimmten Person zu fördern, dabei jedoch zugleich ihre Autonomie verletzen [16].

Solche paternalistischen Handlungen treten in vielen Bereichen des persönlichen und öffentlichen Lebens auf: Eine Regierung kann beschließen, eine Zuckersteuer einzuführen, um Fettleibigkeit unter den Bürgern entgegenzuwirken, ein Arzt beschließt, die Wahrheit über den Gesundheitszustand eines Patienten zurückzuhalten, oder Eltern verlangen von ihren Kindern, ihre Hausaufgaben zu erledigen, bevor sie fernsehen dürfen. Selbst wenn diese paternalistischen Handlungen im Interesse von Nutzenden durchgeführt werden, bleiben Bedenken hinsichtlich ihrer moralischen Legitimität bestehen. In erster Linie verletzen sie die Entscheidungsfreiheit einer Person. Selbst wenn es einer Person beispielsweise besser gehen könnte, wenn sie gesündere Lebensmittel isst, besteht die Gefahr, dass sie dies nicht aus freien Stücken tut, sondern gerade durch den Akt der gesunden Ernährung ihre eigene rationale Entscheidungsfreiheit missachtet. Geht man nicht davon aus, dass paternalistische Handlungen niemals zulässig sein können, so benötigen sie jedenfalls eine starke moralische Rechtfertigung.

Aus Sicht der politischen Entscheidungsträger besteht der besondere Reiz von Nudges darin, dass sie zwar als eine Art paternalistischer Akt angesehen werden können, der aber gleichzeitig die Wahlfreiheit einer Person nicht verletzt [7]. Die Grundidee des Nudgings ist es, die Umgebung zu manipulieren, um es einer Person zu erleichtern, das zu tun, was für sie von Vorteil ist. Wie wir bereits im vorherigen Abschnitt diskutiert haben, wurde die Nudge-Theorie von Studien in der Verhaltensökonomie inspiriert und setzt die Duale Prozesstheorie Kahnemanns voraus [15].

Ein paradigmatischer Fall von Nudging ist das Beispiel einer Cafeteria, in der die Reihenfolge der Lebensmittel so angeordnet wird, dass Menschen wahrscheinlich eher gesunde statt ungesunde Lebensmitteloptionen wählen. Alternativ kann man auch kleinere Teller in der Cafeteria verwenden, was die Menge der konsumierten Lebensmittel reduziert. Die Quintessenz ist jedoch, dass Personen, die es vorziehen, ungesunde Lebensmittel zu essen, dies immer noch tun können, auch wenn sie einige zusätzliche Anstrengungen unternehmen müssen (d. h. in diesem Beispiel möglicherweise einige zusätzliche Schritte gehen). Übertragen auf den Bereich des Privacy Nudgings könnte sich ein Nudge Designer etwa den Umstand zunutze machen, dass Menschen dazu neigen, kognitive Anstrengungen zu vermeiden, weshalb sie nur selten die Standardeinstellungen in einem

Softwareprodukt ändern [17]. Dies ist selbst dann der Fall, wenn nur ein paar Klicks erforderlich sind und auch wenn eine Anpassung den Schutz ihrer Privatsphäre signifikant verbessern würde. Die gezielte Gestaltung der digitalen Entscheidungsarchitektur hat somit erheblichen Einfluss auf die Gewährleistung ihrer Privatsphäre.

Auch wenn Nudges theoretisch dem Nudgee (die Person unter Einfluss des Nudges) seine Entscheidungsfreiheit lassen, bleibt unklar, wo die Grenze zwischen Nudges zu ziehen ist, die die Autonomie einer Person ausreichend respektieren und denjenigen, die übermäßig manipulativ wirken. Dieses Problem wird besonders deutlich bei digitalen Technologien. Während wir die Debatte über den Konflikt zwischen Nudges und Autonomie in ihrer Gesamtheit schwer in diesem Text klären können, muss zumindest der Begriff der Manipulation genauer betrachtet werden [18, 19].

Wenn man etwa nur solche Handlungen als manipulativ behandelt, die die rationalen Fähigkeiten einer Person vollständig umgehen oder untergraben, so führt dies zu einem allzu engmaschigen Konzept. Dies zeigt schon das Beispiel von Fake News, die rational überzeugend wirken sollen, gleichzeitig aber eine Person in die Irre führen. Fake News sind aber ohne Zweifel moralisch problematisch, da sie Personen dazu verleiten, sich fehlerhaftes Wissen anzueignen. Darüber hinaus sind einige Fälle nicht-rationaler Überredung (z. B. abschreckende Bilder auf Zigarettenpackungen) in der Regel entweder nicht als manipulativ erdacht oder werden zwar als manipulativ wahrgenommen, aber für moralisch zulässig befunden. Der Grund hierfür ist, dass es dem Wohle der Person dient (es senkt z. B. ihr Krebsrisiko). Aus diesem Grund gehen wir davon aus, dass das Hauptkriterium für die Bewertung der manipulativen Eigenschaften von Nudges nicht darin bestehen sollte, durch welche kognitiven Mechanismen sie herbeigeführt wurden, sondern ob die manipulative Handlung einem Nudgee schadet, z. B. indem man ihn zwingt, einen ausbeuterischen Vertrag einzugehen [20].

In der ethischen Debatte werden Nudges in aller Regel als Mittel zur Verbesserung der öffentlichen Ordnung und damit als staatliches Instrument diskutiert. Dies führt zu der Frage, ob sich die Bewertung ändert, wenn stattdessen ein Unternehmen seine Kunden oder Mitarbeiter nudged (wobei Nudging hier in einem dezidiert paternalistischen Sinne verstanden wird). Wenn überhaupt, haben Regierungen oder staatliche Institutionen das Recht sich in das Leben der Bürger einzumischen und zu nudgen, da staatliche Institutionen besondere rechtliche und ethische Verpflichtungen gegenüber ihren Bürgern haben. Unternehmen haben zwar Verpflichtungen gegenüber Kunden (z. B. im Bereich der Produktsicherheit oder des Verbraucherschutzrechts) und ihren Mitarbeitern (z. B. Arbeitssicherheit). Dennoch sind sie vor allem daran interessiert, Profit zu machen. Auch wenn

ein Nudge mit den besten Absichten entworfen wird, sind die Beweggründe dahinter gemischt – der Nudge ist womöglich Teil des Geschäftsmodells. Angesichts des jüngsten Aufschwungs von Unternehmen, die einen nachhaltigeren Lebensstil bei ihren Kunden fördern wollen, dürfte die Ethik in Zukunft zunehmend im Rahmen von Nudging oder Unternehmenspaternalismus Beachtung finden.

2.3 Die rechtliche Sichtweise

Um die für das digitale Nudging relevanten rechtlichen Fragestellungen zu klären, schlägt Gerg eine zusätzliche rechtliche Definition des Begriffs Nudging vor [21]. Er kommt zu dem Schluss, dass Nudging ohne wirtschaftliche Begriffe als gezielte, möglicherweise sogar unbewusste Willensmanipulation beschrieben werden kann. Das Gesetz verknüpft in der Regel positive oder negative rechtliche Konsequenzen mit einem bestimmten Verhalten. Die Personen können dann entscheiden, ob sie sich an die gesetzlichen Vorgaben halten oder nicht. Nudging beginnt jedoch früher und beeinflusst bereits den Willen eines Nutzenden selbst. Die Entscheidungen der Nutzenden werden daher in einer Weise beeinflusst, die dem Gesetz nicht bekannt ist [21]. Diese Definition verkennt jedoch, dass Verbote und Gebote im Recht durchaus selbst Instrumente zur Verhaltenssteuerung sind [22]. Außerdem gibt es gesetzliche Normen, welche Nudging durch Private anordnen (z. B. Art. 25 Abs. 2 DSGVO). Daher ist weniger eine juristische Definition, sondern eher eine juristische Betrachtung der Sachverhalte notwendig, die nach der verhaltensökonomischen Definition als Nudging eingeordnet werden.

Nicht nur aus ethischer, sondern auch aus rechtlicher Sicht besteht eines der größten Probleme von Nudges darin, dass sie (libertär) paternalistisch sind. Staatliche Bevormundung ist in der Regel unzulässig, weil sie gegen den aus dem Rechtsstaatsprinzip abgeleiteten Grundsatz der Verhältnismäßigkeit verstößt [21]. Kant bezeichnete eine „väterliche Regierung (imperium paternale)“ sogar als den "größten denkbaren Despotismus" [23]. Der Begriff des Staatspaternalismus und vor allem seine Kritik ist ein klassisches Thema der Rechtswissenschaft. In jüngerer Zeit spiegelte sich das Problem der Bevormundung zunächst in der Frage der rechtlichen Zulässigkeit des „Schutzes der Menschen vor sich selbst“ wider, die in den 1990er Jahren besonders intensiv diskutiert wurde [24]. Es besteht ein breiter Konsens darüber, dass paternalistische Handlungen nur legitimiert werden können, wenn neben den Interessen der Betroffenen auch die Interessen der Allgemeinheit oder Dritter beeinträchtigt werden (z. B. [25, 26]. Auch deutsche Gerichte lehnen Einschränkungen der Freiheit verantwortlicher Erwachsener regelmäßig ab, es sei denn, die Allgemeinheit oder Dritte sind ebenfalls negativ

betroffen [27]. Das Bundesverfassungsgericht betont: „Der Staat hat […] nicht die Aufgabe, seine Bürger zu 'bessern' und deshalb auch nicht das Recht, ihnen die Freiheit zu entziehen, nur um sie zu 'bessern', ohne dass sie sich selbst oder andere gefährdeten, wenn sie in Freiheit blieben" [21, 28].

Doch Nudging ist nicht das Gleiche wie Paternalismus [21]. Der libertäre Aspekt, der von Thaler und Sunstein gefordert wird, besteht auf die Wahrung oder sogar Verbesserung der Wahlfreiheit des Individuums [7]. Inspiriert durch das Konzept von Thaler und Sunstein wird Paternalismus, insbesondere in Form libertärer Bevormundung, in der deutschen Rechtswissenschaft immer mehr diskutiert [29, 30]. Dabei scheint Juristen der Umgang mit dieser Mischform und ihre Bewertung schwerer zu fallen als Ethikern oder Vertretern anderer Disziplinen. Denn Juristen wollen einen Nudge in der Regel als paternalistisch oder libertär einordnen, um ihn besser beurteilen zu können [21].

Auch aus rechtlicher Sicht kann Nudging durch Private (z. B. Arbeitgeber oder Dienstleister) besondere Fragen aufwerfen. Zwar ist nur der Staat unmittelbar an Grundrechte gebunden [31]. Diese wirken sich aber auf das Verhältnis zwischen Privatpersonen aus, da alle Gesetze verfassungsrechtlichen Vorgaben entsprechen müssen und insbesondere Generalklauseln Einbruchstellen für den Rechtsgehalt der Grundrechte sind (mittelbare Drittwirkung; grundlegend [32]).

Sofern Private in digitalen Umgebungen nudgen, müssen sie einerseits datenschutzrechtliche Vorgaben eingehalten, andererseits könnten durch Nudges auch datenschutzrechtliche Vorgaben umgesetzt werden (s. a. [27]). Der Rechtsrahmen für digitales Nudging besteht im Wesentlichen aus den in Art. 5 DSGVO kodifizierten Grundsätzen für die Verarbeitung (insb. Grundsatz der Transparenz in Art. 5 Abs. 1 lit. a DSGVO, welcher in den Normen zu den Rechten der betroffenen Personen in Art. 12 ff. DSGVO weiter konkretisiert wird) und den Anforderungen an den Datenschutz durch Technikgestaltung und Voreinstellungen gemäß Art. 25 DSGVO. Sobald es um maßgeschneiderte Nudges geht, müssen auch die Beschränkungen für die automatisierte Entscheidung im Einzelfall (Art. 22 DSGVO i.V.m. der Legaldefinition in Art. 4 Nr. 4 DSGVO) berücksichtigt werden. Die Datenschutzgrundsätze enthalten jedoch eine Reihe undefinierter Rechtsbegriffe und legen daher nur allgemeine Leitlinien fest, die dann in den weiteren Vorschriften der DSGVO konkretisiert werden [33].

Art. 25 Abs. 2 Satz 1 DSGVO besagt, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen muss, um sicherzustellen, dass durch Voreinstellungen grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind. Daher können Nudges in Form von Voreinstellungen, die den

Datenschutz fördern sollen, als Maßnahmen gemäß Art. 25 Abs. 2 DSGVO verstanden werden [24]. Verstöße können mit hohen Geldstrafen nach Art. 83 Abs. 4 DSGVO geahndet werden.

Andere Ausgestaltungsarten von Nudges (z. B. Framing, soziale Normen, Zeitverzögerung oder Feedback), die den Datenschutz oder die Privatsphäre fördern, können als Maßnahmen gemäß Art. 25 Abs. 1 DSGVO angesehen werden. Dieser verpflichtet den Verantwortlichen, geeignete technische und organisatorische Maßnahmen zu ergreifen, die auf die wirksame Umsetzung der Datenschutzgrundsätze ausgelegt sind. Privacy Nudges können einen wichtigen Beitrag zur Festlegung und Umsetzung der abstrakten Anforderungen des Art. 25 DSGVO leisten, aber um einen umfassenden Datenschutz zu gewährleisten, müssen weitere technische und organisatorische Maßnahmen getroffen werden [5].

Gemäß Art. 22 Abs. 1 DSGVO hat die betroffene Person „das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“. Profiling ist dabei eine automatisierte Verarbeitung der erhobenen Daten mit dem Ziel, bestimmte persönliche Aspekte zu bewerten (siehe Art. 4 Nr. 4 DSGVO). Dies würde bei personalisierten Nudges zutreffen, da sie ein Profil erfordern, um Annahmen darüber zu treffen, was die Nutzenden am besten nudgen würde. Hingegen ist zweifelhaft, ob es bei libertären Nudges überhaupt zu einer Entscheidung des Verantwortlichen kommt, da dem Nudgee immer die Möglichkeit offenbleibt, sich gegen die beabsichtigte Verhaltensweise zu entscheiden. Stellt man auf diesen Aspekt ab, so ist Art. 22 DSGVO auch auf personalisierte Nudges nicht anwendbar, da die Nutzenden weiterhin selbst entscheiden (siehe für das parallele Beispiel der personalisierten Werbung: [34]). Denkbar erscheint zwar, dass es durch eine sehr genaue Personalisierung für die Individuen schwer werden könnte, Nudges zu widerstehen. In diesem Fall ließe sich vertreten, dass die Entscheidung doch auf das Individuum verlagert wird und ihr zumindest eine Beeinträchtigung innewohnt, die einer rechtlichen Wirkung gleichkommt, weil das Individuum nach persönlicher Empfindung keine Wahlmöglichkeit mehr hat. Gerade im Bereich des Privacy Nudgings ist dies jedoch regelmäßig nicht der Fall. Wird die oder der Nutzende beispielsweise durch einen guten Privacy Nudge dazu bewogen ein Bild nicht frei im Internet zu teilen, sondern den Empfängerkreis auf enge Freunde zu beschränken, so kommt es zu keiner erheblichen Beeinträchtigung für Nutzende. Dies gilt zumindest dann, wenn der Nudge die weiteren Anforderungen des Datenschutzrechts (v. a. hinsichtlich der Transparenz) einhält.

2.4 Die soziotechnische Sichtweise

Die soziotechnische Perspektive integriert sowohl die ethische als auch die rechtliche Perspektive und betrachtet, wie man die technische Umsetzung und das menschliche Agieren in digitalen Umgebungen gestalten kann [41]. Diesbezüglich möchte die soziotechnische Sichtweise das Verhalten von Individuen besser verstehen und Rückschlüsse ziehen, wie man Systeme entsprechend den Bedürfnissen von Individuen besser gestalten kann. Mit Blick auf digitale Nudges geht es entsprechend darum, diese so zu gestalten, dass sie für die Individuen die bestmöglichen Effekte haben und sie zu einer Handlung bewegen, die sowohl rechtlich als auch ethisch konform ist. Da heute immer mehr Entscheidungen online getroffen werden, wie Einkäufe, Urlaubsbuchungen, Versicherungen usw., wird Nudging auch im digitalen Kontext immer wichtiger [9].

Aus einer soziotechnischen Perspektive wird Nudging als eine Form der Kommunikation zwischen verschiedenen Interessengruppen beschrieben, welche das Ziel verfolgt, autonome Urteile und Handlungen von Individuen zu beeinflussen. Dabei ist zu berücksichtigen, dass zwar ethische und rechtliche Fragestellungen relevant sind, aber nicht immer in Gänze zum Vorteil der Individuen umgesetzt werden (Dark Pattern). Beim Privacy Nudging sollen Nutzende von Informationssystemen dazu gebracht werden, die Datenschutzentscheidungen besser an ihre Präferenzen anzupassen, um sie in ihrem Verhalten zu unterstützen. – hier gilt der Fokus mehr oder weniger der systemisch passenden und geeigneten Gestaltung eines Systems und eines inkludierten Nudges. Studien haben gezeigt, dass vor allem Nutzende digitaler Systeme aufgrund kognitiver, emotionaler und sozialer Faktoren oft irrational handeln [3, 7]. Im Alltag haben Individuen selten genug Zeit und Informationen, um alle Alternativen vollständig auszuwerten. Hier sind für Individuen rechtliche und ethische Themenstellungen ggf. eher nicht primär von Relevanz und werden daher nicht beachtet. Durch die Hervorhebung „populärer“ Entscheidungen wird sozialer Druck auf den Einzelnen ausgeübt, was zu Entscheidungen führt, die manchmal nicht wirklich widerspiegeln, was Nutzende auf Online-Plattformen wirklich wollen.

In der Forschung werden hierzu Ideen ausgetauscht, wie man durch neuartige Techniken im Zusammenhang mit der Ausnutzung der Prinzipien des Nudgings vor allem ungeplantes Verhalten induzieren kann [35]. Es stellt sich die Frage, wie man eine entsprechende Gestaltung von digitalen Privacy Nudges sinnvoll vornehmen kann, sodass die Daten der Nutzenden aktiv geschützt werden. Aus soziotechnischer Sicht ist ebenso relevant, wie man es schafft, mehrere Disziplinen so miteinander zu verbinden, dass diese systemseitig umsetzbar sind. Es ist bisher weniger darüber bekannt, wie man effektive digitale Privacy Nudges

gestaltet, um das Verhalten von Nutzenden zu ihrem Vorteil zu ändern [36]. Um diesen Sachverhalt aus soziotechnischer Sicht besser beurteilen zu können, ist es notwendig, zu verstehen, wie Nutzende auf unterschiedliche digitale Nudges reagieren und wie sie sich voneinander unterscheiden, sodass individuelle Nudging Konzepte gestaltet werden können, die sowohl die Interessen von Nutzenden als auch rechtliche und ethische Fragestellungen berücksichtigen. Hierzu fehlt es an Ansätzen, die alle Disziplinen gleichermaßen aufgreifen.

Mit einem effektiven Konzept zur Gestaltung von Privacy Nudges in digitalen Umgebungen könnten datenschutzrechtliche Anforderungen besser umgesetzt werden. Ohne die Anpassung digitaler Nudges an eine bestimmte Gruppe von Nutzenden sind sie möglicherweise nicht effektiv, wenn es darum geht, das Verhalten von Nutzenden zu ändern. Darüber hinaus stellt sich aus soziotechnischer Sicht die Frage, wie die Umsetzung effektiver Datenschutzbestimmungen die Einstellung von Nutzenden zu einem System oder gegenüber dem Anbieter des Systems verändert. Wirksamkeit und Relevanz sollten im Hinblick auf die Reaktion der Nutzenden und ihr Vertrauen in ein Informationssystem oder eine Plattform, die mit solchen Pattern arbeitet, und ihre Akzeptanz dieser Systeme weiter diskutiert werden.

3 Vorschläge für eine rechtskonforme Gestaltung von Privacy Nudges unter verschiedenen Gesichtspunkten

Für eine effektive und effiziente Gestaltung von digitalen Nudges gilt es, einen Ansatz zu finden, der alle drei Disziplinen miteinander verbindet. Eine Übersicht über die Empfehlungen und deren Einordnung ist in Abb. 1 dargestellt.

3.1 Empfehlung 1 – Vorüberlegungen zum Nudging Konzept

Je nach Einsatzszenario ergeben sich unterschiedliche Gestaltungsgrundlagen für die Auswahl von digitalen Nudges [19]. Nudges können sowohl online als auch offline genutzt werden. Die Wahl des Kontextes und des Zieles bestimmt maßgeblich dessen Gestaltung. Die soziotechnische Perspektive fokussiert sich primär auf den online Kontext und digitale Umgebungen. Hingegen gelten die Anforderungen der ethischen und rechtlichen Sichtweise zumindest hinsichtlich der grundsätzlichen Probleme des Paternalismus sowohl für offline als auch online Nudges. Bevor ein Nudging Konzept entwickelt wird, ist es wichtig, sich das Ziel des Nudgings und den Kontext des Einsatzes vor Augen zu führen. Dies ist von

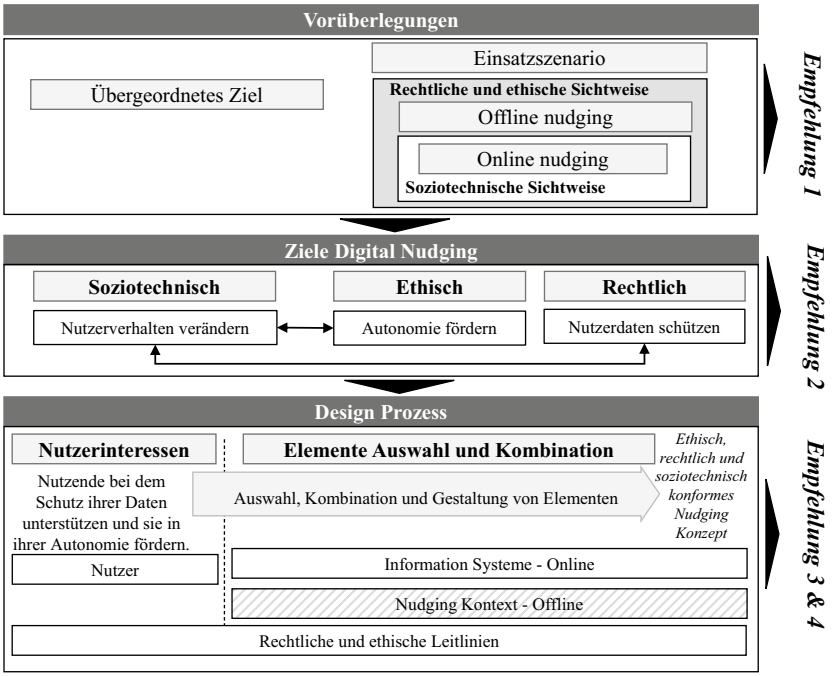


Abb. 1 Der Weg zu ethisch, rechtlich und soziotechnisch konformen Nudge Designs

Bedeutung, um rechtliche und ethische Grauzonen auszuschließen und vor Beginn der Entwicklung eines Nudging Konzeptes entsprechende Maßnahmen in Bezug auf die Gestaltung treffen zu können. Gleichermaßen gilt es zu eruieren, wie und welches Design von digitalen und offline Nudges in Bezug auf deren Effektivität und Wirkung eine Rolle spielt [11, 37]. Hier sollte in künftigen Studien erarbeitet werden, wie genau welche Art von Nudge Gestaltung dessen Effektivität begünstigt. Daher schlagen wir in Bezug auf die Gestaltung von Nudges vor:

Vor der Entwicklung eines Nudging Konzeptes sollten das Einsatzszenario, (offline, online) und das Ziel des Konzeptes erörtert werden, um Gestaltungsansätze auszuschließen, die rechtlich und ethisch nicht konform sind und um solche Ansätze zu wählen, die die gewünschten Nutzungseffekte erzielen, also zum Datenschutz beitragen.

3.2 Empfehlung 2 – Ziel des Nudgings

Die drei vorangestellten Perspektiven verfolgen unterschiedliche Ziele, die es in Einklang zu bringen gilt. Mit einer soziotechnischen Sicht soll durch den Einsatz von Nudges ein besseres Verständnis des Verhaltens von Nutzenden erreicht werden. Die ethische Perspektive soll die Autonomie der Nutzenden schützen. Die rechtliche Perspektive prüft, ob Privacy Nudges mit dem Gesetz, insbesondere den Grundrechten und dem Datenschutzrecht, in Einklang stehen und greift rechtliche Vorgaben bei der technischen Gestaltung mit auf. Es gibt auch Ziele, die alle Perspektiven gemeinsam verfolgen. Hier ist insbesondere die Wahrung der Autonomie von Nutzenden relevant und die Tatsache, dass Transparenz darüber geschaffen wird, was mit den Daten eines Nutzenden geschieht. Obwohl soziotechnische Experten daran interessiert sind, das Verhalten von Nutzenden zu ändern, was auch im Sinne eines nudgenden Unternehmens sein kann, welches z. B. Cookie Einstellungen zu seinem Vorteil vornimmt, streben sie auch danach, zu verstehen, wie digitale Nudges unter bestimmten Bedingungen (rechtliche sowie ethische) gestaltet werden können. Diese Bedingungen können durch die Einbeziehung rechtlicher oder ethischer Perspektiven bei der Gestaltung digitaler Nudges, z. B. durch Audits mit spezifischen Richtlinien, vorangetrieben und geschärft werden [38]. Dies sollte so erfolgen, dass durch den Einsatz von digitalen Nudges die Effektivität ihres Einsatzes unterstützt wird, was die soziotechnische Sichtweise primär bestärkt [3, 39]. Genauer zu erarbeiten ist die Frage, wie man effektiver und effizienter in der Umsetzung und Konsolidierung von drei verschiedenen Disziplinen agieren kann. Zusammengefasst resultiert folgende Designempfehlung:

Digitale Nudges erfordern es, ethische, rechtliche und soziotechnische Aspekte für die Gestaltung zu berücksichtigen, um Nutzende bei Entscheidungen, die sie in digitalen Umgebungen treffen müssen, zu unterstützen.

3.3 Empfehlung 3 – Nutzerinteressen

Wenn man den Fall von Privacy Nudging betrachtet, weisen alle Disziplinen eine Gemeinsamkeit auf. Sie konzentrieren sich auf Nutzende, deren Daten verarbeitet werden und geschützt werden müssen. Damit Nudges entsprechend effektiv und zielführend eingesetzt werden können, gilt es, die Bedürfnisse von Nutzenden zu erfassen und zu verstehen, was ihre Handlungen leitet. Aus rechtlicher Sicht ist es wichtig, die Daten der Nutzenden zu schützen und proaktiv zu prüfen, wo

Daten geteilt werden sollen. Nutzenden fällt es ggf. schwer zu verstehen, welche Daten rechtlich sensibel und schützenswert sind. Weiterhin befasst sich die Forschung damit, ein tiefergehendes Verständnis zu erlangen, wie Nutzende auf Nudging Elemente reagieren und wie effektiv diese das Verhalten von Nutzenden ändern [35, 40]. Hier könnte durch die Erfassung von Nutzerpräferenzen in Bezug auf die Gestaltung erarbeitet werden, was Nutzende in ihrem Entscheidungsprozess bestmöglich unterstützt [10]. Insoweit ist es aus ethischer als auch aus rechtlicher Sicht notwendig, vorab zu überlegen, wie Nudges entworfen werden können und sollten, um die Nutzenden beim Schutz ihrer Daten zu unterstützen und gleichzeitig ihre Interessen mit aufzugreifen. Der gesamte Prozess sollte aus einer soziotechnischen Perspektive betrachtet werden. Bei der Abwicklung des Prozesses ist von Bedeutung, dass alle Disziplinen mit ihren Erwartungen und unterschiedlichen Sprachen miteinander vereint werden. Zwar existieren Methoden [9], die Forscher und Praktiker bei der Gestaltung von Nudging Konzepten unterstützen, allerdings sind diese oftmals nicht interdisziplinär ausgerichtet und greifen primär die soziotechnische Sichtweise auf. Innerhalb eines Prozesses könnte man somit, nachdem man ein Verständnis von den Interessen und Präferenzen der Nutzenden gewonnen hat, rechtliche und ethische Perspektiven für die Gestaltung von Nudging Konzepten mit aufgreifen und berücksichtigen. Daraus resultiert der folgende Vorschlag:

Digitale Nudges sollten unter Berücksichtigung von ethischen und rechtlichen Fragestellungen auf die Interessen und Bedürfnisse der Nutzenden abgestimmt werden, um diese bei ihren Handlungen zum Schutz ihrer Daten zu unterstützen.

3.4 Empfehlung 4 – Nudge-Elemente

Wie im vorherigen Kapitel demonstriert, existieren eine Vielzahl von verschiedenen Nudge Elementen, die zur Gestaltung von Nudging Konzepten eingesetzt werden können. Deren Auswahl und Kombination erfordert wichtige Vorüberlegungen, die je nach Kombination anders ausfallen. Dies möchten wir anhand von Voreinstellungen erläutern. Diese haben sich als zentrales und sehr wirksames Element erwiesen, um die beabsichtigten Verhaltensweisen zu bewirken. Bei Privacy Voreinstellungen handelt es sich um vorausgewählte Einstellungen in einem System, die als Standardwerte festgelegt sind, welche automatisch alle privaten Daten schützen [10]. Aus soziotechnischer Sicht sind Voreinstellungen einfach zu implementieren und für Nutzende ebenfalls einfach anwendbar. In ähnlicher Weise wie andere digitale Nudges unterstützen Voreinstellungen Nutzende aus rechtlicher Sicht beim Schutz ihrer Daten. Art. 25 Abs. 2 DSGVO schreibt

sogar ausdrücklich datenschutzfreundliche Voreinstellungen vor. Aus ethischer Sicht unterstützen Voreinstellungen jedoch nicht unbedingt die Autonomie des Benutzers. Um die Autonomie der Nutzenden zu unterstützen, können Voreinstellungen mit Informations Nudges verbunden werden, indem Informationen in Online-Entscheidungssituationen im Zusammenhang mit dem Datenschutz zur Verfügung gestellt werden, um eine realistische Perspektive auf das Risiko von Datenschutzverletzungen zu ermöglichen [10]. Voreinstellungen können außerdem mit Farbelementen kombiniert werden. Diese Kombination würde wiederum andere rechtliche und ethische Fragestellungen aufwerfen. Nutzt man beispielsweise eine rote Farbe, stimuliert dies stärker das Handeln von Nutzenden als beispielsweise eine grau hinterlegte Fläche. Hier muss entsprechend darauf geachtet werden, dass die Farbgebung die datenschutzfreundliche Handlung unterstützt und sie nicht manipuliert, wie dies bei „Dark Pattern“ oft der Fall ist.

Voreinstellungen stellen nur eine Art von Elementen dar, die neben sozialen Normen, Informationen oder Zeitverzögerung auch in Kombination miteinander eingesetzt werden können. Jedes einzelne Element erfordert es dabei, sein Design individuell so zu gestalten, dass dieses rechtlich und ethisch konform ist. Dementsprechend empfehlen wir zum Schluss:

Nudge Elemente sollten so ausgewählt und kombiniert werden, dass diese rechtliche, ethische und soziotechnische Kriterien bei der Gestaltung berücksichtigen, um ihre Effektivität im Sinne des Schutzes von Nutzerdaten zu unterstützen.

4 Zusammenfassung

Mit unserem Beitrag präsentieren wir eine umfassende, interdisziplinäre Perspektive zum Thema Privacy Nudging. Wir präsentieren vier Gestaltungsvorschläge, um die Gemeinsamkeiten und Herausforderungen zusammenzufassen, denen wir uns in Bezug auf die Gestaltung digitaler Nudges stellen müssen und die rechtlichen und ethischen Anforderungen, um Nutzende dabei zu unterstützen so zu handeln, dass sie ihre Daten aktiv schützen. Unsere Studie zeigt, dass die Disziplinen einige Aspekte in Bezug auf das digitale Nudging teilen, sich aber auch in einigen Standpunkten unterscheiden. Während sich die soziotechnische Perspektive auf Nudges im digitalen Bereich konzentriert, fokussieren sich die rechtlichen und ethischen Disziplinen nicht nur auf digitale Nudges, sondern auch auf die Gestaltung von Offline-Nudges. Jede unserer drei Disziplinen hat unterschiedliche Ziele in Bezug auf die Nutzung und Gestaltung von digitalen Nudges. Rechtliche und ethische Disziplin teilen gemeinsame Vorstellungen über das Ziel und die Nutzung digitaler Nudges. Die soziotechnische Disziplin fokussiert sich auf

das Nutzungsverhalten und dessen Intensivierung. Hierbei sind Themenstellungen wissenschaftlich interessant, die sich nicht nur auf positive Absichten von Nudges fokussieren, sondern auch die Nutzung von Dark Pattern verständlicher gestalten. Übergeordnet sollte jedoch das Ziel sein, die Nutzung so zu unterstützen, dass Nutzende nicht manipuliert, sondern gefördert werden, ihre eigenen Daten zu schützen und dementsprechend zu handeln.

Förderhinweis
Dieser Artikel wurde im Rahmen des Projekts „Nudger“ (www.nudger.de; Förderkennzeichen: 16KIS0890K) unter der Projektträgerschaft des VDI/VDE-IT erarbeitet und mit den Mitteln des Bundesministeriums für Bildung und Forschung gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autoren.

Literatur

1. O’Halloran, D., Griffin, W.: Our shared digital future – responsible digital transformation. World Econ. Forum 5–20 (2019)
2. Belanger, F., Hiller, J.S.: A framework for e-government: privacy implications. Bus. Process Manage. J. 48–61 (2006)
3. Acquisti, A., Sleeper, M., Wang, Y., et al.: Nudges for privacy and security. ACM Comput. Surv. **50**, 1–41 (2017). https://doi.org/10.1145/3054926
4. Weinmann, M., Schneider, C., Vom Brocke, J.: Digital nudging . Bus. Inf. Syst. Eng. **58**, 433–436 (2016). https://doi.org/10.1007/s12599-016-0453-1
5. Schomberg, S., Barev, T.J., Janson, A., et al.: Ansatz zur Umsetzung von Datenschutz nach der DSGVO im Arbeitsumfeld: Datenschutz durch Nudging. Datenschutz Datensicherheit **43**, 774–780 (2019). https://doi.org/10.1007/s11623-019-1204-5
6. Eigenbrod, L., Janson, A.: How digital nudges influence consumers–Experimental investigation in the context of retargeting. In: European Conference on Information Systems (ECIS) (2018)
7. Thaler, R.H., Sunstein, C.R.: Nudge: improving decisions about health, wealth, and happiness. In: A Caravan book large print edition. Yale University Press, New Haven (2008)
8. Nouwens, M., Liccardi, I., Veale, M. et al.: Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing System, S. 1-13, arXiv:2001.02479 (2020)
9. Mirsch, T., Lehrer, C., Jung, R.: Making Digital Nudging Applicable: The Digital Nudge Design Method. In: European Conference on Information Systems (2018)
10. Schöbel, S., Barev, T., Janson, A. et al.: Understanding user preferences of digital privacy nudges – a best-worst scaling approach. In: Bui, T. (ed) Proceedings of the 53rd Hawaii International Conference on System Sciences. Hawaii International Conference on System Sciences (2020)

11. Hummel, D., Maedche, A.: How effective is nudging? A quantitative review on the effect sizes and limits of empirical nudging studies. J. Behav. Exp. Econ. **80**, 47–58 (2019). https://doi.org/10.1016/j.socec.2019.03.005
12. Meske, C., Potthoff, T.: The DINU-model–a process model for the design of nudges. In: European Conference on Information Systems (2017)
13. Schneider, C., Weinmann, M., Vom Brocke, J.: Digital nudging. Commun. ACM **61**, 67–73 (2018). https://doi.org/10.1145/3213765
14. Mongin, P., Cozic, M.: Rethinking nudge: not one but three concepts. Behav. Public Policy **2**, 7–124 (2018). https://doi.org/10.1017/bpp.2016.16
15. Kahneman, D.: Maps of bounded rationality: psychology for behavioral economics. Am. Econ. Rev. **93**, 1449–1475 (2003). https://doi.org/10.1257/000282803322655392
16. Bullock, E.C.: A normatively neutral definition of paternalism. Philos. Q. **65**, 1–21 (2015)
17. Sunstein, C.R.: Choosing Not to Choose: Understanding the Value of Choice. Oxford University Press, USA (2015)
18. Barnhill, A.: What is manipulation? In: Coons, C., Weber, M. (eds.) Manipulation: Theory and Practice, S. 51–72. Oxford University Press, Oxford (2014)
19. Wilkinson, T.M.: Nudging and manipulation. Polit. Stud. **61**, 341–355 (2013)
20. Noggle, R.: The ethics of manipulation. In: Stanford Encyclopedia of Philosophy Archive, Online verfügbar über: https://stanford.library.sydney.edu.au/archives/win2018/entries/ethics-manipulation/ (2018)
21. Gerg, S.: Nudging: Verfassungsrechtliche Maßstäbe für das hoheitliche Einwirken auf die innere Autonomie des Bürgers, 1. Aufl. Beiträge zu normativen Grundlagen der Gesellschaft (2019)
22. Krimphove, D.: Nudging als Mittel der ergänzenden Verhaltenssteuerung im Rechtssystem? Rechtstheorie **48**(3), 299-314 (2017)
23. Kant, I.: Über den Gemeinspruch: Das mag in der Theorie richtig sein, taugt aber nicht für die Praxis, 1. Aufl. Contumax, Hofenberg, Berlin (2016)
24. Krönke, C.: Datenpaternalismus. Staatliche Interventionen im Online-Datenverkehr zwischen Privaten, dargestellt am Beispiel der Datenschutz-Grundverordnung. Der Staat **55**, 319–351 (2016). https://doi.org/10.3790/staa.55.3.319
25. Hillgruber, C.: Der Schutz des Menschen vor sich selbst. JZ **2**, 66-75 (1992)
26. Schwabe, J. Der Schutz des Menschen vor sich selbst. JZ 66–75 (1998)
27. Sandfuchs, B., Kapsner, A.: Privacy nudges: conceptual and constitutional problems. In: Bürk, S., Hennig, M., Heurich, B., et al. (Hrsg.) Privatheit in der digitalen Gesellschaft, S. 319–338. Duncker & Humblot, Berlin (2018)
28. BVerfGE 22, 180(219)
29. Eidenmüller, H.: Liberaler Paternalismus. Juristenzeitung 814–821 (2011)
30. Wolff, J.: Eine Annäherung an das Nudge-Konzept nach Richard H. Thaler und Cass R. Sunstein aus rechtswissenschaftlicher Sicht. Rechtswissenschaft **6**, 194–222 (2015). https://doi.org/10.5771/1868-8098-2015-2-194
31. Kirchhof, G.: Nudging – zu den rechtlichen Grenzen informalen Verwaltens. ZRP 136–137 (2015)
32. BVerfGE 7, 198 – Lüth
33. Laue, P., § 1 Einführung, In: Laue, P./Kremer, S. (Hrsg.): Das neue Datenschutzrecht in der betrieblichen Praxis, 2. Aufl, Nomos, Baden-Baden, (2019)

34. Martini, M., Art. 22 DS-GVO, In: Paal, B./Pauly, D. (Hrsg.): Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl. C.H. Beck, München (2018)
35. Ho, S.Y., Lim, K.H.: Nudging moods to induce unplanned purchases in imperfect mobile personalization contexts. MISQ 42 757–778. https://doi.org/10.25300/MISQ/2018/14083 (2018)
36. Caraban, A., Karapanos, E., Gonçalves, D. et al.: 23 ways to nudge: a review of technology-mediated nudging in human-computer interaction. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, S. 1–15 (2019)
37. Lembcke, T.-B., Engelbrecht, N., Brendel, A.B. et al.: To nudge or not to nudge: ethical considerations of digital nudging based on its behavioral economics roots. Eur. Conf. Inf. Syst. (ECIS) 1–17 (2019)
38. Meske, C., Amojo, I.: Ethical guidelines for the construction of digital nudges. In: Proceedings of the 53rd Hawaii International Conference on System Sciences (2020)
39. Warberg, L., Acquisti, A., Sicker, D.: Can privacy nudges be tailored to individuals' decision making and personality traits? In: Cavallaro, L., Kinder, J., Domingo-Ferrer, J. (eds.) Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society – WPES'19. ACM Press, New York, New York, USA, S. 175–197 (2019)
40. Kroll, T., Stieglitz, S.: Digital nudging and privacy: improving decisions about self-disclosure in social networks. Behav. Inf. Technol. 1–19 (2019)
41. Leimeister, J.M.: Einführung in die Wirtschaftsinformatik. Springer Gabler. (2021). ISBN: 978-3-662-63559-9

Conducting a Usability Evaluation of Decentralized Identity Management Solutions

Alina Khayretdinova, Michael Kubach, Rachelle Sellung and Heiko Roßnagel

Abstract

New approaches to identity management based on technologies such as blockchain and distributed ledgers are promoted as a chance to give users full control over their own identity data. Despite being often called the future of digital identity management, Decentralized Identity Management (DIdM) and Self-sovereign Identities (SSI) are still facing a number of challenges, usability being a major one: their concepts are too sophisticated for users and do not fit their mental models. We address this by conducting a study that analyses and evaluates the usability and practical applicability of some of the most advanced DIdM solutions. The results of the user tests reveal existing usability issues and outline the way they deprive end users of experiencing the entire range of claimed privacy and security benefits of these identity solutions.

A. Khayretdinova
University of Stuttgart IAT, Institute of Human Factors and Technology Management, Stuttgart, Germany
E-Mail: alina.khayretdinova@iat.uni-stuttgart.de

M. Kubach (✉) · R. Sellung · H. Roßnagel
Fraunhofer IAO, Fraunhofer Institute for Industrial Engineering, Stuttgart, Germany
E-Mail: michael.kubach@iao.fraunhofer.de

R. Sellung
E-Mail: rachelle.sellung@iao.fraunhofer.de

H. Roßnagel
E-Mail: heiko.rossnagel@iao.fraunhofer.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_19

Keywords

Decentralized identity management • Blockchain • UX • Usability • SSI • Self-sovereign identity

1 Introduction

Despite of numerous state-sponsored efforts over the last twenty years to provide European citizens with high assurance electronic identities, today's digital identity market is heavily dominated by single-sign-on solutions that are offered by big international corporations. Nevertheless, the market for digital identities is not saturated yet. Many use cases still wait for a suitable, e.g. interoperable, easy-to-use, widely adopted, secure, privacy friendly ID-solution. This is why market researchers still see a high potential in this sector [1, 2]. New approaches, initially based on Blockchain and distributed ledger technologies (DLT) have been getting a lot of attention in the past 3–4 years and are promising to disrupt the digital identity market [3]. Such approaches, often also called Decentralized Identity Management (DIdM) and Self-sovereign Identities (SSI), are often marketed as the future of digital identity management [4, 5]. In the following, we will use the term Decentralized Identity Management solutions (DIdM) for these approaches.

Numerous companies and projects (Sovrin, Jolocom, W3C Decentralized Identifier Working Group, Decentralized Identity Foundation, Hyperledger of the Linux Foundation etc.) are currently working on technologies that make it possible to use decentralized identities for trustworthy and privacy-friendly identification in digital interactions. The European Commission supports such approaches, for example through the European Self-Sovereign Identity Framework (ESSIF) as part of the European Blockchain Service Infrastructure (EBSI) [6] and the SSI eIDAS bridge [7]. Those actors see security and privacy as the main challenges in the currently available approaches to digital identities and promise to give the user the power to reclaim control over their own identity data in digital interactions [8, 9].

Nevertheless, experience shows that technical functionality even together with high levels of security and privacy protection are not sufficient for the diffusion of new information technologies [10]. Many technologies in the identity management sector that were previously regarded as disruptive, such as CardSpace,

Uprove, and Attribute Based Credentials, have failed to find adoption by a significant share of the market [11, 12]. Hence, it has been argued that the consideration of multidisciplinary aspects, such as security, usability, and socioeconomics, is crucial for the success of a software product on the market [13]. However, it is a common issue that developers tend to focus on the former aspects while neglecting the latter [14].

We agree that there remains a growing need for identity management solutions to replace username/password and the solutions provided by the mighty GAFA platform-corporations (Google, Apple, Facebook, Amazon) — as has been countlessly discussed in information (security/privacy) science as well as in the public. New approaches entering the market for alternative identity management solutions still struggle with its multi-sided structure, leading to a "chicken or the egg" dilemma. Uptake with end-users and services providers and the sustainable as well as balanced trust relationship among the relevant stakeholders is a big challenge [15]. Therefore, we think that is important to critically assess the current promises, intentions and practices of DIdM solutions, in order to avoid mistakes that could, again, lead to the failure of a promising technology on the market. This is what we aim for with this paper. Our analysis is focused on the usability aspects of DIdM solutions, and studies them empirically with end users. Our research approach addresses the challenge of usability in DIdM solutions by conducting a user study that analyses and evaluates currently available DIdM solutions towards their practical applicability for end users. This paper presents the results of the usability tests with end-users that will be later used to build a user-friendly prototype and to give design guidelines to DIdM solution developers aiming to increase the adoption potential of their products. Other important aspects, such as the perspectives and requirements of service providers (relying parties) [16], will have to be kept aside for future work.

Our paper is structured in the following way. In section two we give an overview of the background and current state of Decentralized and Self-sovereign Identities. We briefly introduce the approach and terms, principles being followed, market overview and related research. Next, in section three, we present our user test of three DIdM solutions, describing methods, results, and analysis. Continuing, in section four we discuss the key results of the study and what we regard as its main outcomes. Lastly, section five presents the limitations and section six briefly concludes our paper.

2 Overview: Decentralized and Self-sovereign Identities

Decentralized and Self-sovereign Identities (SSI) are currently being marketed as the future of digital identity management as opposed to traditional approaches that are often simply called "legacy systems" [17–19]. The promise of these approaches is that they are able to empower users to take back control over their data [20, 21], and to overcome the dominance of the GAFA platforms [22, 23].

When it comes to new, alternative, decentralized approaches towards identities, the term Self-sovereign Identity has become more and more prominent. Although it is not always being used consistently, Mühle et al. [24] summarize the key properties of the concept as that a Self-sovereign identity management system would allow users to fully own and manage their identity without having to rely on a third party. The origin of the concept under this name can be traced back to 2016, when Allen published his so called "Ten Principles of Self-sovereign Identity" [20]. There, he also refers to the earlier proclaimed "Laws of identity" by Cameron [25], which illustrates that the basic approach is not entirely new. Following the taxonomy by Lesavre et al. [26], Self-sovereign Identity can be seen as a bottom-up approach, where no single entity acts as central authority that has control over identifier origination and/or credential issuance. Identifiers and credentials are solely managed by the users, without requiring any permissions. On the other side of the spectrum would be top-down approaches relying on central authorities as identity providers and federated approaches somewhere in between.

However, it is important to recognize that the reasoning provided for the DIdM approach and the SSI principles or laws are not founded on empirical studies of the requirements of users (and neither service providers). In addition, there are still some open questions on whether the users actually desire so much control and whether the solutions not only provide users with the theoretical opportunity to exercise this control through their technical architecture, but also empower them in practice and not confuse and overburden them. For users to be able to fully manage and own their identity without having to rely on a third party, they are required to somehow understand the concept and be assisted with usable tools that do not frustrate them. After all, typical users do not use identity management because it is such great fun, but rather to access services they want to use. Being in theoretical control of their identity could become a similar experience as the current total control users have over trackers and cookies when visiting a website. Having to manage those detailed settings manually through annoying dialogues might simply frustrate them. The lack of usability could then lead average users to

simply use privacy unfriendly, but convenient solutions—a pattern we frequently observe.

One of the potential usability issues of Blockchain-based DIdM solutions is the fact that the private key that ensures the access to user's personal data is in total responsibility of the user [27]. While this is often marketed as one of the most significant benefits of DLT-based and DIdM solutions, it also comes with significant challenges such as how to securely store and manage those keys to avoid irretrievable loss of key and connected accounts [28]. If such issues are not properly explained and handled, end users will have troubles understanding and using the new technology. This makes the solutions less attractive to average users and leads to lower levels of adoption. Especially, if it may seem that they require more and complex user involvement while not offering other benefits except for being more privacy friendly (something the average user cannot even personally assess as we are clearly in some kind of "market for lemons" here [29, 30]). Moreover, if such solutions are not widely supported by service providers and thus not integrated into a sufficient variety of services, their value for end users is even lower.

The issue of usability in privacy and security tools has already been subject of research efforts for quite some time [31, 32]. Nevertheless, there seem to be only few attempts to explicit fix user experience challenges for security tools and so also for DIdM. Following [33–35], the major problems that go beyond the mere graphical user interface are:

- The concepts and interface presentations do not fit the underlying mental models of the users.
- Tools offer actions, such as e.g. obtaining, managing, and securing private keys, passwords, credentials, etc. that are either too complicated to be carried out, or not presented clearly enough and therefore executed wrongly.

This seems particularly important when it comes to a technology like DIdM that puts as much power into the hands of the individual user and builds on concepts such as public and private keys that are not trivial to the average online-shopper. We see this lack of consideration of the usability and mental models in current approaches to DIdM as an important potential weakness that needs to be studied empirically with explicit user involvement. Therefore, we want to address it through our work.

For our user study, we are dependent on publicly available and testable DIdM solutions. In their public presentations, proponents of DIdM give the impression, that the technology is ready to replace legacy IdM systems. On their website,

for example, uPort writes of "easy-to-use data management and control to your business and customer" [36], Evernym of "The fastest, most efficient way for organizations to offer an SSI-enabled solution for their users" [37]. That of course raises high expectations regarding their solutions technology readiness and current practical applicability.

However, another consideration that needs to be made is that DIdM technology is still under heavy development and different approaches are currently being pursued. For example, those can be differentiated according to organizational structure, models for identifier and credential management, presentation disclosure, general system architecture design and the use of public registries. A systematic overview and discussion can be found at Lesavre et al. [26]. First standards are currently being finalized, e.g. by the W3C [38] and the DID [39], but the work is still ongoing. This makes interoperability between the different approaches challenging.

At this time, a significant number of companies and projects are working on decentralized identity solutions. In a thorough survey of market of Blockchain-based Identity Management solutions and technologies, Kuperberg [27] analyses 43 approaches with different levels of maturity and availability. He concludes that only a couple of these approaches could compete with established solutions when it comes to end-user convenience, though it has to be noted that his analysis has to remain on a rather high level due to the high number of solutions considered. What he misses in particular, is a clear and sustainable business model. Dunphy and Petitcolas [33] analyse IdM schemes of three Blockchain-based products (uPort, ShoCard, Sovrin) according to the Cameron's "laws of identity" [25]. Regarding usability, they conclude that all of those projects have an "unclear usability and user understanding of […] (the) privacy implications." None seems to actively address the issues in regard to fitting mental models and usability. All this apparently supports need for our research approach.

3 User Test of DIdM Solutions

In our research, we are addressing the challenge of usability in DIdM solution by conducting a user study that analyses and evaluates DIdM solutions that are currently (beginning of 2020) available on the market towards their practical applicability and acceptance for end users. For our study, we identified 23 DIdM solutions. In April 2020, those identified solutions were on a sufficient level of maturity (and/or transparency in public communication) to provide enough information for an analysis that would determine whether they would be suitable for

an end-user study. In order to identify which DIdM solutions would best fit a usability study with end users, we analyzed those 23 DIdM solutions by their differences in maturity, purpose and functionality. The suitability of solutions for the user test was evaluated according to the following set of requirements: DIdM as the core technology; minimal level of technology readiness (at least TRL 7); wide functionality (to be able to carry out at least 3 scenarios for user testing); availability of the wallet for both iOS and Android platforms; availability of a demo scenario or even real services to test the solution; interface language English and/or German. According to these conditions, three DIdM digital wallets qualified for then being evaluated in a systematic study including end-users in a usability test: Evernym ConnectMe, Jolocom SmartWallet, and uPort ID.

3.1 Method

In order to obtain a full understanding of the user's impression of each tested identity solution and the concept of DIdM solutions in general we employed a combination of usability and user experience evaluation methods (following the approach of Tomlin [20]).

In Summer 2020, the user tests were conducted remotely via individual video calls, each with a duration of 80 to 100 min. The tests consisted of a preliminary questionnaire, a block of 8 tasks to be completed each followed by questions, the User Experience Questionnaire (UEQ) [19], and a post-questionnaire. Participants carried out tasks with the smartphone app and the demo websites that were provided by the solutions.

3.1.1 Pre-questionnaire

The pre-questionnaire consisted of 8 questions to define demographics (gender and age) of participants and their experience with technologies similar to digital wallets they were about to test. Moreover, there were questions aimed to understand how participants create and store their passwords, which would give more information on their further decisions and opinions regarding the seed-phrase technique all three digital wallets were using to recover user accounts.

3.1.2 Tasks

There were 8 tasks during the test: create an account within a digital wallet (1), obtain two personal documents (2 and 3), make sure the digital wallet is ready for future use (4), back-up the digital wallet (5), delete one of the credentials (6), delete the wallet, re-install the app and restore the account (7), delete the account

(8). After each task, there were a set of questions to assess whether a participant managed to perform the task, how difficult it was is to perform the task, how many attempts it took them to get a certain task done, etc.

3.1.3 User Experience Questionnaire (UEQ)

To cover a comprehensive impression of the user experience aspect of digital wallets, an established and tested questionnaire was needed. We opted for the User Experience Questionnaire (https://www.ueq-online.org/) that helps to measure both usability aspects such as efficiency, perspicuity, and dependability, and user experience aspects such as originality and stimulation. According to Schrepp et al., the main goal of the UEQ is to allow a fast and immediate measurement of user experience of a product, which also allows to compare it with its direct competitors to get information on the comparative position of the product [40]. The questionnaire has 26 pairs of terms with opposite meanings grouped into six scales: attractiveness, perspicuity, efficiency, dependability, stimulation, and novelty. The items need to be rated on a 7-point Likert scale from -3 (fully agree with negative term) to $+3$ (fully agree with positive term). In order to avoid automatic response to some terms, half of the items start with the positive term, the rest with the negative term in randomized order [41]. More information on the UEQ, its underlying methodology and reliability as well as validity of its scales can be found at [40–42].

3.1.4 Post-questionnaire

Post-questionnaire consisted of 7 questions and was aimed to find out whether participants liked the apps or not, what they especially they liked and disliked in them. Moreover, some of the questions helped to understand what participants think about the concept of such digital wallets in general and whether they would be ready to switch from their physical wallet to a digital one.

3.2 Results

This section presents the results of user tests conducted on DIdM solutions following each step of the test process.

18 persons took part in the evaluation of three applications (6 participants per app), among which were 9 male and 9 female participants with 78 % of them being under 30 years old and 22 % above 30. All participants were able to complete most of the tasks except a few cases when users experienced connectivity issues between the digital wallet and the demo website, which led to failing some

tasks. Further, we are presenting the results of each tasks that participants were asked to do during the test.

3.2.1 User Test Tasks

Task 1. Create an account within a digital wallet. All the users managed to create an account in all three digital wallets, with 16 % of them finding it a bit difficult to perform the task.

Task 2. Obtain first personal document. All the user of ConnectMe and uPort ID performed the task without the external help with half of them having no difficulties finding the function in the apps. However, a smaller percentage of SmartWallet testers managed to carry out the task completely on their own—83 %.

Task 3. Obtain second personal document. All of the users that were testing SmartWallet and uPort ID managed to obtain the second credential without any external help compared to 67 % of those who tested ConnectMe. However, a smaller number of participants managed to perform the task from the first try in comparison to obtaining the first credential and the task seemed more difficult to a bigger number of people.

Task 4. Make sure the digital wallet is ready for future use. The participants were asked the following questions: "Have you done everything that was necessary with your digital wallet? Is everything set up now for the use in future?" Not all the users were sure the digital wallet was all set for future use, with some doubts being connected to the security of their account and the general purpose of the digital wallet.

Task 5. Back-up the digital wallet. Almost all the participants managed to back-up their credentials without the external help, however, almost half of them found the task somewhat difficult to perform. Moreover, less than 50 % of participants had the confidence that their documents are indeed backed up: 83 % testers of SmartWallet, 50 % of ConnectMe users and 33 % of those who tested uPort ID answered negatively to the question whether they think their documents are well protected after the back-up process. The most common doubts were about the back-up choice that was given in the apps and the back-up being saved on the server of the digital wallet. Another issue appeared in this task was the use of the "seed" or "recovery" phrase: most of the test participants did not understand its purpose and had doubts on whether it would help them to restore their account in future in case of a lost or a compromised device.

Task 6. Delete one of the credentials. None of the SmartWallet users performed this task due to the absence of this function in the app. A bit more than a half of ConnectMe users managed to delete one of the credentials with most of them being confused that they had to delete a connection instead of the credential. On

the other hand, all of the participant that tested uPort ID performed the task and found it not difficult at all.

Task 7. Delete the wallet, re-install the app and restore the account. All of the ConnectMe and uPort ID users managed to perform the task without any external help and the majority did not find the task difficult. However, only 67 % of them were sure they would be able to restore their account in case they do not have the access to their current mobile device (due to the fact that they stored their "seed" or "recovery" phrase on the mobile device where they interacted with the digital wallet).

Task 8. Delete the account. The success rate of the task performance is clearly much lower compared to other tasks. Only half of participants that tested uPortID managed to carry out the task; 17 % of ConnectMe testers and none of the participants could delete their account in the SmartWallet app. 50 % to 100 % of participants found it highly difficult to carry out this task for each digital wallet with almost all of them not being sure that their personal information was deleted everywhere.

3.2.2 UEQ

As stated earlier in the paper, the User Experience Questionnaire consists of 26 different aspects of design, usability and different requirements that the users had to rate from −3 to 3. Having subtracted the best and the worst scores for each digital wallet, we found the following results: ConnectMe received the highest average score of satisfaction with 1.8, uPort ID followed with a rating of 0.9 and the SmartWallet had a rating of 0.4. In addition, Users presented the following results in regards to understanding (3) and not understanding (−3), Smart.Wallet −0.5, uPort 0.8, and Connect.Me 1.0. Regarding feeling secure (3) and not secure (−3), users averaged with Smart.Wallet, −1.0, Connect.Me 1.0, and uPort with a 1.3.

3.2.3 Post-questionnaire

A little less than a half of all users found the digital wallets as "rather good", however only SmartWallet received 50 % of negative overall evaluation of the app with none of the testers saying they really liked it. Two other digital wallets were rated more positively with 33 % and 17 % of them respectively being really liked by users. The biggest problem found by users of SmartWallet was the fact that it is not protected by a passcode and the overall interaction was sometimes confusing with the app not letting to delete the credentials and the recovery process being difficult. The testers of ConnectMe enjoyed the intuitiveness and the interface design of the wallet, however some of the users mentioned confusing terms used

in the app. The users of uPort ID also stated interface design being one of the advantages of the application and the biggest drawbacks was its functionality: difficulty to obtain the credentials (except the first one) and not being able to delete the account.

Overall, most of the test participants of all digital wallets shared the opinion that the security of their personal information and documents in this kind of apps is the most important part that needs improving. Some of them also stated that in case those security aspects are improved, they would consider switching to a digital wallet.

3.3 Analysis

After carefully analyzing the results of the user study, two main points can be highlighted. First, the results show the apparent need of improvements of the DIdM solutions regarding user mental models and user understanding. Second, there are serious usability problems found in some of the key functions (e.g. backup and restoration) that are essentially required in DIdM wallets. We elaborate on these two points in the following section.

3.3.1 User Mental Models and User Understanding

The existing identity solutions are not as intuitive and easy to use as they claim to be. It would be expected that a market-ready solution is able to compete with the simple interaction patterns provided by the traditional username-password approach and the approach provided by web-single-sign-on solutions by Facebook and Google. This is not the case even for the quite tech-savvy users in our study: many users experienced problems not only in setting up and launching the interaction but also in obtaining credentials. In addition, The UEQ results presented rather weak results for the wallets regarding on whether or not users thought the app was ‘understandable (3) or not understandable (−3), where Smartwallet had a −0.5 average score, uPort had 0.8, and Connect.Me had 1. The interaction paradigm of those DIdM solutions is different and does not fit the user’s established mental models and apparently the solutions are still in a relatively early phase of development.

Moreover, test subjects had a trouble understanding the necessity and importance of backing up their keys (“seed/recovery phrase”). Most of the participants did not write them down even if the app suggested to do so, which in real life would lead them to not being able to recover their personal data in case the device breaks, is lost, stolen, or compromised in any other way. In addition to

that, some of the tested solutions do not explicitly explain the difference between the concepts of "backing up" credentials and setting up a "recovery" of the account ID and the importance of both functions, which in some cases led participants to carry out only one function and not considering the other. Again, this shows that the mental models of the users do not fit to the user experience that the DIdM solutions provide — which can lead to frustration, security problems and finally adoption problems on the mass market (again, this is even the case for the relatively tech savvy participants of our study).

Problems with mental models become apparent as well from the finding that it was unclear to most of the test subjects how and where their data is actually saved. This is quite surprising, as those DIdM solutions claim that local storage under full control of the user would be their key feature and advantage. This gave some of the participants an insecure feeling when they wanted to delete their data "on the servers"—which of course was not possible. Again, a problem of the users' mental models that is not being adequately addressed by the DIdM wallets.

Another problem that became obvious in our study is learnability or the ability for users to 'learn as you go' with completing similar tasks. For instance, in some applications users obtained the first credential and naturally were searching for the same way to obtain the second credential but were unable to do so.

3.3.2 Usability Regarding Vital Functions: Backup and Restoration

The backup and restoration functionality was either not fully implemented (Jolocom — for credentials), not very convenient (manually saving a.zip-file, writing down the mnemonic key phrase), or relied on a server(s) under control of a single entity ("Evernym Cloud") and thus contradicting the whole decentralized and user controlled aspect of the DIdM approach. That such an essential function of the digital identity lifecycle is not properly implemented in the current versions of the wallets that were studied came as quite a surprise — considering how the solutions claim to be "ready for use" and beyond mere Proof-of-concept stage.

Moreover, not all of the three wallets pointed out the importance of the backup function enough (even if it was implemented). After all, this is the only way that users can restore access to their important private accounts if they are managed through the DIdM solution. Push-notifications and other warning messages would be advisable to remind users of this important function.

4 Discussion

According to its advocates, the main benefit of SSI is to put the users in full control of their identities. This is supposed to help to protect their right of informational self-determination. However, with more control also comes the burden of more responsibility and more effort to manage and use these identities and credentials. To be able to manage them effectively, users need to form some sort of rough understanding of how the technology works (aka mental model). Though, our results show that the mental models of the users not necessarily align with those of the developers that are quite familiar with technologies like public key infrastructures end electronic signatures. Users quite often form a different understanding that is shaped by the traditional, hierarchical solutions they are currently using and therefore experience problems when trying to use and manage the credentials in a decentralized architecture. This is especially apparent when it comes beyond the simple use case of issuing and verifying credentials. Important aspects of the identity lifecycle like backup and recovery as well as deleting credentials or whole accounts, constitute huge challenges for the users of the DIdM solutions in our study.

These difficulties are further emphasized by the fact that the basic usability of current DIdM solutions leaves a lot to be desired. This leads to further frustration of the users. Another problem for the approach is that the development of the available solutions is often not as advanced as it is being advertised by their advocates. Essential features are often missing which can be observed by the fact that out of the 23 solutions we examined, only three could offer all the features that we required for our study. And even those three resembled more a work in progress than a mature market ready solution. As just one example, one wallet application (Evernym ConnectMe) in the Fall of 2020 completely removed the backup functionality. It had been available during the user tests, but an update of the application removed the function. Such a gap between promises and actual performance that can be delivered at this point could lead to exaggerated expectations that can only be disappointed if one wants to implement the immature technology right now. This might sustainably damage the reputation of DIdM solutions. The danger is that this could also be regarded as another example that privacy friendly solutions just do not work in practice.

Moreover, to be successful on the market, DIdM faces the same challenge as all other competing and often much more mature identity management solutions. It has to attract a high amount of users and relying parties to benefit from network effects in a two sided market [15]. To achieve this, the perceived benefit by users and relying parties or relative advantage of the DIdM solutions has to be

higher than the competition. The main question will be if — in the eyes of the end users and service providers — the perceived benefit of more user control and more privacy will outweigh the drawbacks such as increased effort to manage the credentials (potentially more annoying dialogues to answer), higher responsibility e.g. to secure the device that is used to control the identity, more complicated backup in case of lost credentials, and particularly at the current state, poor usability and lack of maturity. An empirical user study on web identity management raises some doubts in this regard [43]. Their results show that users do not value control over their identity data as much as many proponents of DIdM apparently expect. Therefore, we believe that it is essential for developers of DIdM to address the current drawbacks we pointed out in a multidisciplinary fashion to improve the likeness of their success on the market.

5 Limitations

Our empirical user study and the derived analysis have undoubtedly some limitations, particularly regarding the sample of end users that participated in the test, the testing setup and the development state of the digital products that were tested.

A sample of 18 participants certainly cannot be regarded as representative of the general population. Most of the test participants were young people around 30 years. In most of the cases they reported themselves as being tech-savvy and could speak a high level of English while living in a non-native English-speaking country, which points to a higher level of education. However, while this is certainly biased sample, we can reasonably assume the results of the user tests could have been even more negative for the case that a broader sample of participants would have been available for us. An example would be end-users who are not as confident with smart phones, scanning QR-Codes, and other relatively new technology.

Another fact that needs to be considered is that the participants tested the DIdM solutions at home having a good internet connection for their smartphone (and desktop computers if used as well). Thus, at least connectivity-wise the whole process (e.g. obtaining credentials) ran smoothly for most of them. However, even under such perfect conditions there were cases when the connection between the digital wallet and the demo website was broken for some time and there was no way of getting back seamlessly to the process. Some of the tested wallets did not offer any solution for such cases and users had to start the whole process from the beginning. It would be interesting to learn about how DIdM solutions relying on mobile smartphone wallets perform in practice when there is

actually still a significant number of situations when smartphone connectivity is limited (Sign on at a desktop computer with no WiFi available for the smartphone and no high speed mobile internet connection).

Also, the evaluation of wallets was conducted at a particular time (April to June 2020) and only the three selected DIdM digital wallets had the level of maturity that was necessary for our user tests. However, even at that time these products were constantly changing significant aspects of their functionality (e.g. backups), one became temporarily unusable.

Finally, we could test the available digital wallets only with demo scenarios provided by the solutions themselves. The use cases were chosen by solutions, thus might be selective to work particularly well, and this was of course not a productive environment. Still, even in this optimized environment, the issues were apparent.

6 Conclusion

After conducting an initial analysis of 23 Blockchain-based DIdM solutions and performing 18 user tests with three of the more advanced applications, the current usability problem of DIdM and SSI solutions can be defined as significant. Principally, we found the overall issue that the new concept of decentralized identity while apparently seeming self-evident to its developers is not explained well enough to the end users, which leads to substantial problems that encumber the practical use and purpose of the technology.

In addition, the major importance of easy-to-use functionalities to backup and recover the account as fundamental step in the identity lifecycle does not seem to be understood by the developers. Its importance is not prominently highlighted in the applications — maybe as the functions currently are too complex for the average user and their practicality is debatable.

We want to conclude by highlighting the concern that even though such solutions are marketed as ready to be practically used, their usability and current state of the technology stack might deprive end users of experiencing the entire range of claimed privacy and security benefits. DIdM solutions that exist nowadays need to provide a solidified explanatory basis and carefully guide the user with a good user experience, for example through the interface. This requires an explanation that is beyond providing basic instructions on how to use certain functions but also providing clarification of why certain functions need to be carried out in one way, while solutions that are more traditional and familiar to users have been offering similar functions in another way. To sum up the results of our study, to

our knowledge the existing market does not yet offer Blockchain-based DIdM solutions with usability mature enough to be accepted and securely used by end users.

Acknowledgements Project DECIDE was funded and supported by the Next Generation Internet Initiative and was selected by the open call for proposals from the Partnership for innovative technological solutions to ensure privacy and enhance trust for the human-centric Internet — NGI TRUST (https://www.ngi.eu/ngi-projects/ngi-trust/).

References

1. MarketsandMarkets: Digital Identity Solutions Market Size, Share and Global Market Forecast to 2024. https://www.marketsandmarkets.com/Market-Reports/digital-identity-solutions-market-247527694.html
2. White, O.: Digital Identification: A Key to Inclusive Growth. McKinsey Global Institute, Washington, D.C (2019)
3. Kubach, M., Schunck, C.H., Sellung, R., Roßnagel, H.: Self-sovereign and Decentralized identity as the future of identity management? In: Open Identity Summit 2020, (GI-Edition - Lecture Notes in Informatics (LNI). Proceedings P-305), S. 35–47 Bonn, Köllen, (2020)
4. Simons, A.: Decentralized Digital Identities and Blockchain: The Future as We See it. https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/
5. Arun, J.S.: Reimagining the Future of Identity Management With Blockchain. https://securityintelligence.com/reimagining-the-future-of-identity-management-with-blockchain/
6. Introducing the European Blockchain Services Infrastructure (EBSI). https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi
7. SSI eIDAS Bridge reference Implementation. https://joinup.ec.europa.eu/solution/ssi-eidas-bridge-reference-implementation
8. Haenen, A., Jessen, J.: Sustainable hybrid financial services models. https://www.accenture.com/nl-en/blogs/insights
9. Smolenski, N.: Identity and Digital Self-Sovereignty. https://medium.com/learning-machine-blog/identity-and-digital-self-sovereignty-1f3faab7d9e3
10. Flechais, I., Mascolo, C., Sasse, M.A.: Integrating security and usability into the requirements and design process. Int. J. Electron. Secur. Digit. Forensics. **1**, 12–26 (2007)
11. U-Prove. https://www.microsoft.com/en-us/research/project/u-prove/?from=https%3A%2F%2 Fresearch.microsoft.com%2Fen-us%2Fprojects%2Fu-prove
12. Zibuschka, J., Hinz, O., Roßnagel, H., Muntermann, J.: Zahlungsbereitschaft für Föderiertes Identitätsmanagement. In: Der digitale Bürger und seine Identität. Nomos Verlagsgesellschaft mbH & Co. KG. S. 225–246 (2016)
13. Koçak, S.A., Alptekin, G.I., Bener, A.B.: Integrating Environmental Sustainability in Software Product Quality. Presented at the RE4SuSy@ RE (2015)

14. Khayretdinova, A., Kubach, M.: A methodology for experimental evaluation of a software assistant for the development of safe and economically viable software. In: Presented at the 15th International Conference on Web Information Systems and Technologies (2019)
15. Zibuschka, J., Roßnagel, H.: Stakeholder economics of identity management infrastructures for the web. In: Proceedings of the 17th Nordic Workshop on Secure IT Systems (NordSec 2012). Karlskrone, Sweden (2012)
16. Kubach, M., Roßnagel, H., Sellung, R.: Service providers' requirements for eID solutions: empirical evidence from the leisure sector. In: Hühnlein, D., Roßnagel, H. (eds.) Open Identity Summit 2013—Lecture Notes in Informatics (LNI)—Proceedings. S. 69–81. Ges. für Informatik, Bonn (2013)
17. Simons, A., Management, V.P. of P., Division, M.I.: Decentralized digital identities and blockchain: The future as we see it. https://www.microsoft.com/en-us/microsoft-365/blog/2018/02/12/decentralized-digital-identities-and-blockchain-the-future-as-we-see-it/
18. Aitken, R.: Blockchain To The Rescue Creating A 'New Future' For Digital Identities. https://www.forbes.com/sites/rogeraitken/2018/01/07/blockchain-to-the-rescue-creating-a-new-future-for-digital-identities/
19. Use case spotlight: Quick SSI integration for identity and access management with IdRamp, Use case spotlight: Quick SSI integration for identity and access management with IdRamp
20. Allen, C.: The Path to Self-Sovereign Identity. https://github.com/ChristopherA/self-sovereign-identity
21. Jessen, J., McLeese, V., van de Weerdt, M.: Identity management on blockchain: a new era of data privacy. https://www.accenture-insights.nl/en-us/articles/identity-management-on-blockchain
22. van Bokkem, D., Hageman, R., Koning, G., Nguyen, L., Zarin, N.: Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology. ArXiv190412816 Cs. (2019)
23. Wang, F., De Filippi, P.: Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion. Front. Blockchain. **2**, 1–22 (2020). https://doi.org/10.3389/fbloc.2019.00028
24. Mühle, A., Grüner, A., Gayvoronskaya, T., Meinel, C.: A survey on essential components of a self-sovereign identity. Comput. Sci. Rev. **30**, 80–86 (2018). https://doi.org/10.1016/j.cosrev.2018.10.002
25. Cameron, K.: The Laws of Identity. Microsoft Corporation (2005)
26. Lesavre, L., Varin, P., Mell, P., Davidson, M., Shook, J.: A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. National Institute of Standards and Technology (2020)
27. Kuperberg, M.: Blockchain-based identity management: a survey from the enterprise and ecosystem perspective. IEEE Trans. Eng. Manag. (2019). https://doi.org/10.1109/TEM.2019.2926471
28. The Importance of User Experience for Blockchain Applications. https://upvest.co/blog/the-importance-of-user-experience-for-blockchain-applications
29. Anderson, R., Moore, T.: The economics of information security. Science **314**, 610–613 (2006). https://doi.org/10.1126/science.1130992
30. Akerlof, G.A.: The Market for "Lemons": Quality Uncertainty and the Market Mechanism. Q. J. Econ. **488**, 235–251 (1970)

31. Kirlappos, I., Sasse, M.A.: What usable security really means : trusting and engaging users. Hum Asp Inf Secur Priv Trust HAS Lect Notes Comput Sci. **11** (2014)
32. Zurko, M.E., Simon, R.T., Street, S.: User-Center. Secur. **1**, 1–9 (1996)
33. Dunphy, P., Petitcolas, F.: A First Look at Identity Management Schemes on the Blockchain 2018 (2018)
34. Fischer-Hübner, S., Lacono, L., Möller, S.: Usable security und privacy. Datenschutz Datensicherheit - DuD. **34**, 773–782 (2010)
35. Prieto, L.P., Rodriguez-Triana, M.J., Kusmin, M., Laanpere, M.: Maybe poor Jhonny Really Cannot Encrypt—The Case for a Complexity Theory for Usa-ble Security. In: CEUR Workshop Proc. S. 53–59 (2017)
36. uPort—Tools for Decentralized Identity and Trusted Data. https://www.uport.me/
37. Products - Evernym's Verifiable Credential Platform. https://www.evernym.com/products/
38. W3C: Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/
39. Authentication. https://identity.foundation/working-groups/authentication.html
40. Schrepp, M., Hinderks, A., Thomaschewski, J.: Applying the User Experience Questionnaire (UEQ) in Different Evaluation Scenarios. In: Marcus, A. (ed.) Design, User Experience, and Usability. Theories, Methods, and Tools for Designing the User Experience. S. 383–392. Springer International Publishing, Cham (2014)
41. Schrepp, M., Hinderks, A., Thomaschewski, J.: Construction of a Benchmark for the User Experience Questionnaire (UEQ). IJIMAI. **4**, 40–44 (2017)
42. Laugwitz, B., Held, T., Schrepp, M.: Construction and evaluation of a user experience questionnaire. In: Symposium of the Austrian HCI and usability engineering group. S. 63–76. Springer (2008)
43. Roßnagel, H., Zibuschka, J., Hinz, O., Muntermann, J.: Users' willingness to pay for web identity management systems. Eur. J. Inf. Syst. **23**, 36–50 (2014). https://doi.org/10.1057/ejis.2013.33

Technische Ansätze

Ausprägungen von Uploadfiltern

Martin Steinebach

Zusammenfassung

Uploadfilter sind in der jüngeren Vergangenheit Gegenstand von zahlreichen Diskussionen geworden, die teilweise verschiedene Aus-prägungen dieser Systeme vermischen und oft nur unzureichend auf die Herausforderungen und Limitierungen eingehen. In diesem Beitrag soll daher das Thema strukturiert werden, um die Möglichkeiten und Risiken, die bei einem Einsatz von Uploadfiltern entstehen, zu strukturieren. Diese Filter können entweder Inhalte wiedererkennen, was vergleichsweise einfach ist und niedrige Fehlerraten aufweist, oder sie sollen auch Ähnlichkeit erkennen können, wodurch die Fehler ansteigen. Wiedererkennen ist eine beispielsweise Aufgabe bei Urheberrechtsverletzungen, Ähnlichkeit bei Hate Speech. Die Fehlerraten reichen dabei vom Promille bei zu zweistelligen Prozenten und haben dadurch deutliche Auswirkungen auf die Praktikabilität und Auswirkungen der Lösungen. So kann ein autonomer Einsatz in sozialen Medien zu einer hohe Anzahl Fehleinschätzungen führen, was wiederum manuelle Kontrolle erfordert.

Schlüsselwörter

Uploadfilter • Schwellwerte • Klassifizierung

M. Steinebach (✉)
Fraunhofer SIT, Darmstadt, Deutschland
E-mail: martin.steinebach@sit.fraunhofer.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_20

1 Einsatzszenarien von Uploadfiltern

Unter dem Begriff „Uploadfilter“ werden Systeme verstanden, die digitale Werke beim Hochladen auf die Plattform eines Onlinedienstes untersuchen und basierend auf dem Untersuchungsergebnis eine Entscheidung über die nachfolgende Verfahrensweise mit diesem Inhalt treffen. Bekannt ist dabei der Onlinedienst YouTube mit seinem Verfahren ContentID, welches hochgeladene Videoinhalte Rechteinhabern zuordnen kann und diesen verschiedene Möglichkeiten bietet, auf das Verwenden ihrer Inhalte zu reagieren. Aber auch ein Erotikfilter, der selbständig erotische oder pornographische Aufnahmen erkannt und deren Verbreitung auf einer Webseite oder einem Firmennetzwerk unterbindet sowie Methoden, die automatisiert Hasskommentare in Foren erkennen und ablehnen, können als Uploadfilter angesehen werden.

1.1 Schutz von Urheberrechten

Lösungen wie das bereits erwähnte ContentID sind sicher die bekanntesten Vertreter von Uploadfiltern, die bereits lange in der Praxis verwendet werden. Ihre Aufgabe ist es, urheberrechtlich geschütztes Material zu erkennen, welches auf eine Internetplattform angeboten werden soll. Dazu werden die zu filternden Materialen entweder im Vorhinein in einer geeigneten Form in einer Datenbank hinterlegt oder bei einer Urheberrechtsverletzung auf der Plattform im Nachhinein der Datenbank hinzugefügt. Solche Lösungen regieren nur auf inhaltlich identische Kopien, ein Konzept von Ähnlichkeit wird hier nicht verfolgt: Ein geschütztes Musikstück wird erkannt, nicht aber ähnlich klingende Werke oder andere Werke des gleichen Musikers.

1.2 Schutz von Persönlichkeitsrechten

Ähnlich wie bei Uploadfiltern zum Urheberschutz agieren Lösungen zum Schutz von Persönlichkeitsrechten. Sie sollen verhindern, dass einmal als verletzend erkannte Inhalte erneut verbreitet werden können, beispielsweise in sozialen Netzwerken. So kann ein kompromittierendes Foto an einer weiteren Verbreitung gehindert werden. Auch hier sollen nicht alle Aufnahmen einer Person gelöscht werden, ebenso nicht andere Fotos, die ähnliche Inhalte zeigen. Im Falle einer ungewollten Nacktaufnahme beispielsweise soll weder jedes Foto der gezeigten Person aus einem sozialen Netz entfernt werden, sondern nur das von ihr als verletzten empfundene.

Ebenso wenig sollen allerdings andere Fotos gelöscht werden, die einen vergleichbaren Grad von Nacktheit zeigen, was von anderen Personen aber gegebenenfalls gewollt ist.

1.3 Schutz vor Hate Speech

Beleidigende, verleumderische oder hetzende Kommentare sollen in sozialen Netzen und ähnlichen Umgebungen möglichst effizient entfernt werden. Wird eine entsprechende Äußerung gefunden, soll nicht nur diese gelöscht, sondern auch ihre Wiedereinstellung verhindert werden, und dabei möglichst auch alle Abwandlungen davon. Während die erste Variante, also das Erkennen einer Wiedereinstellung, den Uploadfiltern im Urheberechtsschutz gleicht, erfordert das Erkennen von Abwandlungen eine andere und komplexere Lösung. Hier kann nicht mehr eng zwischen einem Text und allen anderen denkbaren Texten unterschieden werden, sondern Texte sollen auch erkannt werden, wenn sie ausreichend ähnlich zu dem ursprünglichen Text sind.

1.4 Schutz gegen „Fake News“

Noch weiter gehen die Anforderungen bei der Erkennung von Desinformationen oder „Fake News“. Soll automatisiert eine Falschmeldung gefiltert werden, so ist ein System notwendig, welches autonom zwischen Wahrheit und Unwahrheit entscheiden kann. Weiterhin muss es in der Lage sein, den Kontext einer Aussage zu bewerten, da Desinformationen oft durch das verbreiten korrekter Sachverhalte in einem bewusst missverständlichen Zusammenhang entstehen. Ein System, welches dazu in der Lage ist, wäre das Ideal eines Uploadfilters gegen Desinformationen, hilfreich sind aber auch einfachere Ausprägungen, die den Ansätzen der vorherigen Abschnitte mehr ähneln und so technisch weniger anspruchsvoll sind.

1.5 Umsetzung

Uploadfilter sind eine verkürzte Bezeichnung für komplexe Systeme, in denen das eigentliche Filtern nur eine von vielen Komponenten ist. Entsprechende Lösungen müssen ja neben der Analyse beispielsweise auch die Umsetzungen der Reaktionen auf das Ergebnis der Analyse bereitstellen. Und bei dynamischen Vorgängen wie

insbesondere der „Fake News“ Erkennung auch eine Anbindung an Wissensquellen beinhalten. Wir beschränken uns an dieser Stelle auf die Herausforderungen der Umsetzung der grundsätzlichen Aufgabe wie in Abschn. 1.1. bis 1.4. beschrieben. Diese Funktionen lassen grob unterscheiden in solche, die ein Wiedererkennen von Inhalten wie in 1.1. und 1.2. ermöglichen und solche, die ein Klassifizieren beliebiger Inhalte wie in 1.3 und 1.4 ermöglichen.

Das Wiedererkennen bzw. (Re-Identifizieren) von Inhalten geschieht entweder über sogenannte robuste Hashverfahren oder über Verfahren zur Extraktion von Merkmalen („Features“). Entsprechende Verfahren erzeugen eine kompakte Darstellung des Inhalts und speichern diese in einer Datenbank. Zum Prüfen wird dann vom Medium mit derselben Methode ein weiterer Hash oder ein Merkmalsvektor errechnet und mit der Datenbank verglichen. Diese Methoden sind schnell und einfach zu berechnen, weiterhin weisen sie niedrige Fehlerraten auf. Entsprechende Verfahren sind in erster Linie für Multimedia Daten bekannt und werden für Bild, Video und Ton in zahlreichen Anwendungen eingesetzt. Aber auch für Text sind robuste Hashverfahren bekannt, womit Anforderungen in 1.3 adressiert werden können, bei denen Texte wiedererkannt werden sollen, auch wenn diese leicht abgeändert wurden.

Sollen Entscheidungen nicht für bereits bekannte Inhalte getroffen werden, sondern auch Inhalte bewertet werden, welche nur eine gewisse Ähnlichkeit zu bereits bekannten Inhalten aufweisen, so müssen diese klassifiziert werden. Dazu wird heute in der Praxis Maschinelles Lernen eingesetzt. Anhand von Beispielen wird dem System während des Trainings beigebracht, wie die Ausprägungen der zu erkennenden Inhalte sind und welche Einordnung erfolgen soll. Dann können neue Inhalte durch das so trainierte Netz klassifiziert werden. Die Herausforderung ist hier, dass es eine Vielzahl möglicher Texte und Nachrichten gibt, die alle auf die beschränkte Zahl von Trainingsdaten abgebildet werden müssen. Dementsprechend sind die Fehlerraten hier deutlich höher als im Wiedererkennen.

Der folgende Abschnitt betrachtet die Umsetzung von Uploadfiltern in einem höheren Detailgrad und greift dabei die Unterscheidung zwischen Wiedererkennen und Klassifizieren auf. Auch wird die technische Umsetzung der Uploadfilter etwas breiter betrachtet. Wichtig ist dabei die kurze Bestandsaufnahme der aktuellen Erkennungsraten, die im späteren Kapitel „Herausforderungen“ im Zusammenhang mit den Schwellwerten von großer Bedeutung ist.

2 Technologie

Ein Uploadfilter besteht aus eine Reihe von Komponenten. Abstrakt müssen dabei zumindest die folgenden Vorhanden sein:

Referenzdatenbank Anhand dieser Referenzdaten entscheidet der Uploadfilter, wie seine Reaktion ausfallen soll. Üblich ist hier eine Art „Blacklist“, in der die Fälle gespeichert sind, auf die der Uploadfilter mit weiteren Maßnahmen reagieren soll. Je nach Strategie zur Erkennung können die Daten beispielsweise zur effizienten Handhabe abstrahiert oder als Trainingsdaten für Maschinelles Lernen eingesetzt werden. Ebenso kann die Datenbank eine Liste von Signalworten zur Erkennung von Hassrede darstellen. Nur, wenn ein generelles Modell der zu erkennenden Daten gefunden werden kann, dann ist eine Referenzdatenbank nicht notwendig, beispielsweise, wenn Nacktheit anhand des Anteils von hautfarbenen Pixeln erkannt wird [1, 20]. Wenn die Reaktion auf erkannte Inhalte es erfordert, können hier auch weitere Metadaten hinterlegt sein, beispielsweise Kontaktadressen von Rechteinhabern zur Klärung von Nutzungsfragen.

Entscheidungsverfahren Im Kern des Uploadfilters muss immer die Frage geklärt werden, ob ein eingehendes Datum (also beispielsweise ein Bild, ein Text oder ein Video) eine Eigenschaft hat, die eine Reaktion erfordert. Diese Einordnung kann auf vielfältige Weise geschehen. Ihre Zuverlässigkeit ist dabei davon abhängig, wie hoch der Freiheitsgrad der eingehenden Daten in Bezug auf die Referenzdatenbank ist. Soll nur auf Inhalte reagiert werden, die genau so in der Datenbank vorhanden sind, ist ein zuverlässiger Betrieb möglich, als wenn auch den Referenzen ähnliche Inhalte erkannt werden sollen.

Reaktionsmechanismus Auf Basis der Entscheidung des Einordnungsverfahrens muss der Uploadfilter in der Lage sein, eine abhängige Handlung durchzuführen. Diese Reaktion kann wieder in Abhängigkeit vom Einsatzszenario vielfältig ausfallen. Zur Vermeidung von Urheberrechtsstreitigkeiten wird ein Inhalt vielleicht blockiert oder dem Rechteinhaber und dem Uploader zur Klärung übergeben. Ein Fall von vermeintlich erkannter Hassrede in einem sozialen Netzwerk wird dahingegen wahrscheinlich einem Moderator übergeben, der hier eine abschließende Entscheidung über Blockieren oder Veröffentlichung trifft.

2.1 Entscheidungsverfahren

Es gibt unterschiedliche Ansätze, die sich mit der Einordnung von Inhalten befassen, also im Kontext eines Uploadfilters die Aufgabe übernehmen, über einen eingehenden Inhalt eine Entscheidung zu treffen. Dabei unterscheiden sich die Verfahren für verschiedene Inhalte deutlich. Eine Lösung für Bilder ist nicht ohne weiteres auf Texte übertragbar. Auf der obersten Ebene lässt sich dies in zwei Gruppen einteilen:

Wiedererkennen Hier wird angenommen, das ein Inhalt bereits bekannt ist, z. B. aus einer früheren Untersuchung. Er soll re-identifiziert und mit einigen in einer Datenbank gespeicherten Informationen darüber abgeglichen werden. Diese kann beispielsweise durch kryptographische (üblich bei Texten) oder robuste Hashes (üblich bei Medien wie Audio, Video und Bild) geschehen. Es muss betont werden, dass es bei dieser Aufgabe darum geht, die Inhalte selbst zu identifizieren und nicht darum, weitere Informationen daraus zu gewinnen. So zählt die Aufgabe, in einem Bild eine abgebildete Person zu erkennen, wie z. B. in [6] besprochen, nicht zur hier diskutierten Re-Identifikation.

Klassifizierung In diesem Fall wird nicht davon ausgegangen, dass der Inhalt bereits bekannt ist. Statt dessen werden automatisch Metadaten generiert, z. B. durch Abgleich des Bildes mit Referenzbildern mit ähnlichen Merkmalen. Auf diese Weise kann ein Filtern nach relevanten Merkmalen erfolgen. Es existieren zahlreiche unterschiedliche Ansätze, wie beispielsweise Bilder klassifiziert werden können [11]. Für die Bildklassifikation sind trainierte tief lernende Netze bekannt, die die besten Ergebnisse [5] liefern. Es stehen mehrere allgemeine Netze zur Verfügung, die eine automatische Markierung oder Annotation von Bildern ermöglichen. Die eigentliche Entscheidung wird dann auf Basis der gewonnenen Annotationen gewonnen.

In den folgenden Abschnitten gehen wir auf eine Reihe von Methoden ein, mit denen Wiedererkennen und Klassifizierung umgesetzt werden können. Diese sind eher beispielhaft zu sehen. Ziel ist es, zu zeigen, wie unterschiedlich eine Einordnung erfolgen kann.

2.2 Kryptographische Hash-Funktionen

Kryptographische Hash-Funktionen (siehe z. B. [12]) sind ein Primitiv der Sicherheitsprotokolle mit vielen Anwendungen, die in der IT-Sicherheit schon sehr lange bekannt sind [4]. Sie berechnen Hash-Werte fester Länge aus Informationen belie-

biger Länge. Sie müssen eine Reihe von Anforderungen erfüllen, unter anderem die folgenden:

- Effizienz: Sie müssen mit geringem Aufwand berechnet werden können.
- Kollisionsresistenz: Es muss extrem unwahrscheinlich sein, zwei Informationen zu finden, die den gleichen Hash-Wert haben
- Einwegfunktion: Es muss praktisch unmöglich sein, die mit einem Hash-Wert verbundene Information zu finden.

Diese Eigenschaften führen dazu, dass Kryptographische Hash-Funktionen nur dazu geeignet sind, identische Kopien eines Inhalts, also beispielsweise eines Fotos oder eines Videos zu erkennen. Sobald auch nur minimale Änderungen an der Datei auftreten, die die Informationen speichert, ist der Hash ein vollständig anderer. Dazu genügt es, die Datei mit einem verlustbehafteten Kompressionsalogrithmus wie JPEG für Bilder oder h.264 für Videos zu speichern. Die dabei erfolgende Quantisierung führt zu Änderungen der Datei und einem Bruch des Hashes. Daher sind entsprechende Verfahren nicht geeignet, eine Re-Identifikation im Rahmen von Uploadfiltern zu ermöglichen. Sie spielen aufgrund ihrer Eigenschaften beispielsweise eine Rolle bei der Integritätsprüfung oder bei der Suche nach digitalen Duplikaten. Da im Kontext von Uploadfiltern immer mit Veränderungen der Inhalte gerechnet werden muss, sei es willentlich, um den Filter zu umgehen, oder unbewusst durch Verarbeitungsschritte, sind hier sogenannte „robuste“ Hashverfahren notwendig, die resistent gegen leichte Änderungen sind.

Sollten Texte re-identifiziert werden, kommen kryptographische Hashes allerdings häufig zum Einsatz. Sie werden dabei allerdings nicht als Hash über den vollständigen Text eingesetzt, sondern im Sinne einer fortlaufenden Fensterfunkion werden einzelne Textpassagen gehasht. So können auch Ausschnitte aus Texten erkannt werden. Mehr Details dazu finden sich beispielsweise in [23].

2.3 Robuste Hash-Funktionen

Es sind mehrere robuste oder wahrnehmungsbezogene Hashes für verschiedene Medientypen bekannt, die unterschiedliche Robustheitsgrade bieten. Da es zu viele Algorithmen gibt, um sie hier zu erwähnen, empfehlen wir Erhebungen wie die von Haouzia et al. [10] oder Neemila und Singh [14]. Es existieren auch Methoden für Audio [8]- und Videostreams [15] sowie für Textdaten [23].

Robuste Hash-Funktionen extrahieren wahrnehmungsrelevante Merkmale aus Multimedia-Inhalten zu Identifikationszwecken. Sie müssen eine Reihe von Anforderungen erfüllen. Die wichtigsten sind:

- Unterscheidung: Wahrnehmbar unterschiedliche Stücke von Mediendaten sollen unterschiedliche Hash-Werte haben
- Robustheit: Die robusten Hash-Werte sollen eine gewisse Wahrnehmungsinvarianz aufweisen, d. h. zwei Mediendaten, die für einen durchschnittlichen Zuschauer/Zuhörer hinsichtlich seiner Wahrnehmung ähnlich sind, sollen auch ähnlich sein.
- Sicherheit: Die Merkmale müssen Angriffe überstehen, die direkt auf die Merkmalsextraktion und nachfolgende Verarbeitungsschritte abzielen. Ähnlich wie bei kryptographischen Hash-Funktionen müssen die robusten Hash-Werte gleichmäßig auf alle möglichen Mediendaten verteilt und paarweise statistisch unabhängig für zwei Mediendaten sein, die sich in der Wahrnehmung unterscheiden.

Die Robustheit birgt das Risiko von Informationslecks: Wenn zwei Bilder sehr ähnlich sind, sind auch ihre Hashes ähnlich. Die Unterscheidung geht nur so weit, dass zwei ähnliche Bilder keinen identischen Hash haben, aber beide Hashes ähnlicher sind als die Hashes von zwei Bildern mit unterschiedlichem Inhalt. Als Beispiel: Porträtfotos mit einem menschlichen Gesicht in der Mitte und einem hellen, einfarbigen Hintergrund haben alle eine ähnliche robuste Hash-Struktur. Dies führt zu falsch-positiven Ergebnissen bei einer robusten Hash-Funktion, die höher als erwartet ist, wenn man den theoretischen Zahlenraum betrachtet, der von einem Hash überspannt wird.

Die Zuverlässigkeit robuster Hashverfahren bei der Wiedererkennung ist hoch. So weist beispielweise und Verfahren aus [24] in dem dort durchgeführten Test eine Falsch-Positiv-Rate von 0 % und eine Falsch-Negativ-Rate von 0.2 % auf.

2.4 Feature Matching

Verfahren, die Feature Matching umsetzen, zeichnen sich durch eine höhere Resistenz gegen Bildveränderungen als robuste Hashverfahren aus. Rotation und auch Verzerrung können sie gut überstehen, und auch eine Beschneiden des Bildes ist oft unproblematisch. Die Verfahren basieren darauf, sogenannte Schlüsselpunkte (Keypoints) an mehreren Stellen in einem Bild mit einem Detektor zu erkennen und Deskriptoren mit einem Merkmals-Extraktor zu extrahieren. In einem weiteren Schritt, dem Merkmalsvergleich, werden die gefundenen Merkmale mit Merkmalen

eines anderen Bildes verglichen. Wenn beide Bilder nun das gleiche Objekt enthalten, sollten die Merkmale idealerweise messbar ähnlich sein. Ein Merkmal selbst ist definiert als ein "interessanter" Teil des Bildes. Was genau als "interessanter" Teil des Bildes verstanden wird, variiert je nach Merkmalsdetektor. Der Bildteil, in dem ein Merkmal extrahiert wird, ist oft entweder ein isolierter Punkt, eine kontinuierliche Kurve oder ein verbundener Bereich.

Der Scale Invariant Feature Transform (SIFT) [13] Algorithmus ist einer der bekanntesten und am häufigsten verwendeten Merkmals-Detektoren. Der Speeded Up Robust Features (SURF) Detektor [2] ist teilweise von SIFT inspiriert und ist ein Versuch, schneller und robuster zu sein als SIFT.

Die Verfahren ist allgemein aufwändiger als robuste Hashverfahren und werden daher nur dann eingesetzt, wenn die Anwendung die Resistenz gegen Rotation und Verzerrung erfordert. Auch bei der Erkennung von einzelnen Teilen es Bildes oder dem Einfügen eines Bildes in ein anderes, können diese Verfahren hilfreich sein. So wurden von uns im Rahmen der Erkennung von Bildmontagen 99 % der eingefügten Bildobjekten und 100 % der Bildhintergründe, in denen die Objekte eingefügt wurden, erkannt [21, 22].

2.5 Natural Language Processing

Unter diesem Begriff fallen zahlreiche Ansätze, Informationen aus unstrukturiertem Text zu gewinnen. Methoden reichen dabei von statistischer Analyse des Auftretens von vorher bestimmten Signalworten bis hin zur Erkennung von Kontext oder Autorenschaft anhand Maschinellem Lernens.

Welche Ansätze hier eingesetzt werden, kommt wieder auf die konkrete Anwendung an. Soll durch einen Filter verhindert werden, dass ein einmal geblockter Nutzer erneut Inhalte über einen neuen Nutzernamen hochladen kann, so ist dies eine Aufgabe für die Autorschaftserkennung. Der Schreibstil des geblockten Verfassers wird erlernt und dann neue Texte auf diesen Stil hin geprüft. Dabei wurde beispielsweise in [9] für deutschsprachige Texte eine Accuracy von 79 % erreicht.

Soll verhindert werden, dass Bots Nachrichten in einem Kanal verbreiten können, müssen Bots und Menschen unterschieden werden. Bei der PAN-Challenge, einem internationalen Vergleich von Natural Language Processing Lösungen, lag die die durchschnittliche Erkennungsrate bei einer Unterscheidung zwischen Nachrichten von einem Bot und einem Menschen bei 86 % in englischer Sprache[17].

Ist die Aufgabe, bestimmte Inhalte aus einem Forum herauszuhalten, sind Ansätze notwendig, die eher inhaltlich agieren und unabhängig vom Autor sind.

So konnten im Projekt X-SONAR Inhalte mit „Hate Speech“ in Twitter Nachrichten zu 85 % korrekt erkannt werden [27].

Die Erkennung von Verbreitern von Desinformationen gelang in der entsprechenden PAN-Challenge [16] dem Gewinner [3] mit einer durchschnittlichen Accurarcy von 77,8 %. Auch Lösungen, die auf einfachen Mechanismen wie n-Grammen und Support Vector Machines basieren [26], erreichten eine Accurarcy von über 75 % . Die Liste von technischen Komponenten, mit denen ein Uploadfilter Inhalte verarbeiten kann, ist beliebig erweiterbar. So kann eine Klassifizierung natürlich auch für Videos erfolgen, und auch hier wird heute verbreitet Maschinelles Lernen eingesetzt [25]. Selbst Cover-Versionen von Musikstücken können automatisch erkannt werden, wenn ein System die Audiodaten in Noten übersetzt [28] und dann die Notenfolgen in einer Referenzdatenbank sucht. Letztendlich kann jedes Verfahren, welches automatisiert Metadaten aus einem Inhalt extrahieren kann, potentiell im Rahmen eines Uploadfilters verwendet werden, wenn die Metadaten relevant für die Entscheidung des Filters sind.

2.6 Komplikationen

In der Praxis können die Methoden zur Erkennung auf vielfältige Herausforderungen stoßen, die ihren Einsatz deutlich erschweren. Die oben genannten Ansätze gehen zumeist davon aus, dass der zu untersuchende Inhalt direkt zur Analyse zur Verfügung steht. Allerdings ist dies schon bei relative einfachen Fällen wie der Erkennung von urheberrechtlich geschützten Inhalten auf Videoplattformen oft nicht der Fall. Musikstücke können mit einem robusten Hashverfahren nur schwer erkannt werden, wenn sie im Hintergrund laufen und durch eine Moderation verdeckt werden. Ein Film wird eventuell nicht mehr erkannt, wenn er nur in einem Fenster im Hintergrund läuft oder ein Kommentator im Vordergrund eingeblendet wird.

Dementsprechend müssen die Verfahren wo notwendig durch weitere Mechanismen unterstützt werden. Dazu sind ebenfalls zahlreiche Verfahren bekannt. So können Audioströme separiert werden, also vermischte Klangquellen wieder getrennt werden [7]. Bilder können in Segmente aufgeteilt werden, die individuell betrachtet werden; in Videos kann Vorder- und Hintergrund getrennt betrachtet werden. Auch Verfahren zur Erkennung von Bildern in einem größeren Bild existieren. Sie alle haben gemeinsam, dass ihr Einsatz die Systeme komplexer werden lässt und natürlich auch die Fehlerraten erhöht.

Nicht vergessen werden darf auch, dass Nutzer, die Inhalte hochladen, diese aktiv vor einer Erkennung schützen wollen. Sie verschleiern also den Inhalt. Für

alle oben genannte Methoden existieren auch Ansätze, mit denen diese in die Irre geführt werden sollen. Bekannt sind hier die Bemühungen von Nutzern der Videoplattform YouTube, Inhalte durch Spiegelung oder verlangsamte Wiedergabe vor einer Erkennung zu verbergen. In jüngerer Zeit wurde auch hier Ansätze des Maschinellen Lernens betrachtet [19].

3 Herausforderung Schwellwert

In der Diskussion über Uploadfilter werden deren technische Ausprägungen und Eigenschaften oft nicht berücksichtigt. Systeme, die auf Wiedererkennen basieren, weisen deutlich niedrigere Fehlerraten auf (zumeist unter einem Prozent) auf, als solche, die mit Maschinellem Lernen Inhalte klassifizieren. Hier liegen die Fehlerraten oft über 10 %. Trennt man hier beide Ansätze in der Diskussion nicht deutlich voneinander, können unrealistische Erwartungen hinsichtlich des Einsatzes von Uploadfiltern entstehen: Ein Erkennen von „Hate Speech“ oder „Fake News“ kann heute nicht mit der gleichen Zuverlässigkeit und daher Automatisierung arbeiten wie ContentID in YouTube, bei der Inhalte wiedererkennt werden.

Gleichzeitig sind allerdings die Anforderungen an Uploadfilter zu „Hate Speech“ und „Fake News“ höher als die bei der Wiedererkennung von Inhalten. Ein entsprechender Filter müsste alle Nachrichten in sozialen Netzwerken untersuchen und bewerten. Hier kann mit einem Vielfachen der Anzahl von hochgeladenen Bildern und Videos gerechnet werden. Damit gewinnt die Fehlerrate dieser Verfahren weiter an Bedeutung, da die Betreiber Sozialer Medien mit einer Vielzahl generierter Warnungen ihrer Uploadfilter konfrontiert werden, von denen ein großer Anteil falsch klassifiziert ist. Gehen wir beispielsweise davon aus, dass von 1000 Nachrichten eine „Hate Speech“ enthält, so fallen bei grob 90 % korrekter Erkennung hier bei einer Million Nachrichten 900 korrekte Meldungen an. Gleichzeitig werden aber auch von den restlichen 999.000 Nachrichten 10 % falsch klassifiziert und lösen ebenfalls einen Alarm aus. Auf die 900 korrekten Meldungen kommen also 99.000 Fehleinschätzungen. Würde nun ein System voll automatisiert ablaufen, würden bei diesen Werten 10 % aller Nachrichten fehlerhaft blockiert. Prüfen Menschen die Meldungen, so entsteht ein hoher personeller Aufwand.

Diese Werte können allerdings angepasst werden. Über eine Klassifizierung wird zumeist mit Schwellwerten entschieden: Eine Zuordnung geschieht, wenn ein trainiertes Netz sich zu einem gegebenen Prozentsatz sicher ist. So kann beispielsweise festgelegt sein, dass ein Netz sich zu 80 % sicher sein muss, dass ein Text „Hate Speech“ ist, um diesen entsprechend einzuordnen. So wird aus einer prozentualen eine binäre Entscheidung. Wird dieser Schwellwert verändert, geschehen zwei

Dinge: Die Erkennungsrate echter Treffen sinkt, da weniger Treffer den Schwellwert überschreiten und zu einer Meldung führen. Gleichzeitig fällt aber die Anzahl der falsch als Treffen eingeordneten Beispiele, da auch diese häufiger am Schwellwert scheitern.

Dementsprechend kann ein Uploadfilter parametrisiert werden, um entweder möglichst wenig Fehlalarm auszulösen oder aber möglichst zuverlässig im Ernstfall eine Meldung zu erkennen. Die Entscheidung, wie viel Aufwand bei einer manuellen Nachsichtung anfällt, ist direkt davon abhängig. Ebenso bei einem automatischen Betrieb die Frage, wie viel Störung in der Nutzung eines Sozialen Netzwerks durch falsch eingeordnete Meldungen akzeptiert werden, um zuverlässig unerwünschte Inhalte auszusperren. Um die Bedeutung und das Verhalten von Schwellwerten besser darzustellen, erfolgt hierzu ein etwas ausführlicher Exkurs.

Schwellwerte stellen die Entscheidungsgrenzen für eine Einordnung eines Uploadfilters dar.

$$Entscheidung(x) = \begin{cases} Ablehnung: & x < Schwellwert \\ Annahme: & x \geq Schwellwert \end{cases}$$

Dabei kann der Wert x, auf dem die Entscheidung beruht, aus unterschiedlichen Berechnungen stammen. Im Falle eines robusten Hashverfahrens ist das beispielsweise die Hamming Distanz, also die Anzahl der Bits, an denen sich zwei Hashwerte unterscheiden. Hier liegt der Schwellwert oft bei einem prozentualen Anteil der Anzahl der Bits des Hashwerts. So legen Haitsma et al. [8] für ihren Audiohash den Schwellwert bei 75 % Übereinstimmung fest. Bei einem auf Maschinellem Lernen basierenden Klassifikator ist der Schwellwert erlernt und repräsentiert die Stärke der Übereinstimmung des geprüften Datums mit dem Erlernten. Ganz allgemein kann die Entscheidung positiv oder negativ ausfallen, also eine Annahme oder eine Ablehnung erfolgen. Diese Entscheidung kann richtig oder falsch sein. So entstehen vier Klassen von Entscheidungen:

Richtig Positiv (TP):	korrekte Annahme
Falsch Positiv (FP):	fehlerhafte Annahme
Richtig Negativ (TN):	korrekte Ablehnung
Falsch Negativ (FN):	fehlerhafte Ablehnung

Anhand dieser Klassen wird die Erkennungsleistung eines Einordnungsverfahrens bewertet. Oft wird dazu ein prozentualer Wert berechnet, beispielsweise, wie viele

Positiv-Beispiele von einhundert Fällen korrekt erkannt werden. Dies bezeichnet man dann als „Rate“, aus TP wird eine TPR (True Positive Rate). Zusätzlich werden auch abgeleitete bzw. zusammenfassende Werte verwendet. So gibt die häufig genannte „accurarcy“ an, wie viele aller Entscheidungen richtig waren, „precision“ beschreibt, wie viele aller positiven Einordnungen korrekt waren und „recall“, wie viele positive Fälle erkannt wurden. Welcher Wert hier relevant ist, kommt stark auf die jeweilige Anwendung an.

Um die Auswirkung eines Schwellwerts zu zeigen, verwenden wir an dieser Stelle ein abstraktes Beispiel. Wir erzeugen zwei Mengen A und B von Daten, die vermischt und später durch eine Analyse getrennt werden sollen. Das könnten Bilder sein, die durch ein robustes Hashverfahren erkannt werden sollen und bei dem eine Menge die bekannten und die andere die unbekannten Bilder darstellt. Oder Bilder von Katzen und Hunden, die ein trainiertes Netz klassifizieren soll, also dem Bild die Annotation „Hund“ oder „Katze“ zuweisen soll. In Tab. 1 werden einige Charakteristika der Daten aufgezeigt. Erzeugt wurden sie durch einen Generator für Zufallszahlen, der für beide Gruppen unterschiedliche Parameter verwendete. Bei den Daten handelt es sich um jeweils 100 Werte für jede Gruppe. Die entstehenden Werte dienen direkt als Grundlage für die Entscheidung hinsichtlich des Schwellwerts.

Abb. 1 zeigt, dass die Erkennung gut gelingt, beide Mengen sind getrennt. Es wird allerdings deutlich, dass es keinen Schwellenwert geben kann, der beide Gruppen vollständig voneinander abgrenzt. Abhängig vom Schwellwert werden einzelne Elemente der Gruppen jeweils der anderen zugeordnet. Im Fall eines Uploadfilters würden die Elemente der beiden Gruppen Inhalte repräsentieren, die vom Filter entweder durchgelassen oder gesondert behandelt werden müssten. Gruppe B wären die Inhalte, die der Filter erkennen sollte, Gruppe A die, die er als unbedenklich ansehen sollte.

Eine Darstellung des Problems bietet Abb. 2. Hier ist die Verteilung der Testergebnisse in Abhängigkeit vom Schwellenwert gestapelt. Bei einem zu hohen Schwellenwert von 100, dem Maximum, welches in den Daten auftritt, werden fast

Tab. 1 Statistische Eigenschaften der zwei Gruppen zu je 100 Testdaten

	Gruppe A	Gruppe B
Maximum	85,89	100
Minimum	62	85,05
Mittelwert	73,01	91,90

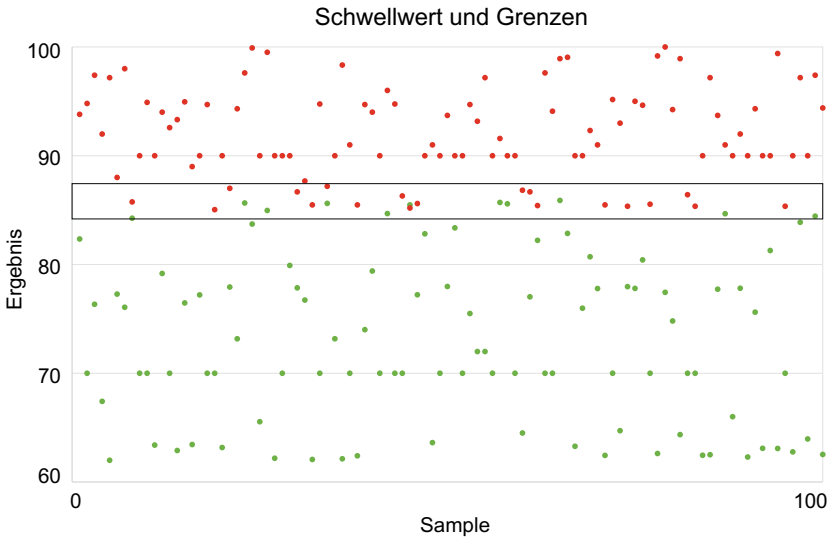


Abb. 1 Eine Verteilung von positiven und negativen Testfällen. Die beiden Mengen sind gut getrennt, an ihrer Grenze gibt es aber Überschneidungen. Betrachtet man die Grenze zwischen beiden Mengen um den Wert 85 herum, wird deutlich, dass es keinen Schwellenwert geben kann, der beide Mengen trennt, ohne dabei entweder FP oder FN zu produzieren

alle Elemente aus Gruppe B fälschlich abgelehnt, es ergibt sich ein großer Anteil von falsch-negativen. Gleichzeitig sind alle Elemente von Gruppe A negativen Daten korrekt zugeordnet. Bei einem Schwellenwert, der unter dem Minimum der Werte von Gruppe A Datensatzes liegt, werden hingegen alle Elemente von Gruppe B korrekt zugeordnet, alle Elemente von Gruppe A aber fälschlich als zu Gruppe B gehörig angesehen.

Die Herausforderung ist es nun, einen Schwellwert zu finden, der für den Zweck des jeweiligen Uploadfilters geeignet ist. Dazu müssen zumindest zwei Fragen bedacht werden:

Welche Annahme kann über die in der Praxis vorkommende Verteilung der Gruppen getroffen werden? In unserem Beispiel ist diese Verteilung gleich. In der Praxis ist es üblich, dass eine Gruppe deutlich größer als die andere ist. Daraus folgt eine Verzerrung des Verhaltens des Filters. Wenn beispielsweise ein Bild einer Katze zu 99 % erkannt werden kann, wenn es wirklich eine Katze zeigt, aber auch in 5 % der Fälle, in denen keine Katze zu sehen ist, fälschlich eine Katze erkannt wird,

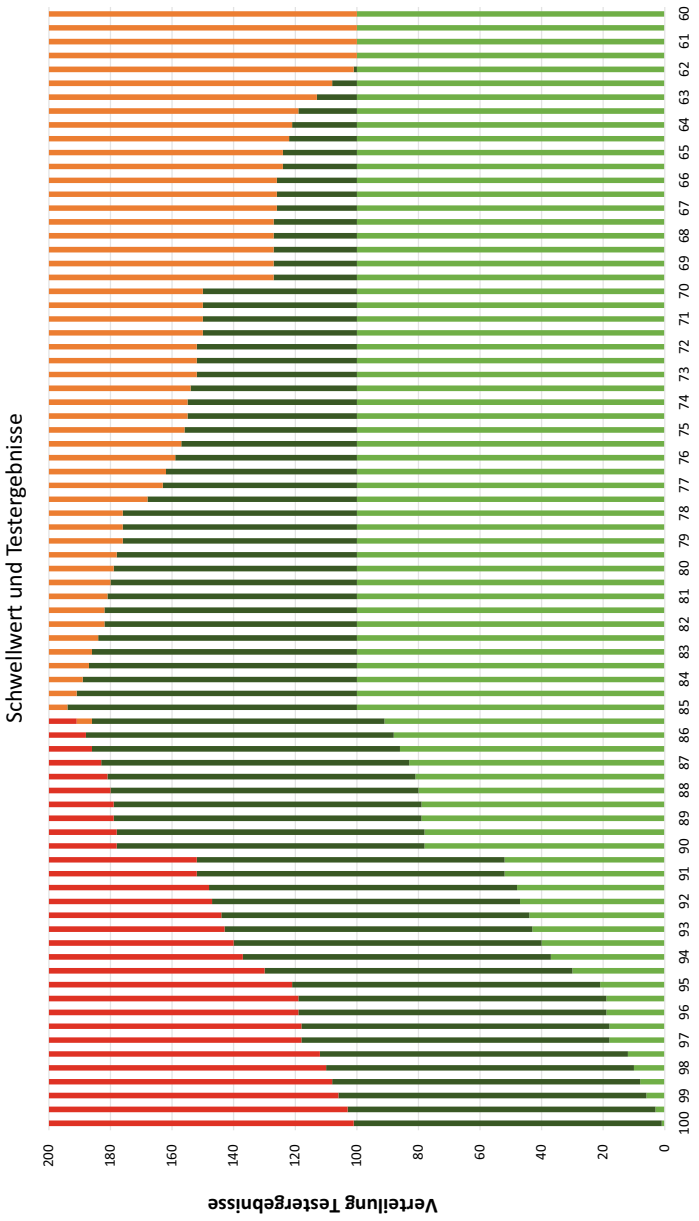


Abb. 2 Die Verteilung von TP, TN, FN und FP verschiebt sich in Abhängigkeit vom Schwellenwert

dann können diese 5 % schnell zu einem häufigeren Grund für das (vermeintliche) Erkennen einer Katze werden. Ist beispielsweise nur jedes tausendste Bild wirklich von einer Katze, so würde durch korrekte Erkennung einmal eine Katze erkannt werden, aber durch Fehlalarme 50 weitere Bilder hinzukommen.

Welche Bedeutung hat eine falsche Zuordung? Je nach Anwendung kann eine Ausprägung von Fehlern bei der Zuordnung weniger relevant als der andere sein. Sollen Hasskommentare aus Nachrichten ferngehalten werden, so kann es in der Praxis notwendig sein, eine gewisse Wahrscheinlichkeit des Scheiterns der Filterung zu akzeptieren, um zu verhindern, dass zu viele an sich unbedenkliche Mitteilungen fälschlich blockiert werden.

4 Diskussion

Die vorhergehenden Kapitel umreißen verschiedene Anwendungsfälle und Technologien zu Uploadfiltern und erörtern dann die Herausforderungen, die beim definieren von Schwellwerten auftreten. An dieser Stelle soll nun kurz erörtert werden, welche Konsequenzen das Zusammenspiel dieser Faktoren hat.

Uploadfilter haben unweigerlich in Abhängigkeit ihrer Aufgaben eine unterschiedliche Zuverlässigkeit. Sollen nur Werke wiedererkannt werden, die vollständig und unverändert vorliegen, so können Systeme mit einer vernachlässigbaren Fehlerrate erreicht werden. Das gilt allerdings nur in technischer Hinsicht, ein Uploadfilter kann nicht prüfen, welche Rechte am Werk tatsächlich bestehen [18]. Sobald allerdings zusätzliche Anforderungen hinzukommen, beispielsweise durch Verdeckung oder das Erkennen auch kleiner Ausschnitte eines Werkes, steigen auch die Fehlerraten. Daher darf ein Uploadfilter zum Urheberrechtsschutz nicht als trivial angesehen werden, denn in der Praxis treten zahlreiche Komplikationen bis hin zur bewussten Verschleierung von Werken als Maßnahme gegen eine Erkennung auf.

Sollen Werke in diesem Kontext dann trotzdem erkannt werden, so müssen die Schwellwerte ihrer Wiedererkennung gesenkt werden. Nun werden auch Kopien der Werke erkannt, die zu einem gewissen Grad von den ursprünglichen Werken abweichen. Das führt aber auch dazu, dass das Risiko steigt, ähnliche Werke, für die kein Urheberrechtsschutz besteht, fälschlich als das gesuchte Werk zu erkennen. Daraus folgen Fehlalarme und fälschliche Sperrungen von Inhalten.

Ähnliches gilt für den Schutz von Persönlichkeitsrechten. Ein Foto oder ein Video, dass von einer Person erstellt und unerlaubt verbreitet wird, ist technisch nicht von einem urheberrechtlich geschützten Werk zu unterscheiden und kann mit

den identischen Methoden behandelt werden. Auch hier spielt der Schwellwert eine entscheidende Rolle. Die betroffene Person wird ihn möglichst niedrig ansetzen wollen, um sicher zu stellen, dass auch stark veränderte Kopien zuverlässig blockiert werden. Betreiber von Plattformen hingegen wollen gegebenenfalls verhindern, dass zu viele Inhalte blockiert werden und dadurch Kundenunzufriedenheit auslösen.

Bei Aufgaben wie dem Schutz vor Hate Speech oder Desinformationen gibt es im Gegensatz zu den beiden ersten Anwendungsfällen keine direkte Referenz. Hier soll im Vorhinein auf etwas reagiert werden, das inhaltlich gewisse Eigenschaften hat, und nicht nur eine bestimmte Nachricht aus dem Kontext blockiert werden. Letzteres wäre natürlich auch umsetzbar: Geht es nur darum, eine bereits als Hate Speech oder Desinformation erkannte Nachricht, ein Bild oder ein Video nicht weiter zu verbreiten, so können die Methoden der Wiedererkennung eingesetzt werden und die Zuverlässigkeit der technischen Umsetzung steigt.

Gilt es allerdings, ganz allgemein Inhalte mit bestimmten Eigenschaften zu erkennen, steigen die Fehlerraten wie im Kapitel Technik beschrieben stark an und liegen dann durchaus bei über 20 %. Das ist primär dem Umstand geschuldet, dass die Erkennung entsprechender Nachrichten sehr komplex sein kann. Eine direkte Beleidigung durch Schimpfworte oder bekannte Phrasen kann noch automatisiert erkennbar sein, allerdings können auch hier schnell Fehler im Kontext entstehen. Werden beispielsweise Schimpfworte in einem Kommentar gezählt und der Verfasser bemängelt nur die Verwendung dieser, so kann es hier schnell zu einer fälschlichen Blockade kommen. Eher verdeckte Angriffe hingegen stellen eine Erkennung vor große Herausforderung.

Das Problem von Kontext und Verdeckung steigert sich bei Desinformationen noch weiter. Da Desinformationen potentiell über jeden Sachverhalt verbreitet werden können, sind hier Methoden notwendig, die völlig unabhängig vom Kontext sind. Und da Desinformationen häufig auch durch das Weglassen von Informationen entstehen, müsste ein Detektor auch ein Idee eines vollständigen Sachverhalts entwickeln können, um das Fehlen von Fakten zu erkennen.

Es wird deutlich, dass eine einfache Antwort auf die Umsetzung von Uploadfiltern nicht möglich ist, insbesondere, wenn der Begriff weit gefasst wird und sich über alle genannten Szenarien erstreckt. Dementsprechend stellen sich zahlreiche Fragen, von denen zum Schluss drei Stück exemplarisch herausgegriffen werden sollen. Anhand dieser Fragen sollte eine vertiefte Diskussion über den Einsatz von Uploadfiltern erfolgen. Als Grundlage dazu muss eine realistische Einschätzung der technischen Möglichkeiten vorhanden sein, die Beantwortung kann allerdings nur interdisziplinär erfolgen. Dementsprechend kommt der Technik hier die Aufgabe zu, ein Verständnis für die Arbeitsweisen, Voraussetzungen und Entscheidungsfindungen der verschiedenen Verfahren zu vermitteln. Um eine fundierte Entscheidung

über die Verwendung von Uploadfiltern treffen zu können, muss allen Beteiligten bekannt sein, welche Eigenschaften diese haben, welche Kosten entstehen und wo derzeit die Grenzen des technisch Machbaren sind.

Wie kann zwischen Wirtschaftlichkeit und Zuverlässigkeit entschieden werden? Selbst bei den Filtern für Urheberrechtsfälle ist es so, dass eine maximale Erkennung von urheberrechtlich geschütztem Material mit einer hohen Zahl von Falsch-Positiven einhergehen muss. Hier ist eine Abwägung zwischen dem Schutz der Rechteinhaber und den Interessen des Beitreibers und seiner Nutzer notwendig, da Fehler zu hohem Arbeitsaufkommen und potentiellem Abwandern von Nutzer führen werden.

Welcher Anspruch wird an Uploadfilter gestellt? Sollen Uploadfilter dem Stand der Technik genügen, so muss im Falle von Hate Speech und Desinformationen akzeptiert werden, dass eine automatische Lösung noch immer zahlreiche Fehler machen wird und einen Teil der zu blockierenden Inhalte nicht erkennt. Dies entspricht dem Stand der Technik. Alternativ könnten Qualitätsmaße gefordert werden, die den Stand der Technik überschreiten und nur durch manuelle Zuarbeit umsetzbar sind, beispielsweise durch niedrige Schwellwerte und menschliche Kontrolle.

Wie hoch ist das Risiko einer automatisierten Zensur? Es ist bekannt, dass bei Algorithmen des Maschinellen Lernens die Gefahr besteht, Vorurteile aus Trainingsdaten zu übernehmen und diese dann unreflektiert anzuwenden. Daher muss es beim Einsatz von Klassifizierungsverfahren, die darüber entscheiden sollen, ob Inhalte blockiert werden sollen, nicht nur auf eine allgemein hohe Korrektheit geachtet werden, sondern auch darauf, dass keine Mindermeinungen benachteiligt werden.

Danksagung Diese Forschungsarbeit wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Literatur

1. Ap-Apid, R.: An algorithm for nudity detection. In: 5th Philippine Computing Science Congress, S. 201–205 (2005)
2. Bay, H., Tuytelaars, T., Van Gool, L.: Surf: Speeded up robust features. In: European Conference on Computer Vision, S. 404–417. Springer, Berlin (2006)

3. Buda, J., Bolonyai, F.: An ensemble model using n-grams and statistical features to identify fake news spreaders on twitter. In: CLEF (2020)
4. Damgård, I.B.: Collision free hash functions and public key signature schemes. In: Workshop on the Theory and Application of of Cryptographic Techniques, S. 203–216. Springer, Berlin (1987)
5. Druzhkov, P., Kustikova, V.: A survey of deep learning methods and software tools for image classification and object detection. Pattern Recogn. Image Anal. **26**(1), 9–15 (2016)
6. Gong, S., Cristani, M., Loy, C.C., Hospedales, T.M.: The re-identification challenge. In: Person Re-identification, S. 1–20. Springer, London (2014)
7. Gu, R., Zhang, S.X., Xu, Y., Chen, L., Zou, Y., Yu, D.: Multi-modal multi-channel target speech separation. IEEE J. Selected Topics Sig. Process 14, 530–541 (2020)
8. Haitsma, J., Kalker, T., Oostveen, J.: Robust audio hashing for content identification. In: International Workshop on Content-Based Multimedia Indexing. Bd. 4, S. 117–124. CiteSeer (2001)
9. Halvani, O., Winter, C., Pflug, A.: Authorship verification for different languages, genres and topics. Digital Invest. **16**, S33–S43 (2016)
10. Haouzia, A., Noumeir, R.: Methods for image authentication: a survey. Multimedia Tools Appl. **39**(1), 1–46 (2008)
11. Kamavisdar, P., Saluja, S., Agrawal, S.: A survey on image classification approaches and techniques. Int. J. Adv. Res. Comput. Commun. Eng. **2**(1), 1005–1009 (2013)
12. Katz, J., Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
13. Lowe, D.G.: Distinctive image features from scale-invariant keypoints. Int. J. Comput. Vision **60**(2), 91–110 (2004)
14. Neelima, A., Singh, K.M.: A short survey on perceptual hash function. ADBU J. Eng. Technol. **1** (2014)
15. Oostveen, J.C., Kalker, T., Haitsma, J.: Visual hashing of digital video: applications and techniques. In: Applications of Digital Image Processing XXIV. Bd. 4472, S. 121–131. International Society for Optics and Photonics (2001)
16. Rangel, F., Giachanou, A., Ghanem, B., Rosso, P.: Overview of the 8th author profiling task at pan 2020: profiling fake news spreaders on Twitter. In: CLEF (2020)
17. Rangel, F., Rosso, P.: Overview of the 7th author profiling task at pan 2019: Bots and gender profiling in twitter. In: Proceedings of the CEUR Workshop, Lugano, Switzerland, S. 1–36 (2019)
18. Reda, J.: Edit policy: Verschärfungen bei der urheberrechtsreform in Deutschland (2020)
19. Saadatpanah, P., Shafahi, A., Goldstein, T.: Adversarial attacks on copyright detection systems. arXiv:1906.07153 (2019)
20. Santos, C., dos Santos, E.M., Souto, E.: Nudity detection based on image zoning. In: 2012 11th International Conference on Information Science, Signal Processing and their Applications (ISSPA), S. 1098–1103. IEEE, Piscataway, NJ (2012)
21. Steinebach, M., Katarina, B., Rinsdorf, L., Krämer, N., Roßnagel, A. (Hrsg.): Desinformation aufdecken und bekämpfen - Interdisziplinäre Ansätze gegen Desinformationskampagnen und für Meinungspluralität. Nomos, Baden-Baden (2020)
22. Steinebach, M., Gotkowski, K., Liu, H.: Fake news detection by image montage recognition. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, S. 1–9 (2019)

23. Steinebach, M., Klöckner, P., Reimers, N., Wienand, D., Wolf, P.: Robust hash algorithms for text. In: IFIP International Conference on Communications and Multimedia Security, S. 135–144. Springer, Heidelberg (2013)
24. Steinebach, M., Liu, H., Yannikos, Y.: Forbild: Efficient robust image hashing. In: Media Watermarking, Security, and Forensics 2012. Bd. 8303, S. 83030O. International Society for Optics and Photonics (2012)
25. Tran, D., Wang, H., Torresani, L., Feiszli, M.: Video classification with channel-separated convolutional networks. In: Proceedings of the IEEE International Conference on Computer Vision, S. 5552–5561 (2019)
26. Vogel, I., Meghana, M.: Fake news spreader detection on twitter using character n-grams. In: CLEF (2020)
27. Vogel, I., Regev, R., Steinebach, M.: Automatisierte analyse radikaler inhalte im internet. INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik–Informatik für Gesellschaft (2019)
28. You, W., Dannenberg, R.B.: Polyphonic music note onset detection using semi-supervised learning. In: ISMIR, S. 279–282. CiteSeer (2007)

Modell der Reichweitenhierarchie: Gestaltungsdimensionen digitaler Souveränität

Alexander Schäfer

Zusammenfassung

Die gesetzgeberische Reichweite eines Staates ist die Voraussetzung zur Gewährleistung der Durchsetzung bestimmter Rechte. Die digitale Souveränität endet mit der Abgabe rechtlicher Durchsetzung. Falls Datensouveränität nicht gewährleistet werden kann, ergeben sich Problemfelder. Im folgenden Paper werden zunächst zwei der vorhandenen Problemfelder (Pattern of Life – Analyse und Industriespionage) erläutert und so die Notwendigkeit aufgezeigt, die einer digitalen Souveränität obliegt. Um diesen Problemen zu begegnen, wird ein Modell dargestellt, welches den notwendigen Unterbau zur Gewährleistung einer ausreichenden Reichweite gesetzlicher Initiativen im digitalen Raum beschreibt. Darauf aufbauend werden Handlungsempfehlungen gegeben, um die beschriebenen notwendigen Bedingungen zu realisieren.

Schlüsselwörter

Reichweitenhierarchie • Reichweitenpyramide • Pyramide digitaler Souveränität • Digitale Souveränität • Informationelle Selbstbestimmung

A. Schäfer (✉)
Darmstadt , Deutschland
E-Mail: A-Shepard@web.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_21

1 Wirkungstiefe europäischer Gesetzgebung

Wenn sich die Legislative eines Staates die Möglichkeit offenhalten möchte, eigene Prinzipien umsetzen zu können, ergibt sich die Notwendigkeit, Maßnahmen zu ergreifen, die eine entsprechende Selbstbestimmung ermöglichen. Konkret muss eine Basis geschaffen werden, die die Durchsetzung der Beschlüsse der Legislative erst ermöglicht.

In diesem Beitrag wird die Realisierung *digitaler Souveränität* des Staatenverbunds der Europäischen Union im Hinblick auf die Datenschutzgrundverordnung (DSGVO) und die *informationelle Selbstbestimmung* thematisiert. Das im Verlauf vorgestellte *Modell der Reichweitentenhierarchie* ist generisch aufgebaut und lässt sich somit auch auf abweichende gesetzgeberische Initiativen übertragen.

In diesem Zusammenhang soll das Recht auf informationelle Selbstbestimmung „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“, gewähren [1]. Um dieses Recht zu gewährleisten, ist digitale Souveränität notwendig. Hierunter wird „die Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im digitalen Raum“ verstanden [2, 3].

Die Wirkungstiefe bestimmter Regularien stellt sich als nicht weitgreifend genug heraus, solange deren Durchsetzung nicht wirkungsvoll umgesetzt werden kann. Daraus resultierende ausgewählte Problemfelder werden nachfolgend dargestellt. Um die Bedingungen einer ausreichenden Reichweite gesetzlicher Initiativen zu gewährleisten, werden im weiteren Abschn. 3 aufeinander aufbauende Freiheitsgrade identifiziert, die die notwendige Grundlage einer entsprechenden Wirkungstiefe darstellen. Diese werden systematisch im Modell der Reichweitenhierarchie zusammengefasst. Auf dieser Grundlage werden in Abschn. 4 Gestaltungsmöglichkeiten dieser Freiheitsgrade diskutiert.

2 Problemfelder mangelnder Datensouveränität

Das zukünftige Verhalten vorherzusagen, sich die momentanen Überzeugungen einer Person zu vergegenwärtigen und deren scheinbare Vergangenheit zu manipulieren, ist ein Teil des Potenzials, welches die Auswertung des digitalen Lebens einer Person ermöglicht. Die Auswertung wie auch die Nutzung von Datensätzen kann in für Personen und Organisationen ungewollten Zuständen resultieren. Im Folgenden wird aufgezeigt, inwieweit die Vorhersehbarkeit von Verhalten und das Ausspähen interner Firmeninformationen Problemfelder von Datenverarbeitung

darstellen können, um anhand dieser ausgewählten Beispiele den notwendigen Handlungsbedarf aufzuzeigen.

2.1 Pattern of life – Analyse

Das Konzept der *Pattern of life – Analyse* (dt. „Lebensmuster-Analyse“) ist ungeachtet der breitflächigen Nutzung zur nachrichtendienstlichen Informationsgenerierung nicht formal definiert [4]. Biltgen und Ryan skizzieren Lebensmuster jedoch als einen spezifischen Satz von Verhaltensweisen und Bewegungen, die mit einer bestimmten Entität über einen bestimmten Zeitraum hinweg verbunden sind [5]. Die technologischen Fortschritte der letzten zwei Jahrzehnte – eine Revolution in der Informationstechnologie und das Aufkommen von Big Data – verbessern die Fähigkeit, große Datenmengen zu sammeln und zu verarbeiten [6]. Mittels der Verarbeitung von Lebensmustern lassen sich Verhaltensweisen und Anomalien analysieren und prognostizieren.

Eine verstärkte Datenbasis führt demnach zu aussagekräftigeren Vorhersagen. Nachfolgend wird anhand ausgewählter Beispiele aufgezeigt, wie entsprechende Datensätze erstellt werden können.

Mit der Nutzung von Services über das Internet hinterlässt der jeweilige Nutzer Spuren, welche ausgewertet werden können und somit Rückschluss auf seine Lebensweisen, Einstellungen und Vorlieben zulassen. Dabei kann nicht nur generierter *Content* analysiert werden. Ebenfalls fallen Metadaten an, die Potenzial für Auswertungen bieten. Bewegungsprofile können unter anderem durch die Kommunikation eines Mobilfunkgeräts mit Mobilfunkmasten erstellt werden [7]. Beispielsweise stellt die amerikanische Telefongesellschaft AT&T amerikanischen Behörden Metadaten getätigter Anrufe, die bis ins Jahr 1987 zurückreichen, zur Verfügung [8].

Mobilgeräte wachsen stetig in ihrer Bedeutung für die Kommunikation [9–12]. Applikationen auf Smartphones verbinden sich mit deren jeweiligem Netzwerk. Textnachrichten, E-Mail-Notifikationen, Standortbestimmungen und Analytic Tools können genutzt werden, um eine Bewegungskarte zu erzeugen, während diese *broadcasten* [13].

Die Videoaufnahmen von Bodycam-Aufnahmen der Bundespolizei werden auf Servern des US-Konzerns Amazon gespeichert [14].

Die entsprechenden Daten können genutzt werden, um die Einstellungen der Betroffenen zu analysieren, deren zukünftiges Verhalten vorherzusagen und Anomalien in deren regulärem Leben festzustellen. Fraglich ist, ob ein Staat solche Datensätze und die damit verbundenen Auswertungsmöglichkeiten an dritte

Unternehmen aushändigen sollte, welche anderen Regularien Folge zu leisten haben als jenen, die dieser Staat bestimmt.

Aufnahmen, die in sozialen Medien wie etwa Facebook hochgeladen werden, lassen sich zur Gesichtserkennung nutzen [15]. So erstellte die amerikanische Firma *Clearview* eine Art Suchmaschine für Gesichter, in die ein Gesicht eingespeist werden kann und anschließend Aufnahmen zurückgegeben werden, auf denen das Gesicht von Interesse abgebildet ist. Die Datenbank, auf die dabei zurückgegriffen wird, wurde nach Aussage des Unternehmens aus frei zugänglichen Quellen erstellt.

2.2 Industriebeeinflussung

Ein über die Verhaltensanalyse hinausgehendes Problemfeld stellt die wirtschaftliche Einflussnahme dar, die im folgenden Unterkapitel behandelt wird. Gesetzesvorgaben anderer Staaten können deren Behörden dazu befähigen, Internetfirmen und IT-Dienstleister mit Sitz in diesem Staat Zugriff auf gespeicherte Daten zu gewähren, selbst wenn sich die Datensätze auf Servern eines anderen Staates befinden. Bei den abgegriffenen Daten kann es sich auch um Firmengeheimnisse handeln. Ein entsprechendes Vorgehen wird beispielsweise seitens der Vereinigten Staaten von Amerika durch den *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act) legitimiert [16]. Diese Daten könnten von der Regierung dieses Staates an andere Unternehmen weitergegeben werden.

Der CLOUD Act wurde 2018 durch den US-Kongress bewilligt und sieht vor, dass sich Cloud Anbieter, die ihren Sitz in den Vereinigten Staaten von Amerika haben, nicht auf nationale und supranationale Datenschutzgesetze berufen können und somit auch entgegen lokal geltender Gesetzgebung Daten herauszugeben haben [17, 18]. Dies gilt für Daten von US-Bürgern, US-Unternehmen und Unternehmen anderer Nationen mit einem Sitz in den USA. Angefragte Unternehmen können sich nur darauf berufen, dass die herauszugebenden Daten weder einen US-Bürger noch einen in den USA ansässigen Nicht-US-Bürger betreffen und zusätzlich die Herausgabe das Datenschutzrecht eines Landes verletzen würde, falls dieses Land mit den USA eine Exekutivvereinbarung abgeschlossen hat [19]. Insgesamt ist es dabei irrelevant, an welchem Ort sich die Server physisch befinden. Bei der Datenherausgabe erfolgt keine Benachrichtigung des Betroffenen.

Der Jurist und mehrjährige Datenschutzbeauftragte des Landes Schleswig–Holstein Thilo Weichert warnt in seiner Einschätzung vor einer aus dem CLOUD

und *Patriot Act* resultierenden Datenweiterleitung an US-Wirtschaftsunternehmen durch US-Geheimdienste [20].

Das 2015 verabschiedete Gesetz der Volksrepublik China zur nationalen Sicherheit verpflichtet alle Bürger der Volksrepublik, staatliche Behörden, Streitkräfte, politische Parteien, Volksgruppen, Unternehmen, öffentliche Einrichtungen und andere gesellschaftliche Organisationen zur Aufrechterhaltung der nationalen Sicherheit. [21, 22]. Hierunter wird auch verstanden, dass Daten auf Verlangen der Regierung herausgegeben werden.

3 Bedingungen informationeller Selbstbestimmung

Im Nachfolgenden werden Freiheitsgrade erläutert, die notwendig sind, um die digitale Souveränität eines Staates zu verstärken und somit Lösungen für die genannten Herausforderungen zu entwickeln. Die Realisierung einer ausreichenden Reichweite gesetzlicher Initiativen bedingt, dass diese auf die notwendigen Stufen technischer Ausgestaltung, die nachfolgend als Freiheitsgrade bezeichnet werden, angewendet werden können. Zur strukturierten Adressierung wurde ein hierarchisches Modell (Abb. 1) entwickelt, das diese Stufen beinhaltet. Nur wenn

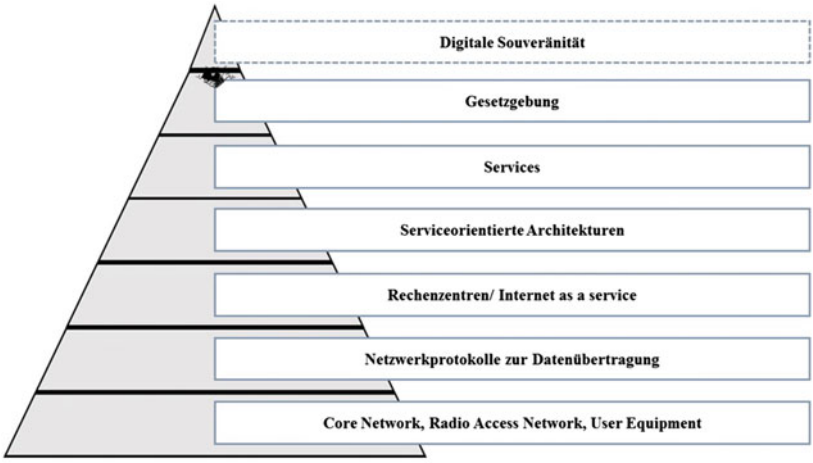


Abb. 1. *Reichweitenhierarchie-Modell.* Um die Wirkung der höherliegenden Stufen im Sinne einer informationellen Selbstbestimmung erreichen zu können, müssen zunächst die darunterliegenden Stufen in den Wirkungsbereich der Gesetzgebung fallen.

sich die Gesetzgebung auf alle die dem Modell der Reichweitenhierarchie zugrundeliegenden Freiheitsgrade erstreckt, kann digitale Souveränität gewährleistet werden.

Gesetzgebung Das Bundesverfassungsgericht stellte 1983 mit seinem Urteil zur Volkszählung folgendes fest [23]:

> „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß [sic.] etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß [sic.] ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.
>
> Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.
>
> Hieraus folgt: Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfaßt. [sic.]“

Um diesen vom Gesetzgeber vorgesehenen Schutz umsetzen zu können, ist es notwendig die Reichweite erlassener Gesetzte zu gewährleisten. Wie im vorherigen Kapitel erläutert, werden aufgrund der Gesetzgebung anderer Staaten Daten über Personen herausgegeben, ohne dass diese selbst über eine entsprechende Preisgabe bestimmen können. Ein solches Vorgehen ist mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar. Hieraus resultiert für einen Staat, welcher andere Werte hinsichtlich der Behandlung von Datenschutz verfolgt, die Notwendigkeit, Datensouveränität zu erhalten, um entsprechende Rechte wirkungsvoll durchsetzen zu können.

Die Umsetzung des grundlegenden Rechts auf informationelle Selbstbestimmung bedingt somit die Gerichtsbarkeit über die zugrundeliegenden Infrastrukturen. Zur Realisierung digitaler Souveränität ist es notwendig, die Reichweite gesetzgeberischer Bestimmungen auf die einzelnen Freiheitsgrade der Reichweitenhierarchie auszuweiten.

Services Im Bereich der Services ist es in diesem Sinne notwendig, dafür Sorge zu tragen, dass Services, die genutzt werden, sich auch dem territorial geltenden

Recht unterwerfen. Dies stellt in Zeiten international operierender Unternehmen keine Trivialität dar. Unter Umständen werden die vom Gesetzgeber beabsichtigten Regelungen durch die Anwendung einer anderen Gerichtsbarkeit ausgehebelt. So zeigte zum Beispiel die 2015 getroffene Entscheidung des *EuGHs* hinsichtlich des *Safe-Harbor-Abkommens* (Urteil Schrems gegen Data Protection Commissioner) einmal mehr, dass in den USA kein gleichwertiges Datenschutzniveau existiert und der Schutz personenbezogener Daten nicht ausreichend gewährleistet ist, wenn diese in die USA transferiert werden [24, 25]. Der Gerichtshof stellte fest, dass das Safe-Harbor-Abkommen ein angemessenes Schutzniveau ohne Faktengrundlage postulierte [26]. Hintergrund dabei war die Realisierung eines problemlosen Datentransfers in die USA und an US-amerikanische Unternehmen. Der „Verantwortliche" muss hierbei beim Transfer und der Speicherung sicherstellen, dass die Daten nach europäischen Datenschutzstandards verarbeitet und gelagert werden. Da die USA jedoch einen anderen Umgang mit Daten durch ihre Ermittlungsbehörden und Geheimdienste per Gesetz beschlossen haben, musste eine entsprechende Regelung getroffen werden. Nachdem das Safe-Harbour-Abkommen gekippt wurde, entstand das *EU-US Privacy Shield,* bei dem US-Konzerne sich selbst durch Zusicherung zertifizieren konnten. Auch diesen Beschluss hat der EuGH für europarechtswidrig und somit nichtig erklärt.

Artikel 48 der DSGVO regelt die Herausgabe von Daten an Behörden eines Landes außerhalb der EU wie folgt [19, 27]:

> „Jegliches Urteil eines Gerichts eines Drittlands und jegliche Entscheidung einer Verwaltungsbehörde eines Drittlands, mit denen von einem Verantwortlichen oder einem Auftragsverarbeiter die Übermittlung oder Offenlegung personenbezogener Daten verlangt wird, dürfen […] nur dann anerkannt oder vollstreckbar werden, wenn sie auf eine in Kraft befindliche internationale Übereinkunft wie etwa ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Union oder einem Mitgliedstaat gestützt sind."

Es kann nicht sichergestellt werden, dass Unternehmen, die gleichzeitig anderen Gesetzen unterliegen, die bei deren Einhaltung einen Bruch mit der DSGVO in Konsequenz aufweisen, die Einhaltung der DSGVO priorisieren. Insbesondere gestaltet sich eine Ahndung schwierig, wenn das Vergehen nicht angezeigt werden kann. Wie bereits ausgeführt, ist beispielsweise eine Benachrichtigung der Betroffenen bei einer Datenherausgabe aufgrund des CLOUD-Acts nicht vorgesehen. Die Nutzung von Services, die entgegengesetzten Gesetzgebungen unterliegen, birgt somit das erwähnte Risiko aufgrund anderer Bestimmungen, sich nicht an hiesige Regularien zu halten. Die Juristin in Irland Yvonne Cunnane (Facebook) deutete an, dass

sich der Konzern wegen der Einschränkungen der DSGVO ggf. aus dem Europa-Geschäft zurückziehen könnte, da er unter diesen Umständen die Services *Facebook* und *Instagram* in der EU nicht weiterführen könne [28, 29].

Serviceorientierte Architektur Um entsprechende Services initial aufzubauen, können wiederverwendbare Programmbausteine genutzt werden [30]. Diese ermöglichen es, Services in viel kürzerer Zeit zu entwickeln. Falls jedoch beim Einsatz entsprechender *serviceorientierter Architekturen* (SoA) auf Anwendungen zurückgegriffen wird, deren Gerichtsbarkeit nicht dem europäischen Recht unterliegt, kann der Einsatz wiederum in datenschutz- und datensicherheitskritischen Konsequenzen resultieren.

Rechenzentren/Internet as a Service Selbst wenn ein Service per se den hiesigen Gesetzen unterliegt, kann informationelle Selbstbestimmung nicht in jedem Fall durch den Gesetzgeber realisiert werden. Dies ist der Fall, wenn ein Rechenzentrum entweder einem nicht der Gerichtsbarkeit unterliegendem Territorium zugeordnet ist oder aber dies zwar territorial erfüllt, jedoch von Unternehmen betrieben wird, die in der Hauptsache Recht befolgen, das nicht der hiesigen Rechtsprechung entspricht. Beispielsweise bietet die *Deutsche Telekom* unter anderem ein Rechenzentrum zur Anmietung an [31]. Hierbei tritt diese jedoch lediglich als *Cloud Solution Provider* auf. Der eigentliche Anbieter des Cloud-Dienstes ist hier die US-amerikanische Firma *Microsoft*. Der 2018 unterzeichnete und bereits erwähnte *CLOUD-Act* befugt US-amerikanische Behörden, Daten von Servern US-amerikanischer Unternehmen, die im US-amerikanischen Ausland stehen, abzufragen [32–34]. Bei Rückgriff auf entsprechende Rechnerkapazitäten, wie dies auch bei *Internet as a Service* (IaaS) der Fall ist, kann somit die europäische DSGVO unter Umständen nicht eingehalten werden.

Netzwerkprotokolle zur Datenübertragung Die den heutigen Datenströmen zugrundeliegenden Netzwerkprotokolle (Internetprotokollfamilie) des *OSI-Referenzmodells* sind in der Hauptsache frei einsehbar [35–37]. Das den offenen Standards zugrunde liegende Regelwerk ist beispielsweise mittels sogenannter *RFC*-Dokumente (Request for Comments) nachzuvollziehen. Damit lassen sich diese auf Schwachstellen untersuchen.

Nichtsdestotrotz kann nicht ausgeschlossen werden, dass das gezielte Ausspielen entsprechender Protokolle genutzt werden kann, um Datenströme auszulesen oder umzulenken.

Core Network, Radio Access Network, User Equipment Die Datenströme selbst werden über das *Core- & Radio Access Network* übertragen und mittels *User Equipment* visuell aufbereitet dem Anwender zur Verfügung gestellt. Der diesen zugrundeliegende Hardwareunterbau stellt die essenzielle Basis digitaler Souveränität dar [38]. In einem Bericht des Geheimdienstausschusses des Repräsentantenhauses in den USA wird ausgesagt, dass Telekommunikationsnetze auf Vertrauen und Verlässlichkeit aufbauen und diese für böswilliges Eindringen oder störende Aktivitäten anfällig sind [21]. Aus diesem Grund sei ein ausreichendes Vertrauensniveau gegenüber dem Ausrüstungslieferanten als auch gegenüber dem Betreiber notwendig.

Der *BND*-Präsident Bruno Kahl stellte in einer Anhörung des parlamentarischen Kontrollgremiums des Bundestags fest, dass Infrastruktur kein tauglicher Gegenstand für einen Konzern sei, „dem man nicht voll vertrauen kann" [39]. Aus einem internen Vermerk des Auswärtigen Amts, der als Verschlussache eingestuft wurde, geht hervor, dass Ende 2019 von US-Seite nachrichtendienstliche Informationen weitergegeben wurden, denen zufolge Huawei nachweislich mit Chinas Sicherheitsbehörden zusammenarbeite [40]. Konkrete Details wurden jedoch nicht öffentlich.

T-Mobile US wurde 2017 in einem Zivilprozess gegen Huawei 4,8 Mio. Dollar Schadensersatz zugesprochen [41, 42]. Ein eindeutiger Nachweis, dass die Mitarbeiter im Auftrag Huaweis gehandelt haben, konnte jedoch nicht erbracht werden. Hintergrund waren Spionagevorwürfe in Bezug auf einen Testroboter.

Darüber hinaus wird Huawei in einer Anklageschrift vorgeworfen im Juli 2013 ein Bonussystem betrieben zu haben, das Mitarbeitern für die Weitergabe von gestohlenen Unternehmensinformationen Boni anbot [42–44]. Diese Informationen beruhen auf E-Mails, an die das *FBI* gelangt ist.

Obwohl der australische Staat 2018 die Verlegung von Unterseekabeln für die Salomonen durch Huawei unterbunden hat, betonte die australische Außenministerin Julie Bishop klar, dass es nicht angebracht wäre, in diesem Kontext auf Sicherheitsfragen einzugehen, sondern Australien den Salomonen lediglich ein billigeres Angebot gemacht habe [45].

In Deutschland wird die weitere Integration von Infrastruktur durch Huawei in manchen Bereichen weiterhin forciert. Beispielsweise verstärkt die Stadt Duisburg ihre Zusammenarbeit mit Huawei im Bereich der Entwicklung von *Smart Cities* [46]. Der Website Huaweis zufolge hat die Zusammenarbeit das Ziel, die Umwandlung Duisburgs von einer traditionellen Industriestadt in eine dienstleistungsorientierte, intelligente Stadt zu fokussieren. Dies soll durch intelligente Verwaltung, Hafenlogistik, Bildung, Infrastruktur, *5G,* Breitband, Häuser und urbanes *IoT* realisiert werden.

Die Deutsche Telekom, die sich zu 32 % in deutschem Staatsbesitz befindet und der größte Mobilfunkanbieter im Land ist, setzt bei ihren Einkäufen auf 30 % amerikanische und jeweils 25 % chinesische und europäische Hersteller [47, 48].

Die Bundesnetzagentur legte im April 2020 einen Sicherheitskatalog für kritische Telekommunikations- und Datenverarbeitungssysteme vor, welcher unter anderem mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) abgestimmt wurde [49, 50]. Dieses soll die für Netzbetreiber geltenden Sicherheitsanforderungen des *Telekommunikationsgesetzes* (TKG) zukunftssicherer gestalten. Der Abschnitt „Zusätzliche Sicherheitsanforderungen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial" zielt auf eine Zertifizierung und Sicherstellung der Produktintegrität kritischer Komponenten ab [51]. Sorge zu tragen hat dafür der Betreiber des Telekommunikationsnetzes. Die Vertrauenswürdigkeit der Lieferanten und Hersteller soll durch eine Eigenerklärung sichergestellt werden, die bei Zuwiderhandlung mit Vertragsstrafen geahndet wird. Diese Versicherung beinhaltet die Verpflichtung, dass „vertrauliche Informationen […] nicht […] in das Ausland gelangen oder ausländischen Stellen im Inland zur Kenntnis gelangen". Insbesondere hat die Bezugsquelle dabei zu versichern, „dass diese rechtlich und tatsächlich in der Lage ist, eine Weitergabe von vertraulichen Informationen von oder über seine Kunden an Dritte abzulehnen". Huawei bezeichnete den Ansatz als „sachorientierten und auf technischen Standards beruhenden". Dabei verspricht das Unternehmen, man wolle „transparent mit Regulierungsbehörden, Kunden und Branchenorganisationen zusammenarbeiten."

Dem Auswärtigen Amt geht eine entsprechende technische Überprüfung einzelner Bauteile nicht weit genug [40]. Eigene Sicherheitsinteressen könnten nur durch Genehmigungsverfahren gewahrt werden, die rechtliche Rahmenbedingungen mit einbeziehen, welchen ein Ausrüster ausgesetzt ist. Vorgeschlagen wird eine Vertrauensprüfung, die durch einen „interministeriellen Ausschuss" durchgeführt wird.

Das Modell der Reichweitenhierarchie Die in diesem Kapitel erläuterten und sich bedingenden Freiheitsgrade wurden zur Veranschaulichung im Modell der Reichweitenhierarchie (Abb. 1) dargestellt. Freiheitsgrade beschreiben hierbei jene Stufen, die der Gesetzgebung zugrundeliegen und auf deren Wirkungstiefe sie Einfluss nehmen. Die vollständige Umsetzung der jeweils höheren Stufe bedingt hierbei die Erfüllung der darunterliegenden Stufe. Um die Reichweite der Gesetzgebung in ihrer Gänze zu erreichen und den damit verbundenen Wirkungsraum informationeller Selbstbestimmung zu realisieren, ist die Eingliederung aller Stufen in den Wirkungsbereich gesetzlicher Initiativen notwendig.

4 Gestaltungsoptionen

Zur Realisierung digitaler Souveränität ist es erforderlich die Reichweite gesetzgeberischer Bestimmungen auf die einzelnen Stufen der Bedingungspyramide auszuweiten. Dieser Beitrag fokussiert sich auf Gestaltungsoptionen für die technischen Ebenen, um der Gesetzgebung die notwendige Wirkungstiefe zu ermöglichen.

Services & serviceorientierte Architekturen Im Bereich der Services ist es in diesem Sinne für einen Staat anzustreben, Gründungen, aus denen potenziell zukunftsweisende Unternehmen entstehen, zu unterstützen. Ebenfalls sollten Bestrebungen gefördert werden, die darauf abzielen, Substitutionsservices anzubieten, die im hauptsächlichen Unterschied zu bestehenden Services den hiesigen Gesetzen unterliegen. Somit können Alternativen angeboten werden, die informationelle Selbstbestimmung anbieten. Gründungsvorhaben weisen jedoch Gründungshemmnisse auf [52]. Beispielsweise fallen diese bei der Finanzierung und bürokratischen Regelungen an. Angebote unkomplizierter Hilfestellungen können hier Hemmnisse adressieren.

Nichtsdestotrotz sind neben staatlichen Förderungen insbesondere die Bürgerinnen und Bürger eines Staates dazu aufgerufen, die Initiative zu ergreifen und Services anzubieten. Forschungsergebnisse belegen, dass es dabei nicht darauf ankommt, ein großes Risiko einzugehen, sondern vielmehr dieses zu minimieren und mit dem zur Verfügung stehenden Repertoire Ideen umzusetzen [53]. Nur wenn diese Initiativen ergriffen werden, kann und sollte von staatlicher Seite Unterstützung erfolgen, die eine Realisierung der Ideen vereinfacht.

Open Source Software ermöglicht, durch die Eigenschaft des frei einsehbaren Quellcodes, Sicherheitslücken in der Software zu untersuchen [54]. Dieser Ansatz sollte gefördert werden. Denkbar wäre auch eine staatlich finanzierte Entwicklung entsprechend freier Software.

Rechenzentren/Internet as a Service Um die benötigten Dienste auch skalierbar zu nutzen, können Clouddienste mit entsprechender quelloffener Software kombiniert werden. Hierfür lassen sich Clouddienste europäischer Anbieter nutzen. Datenschutzhindernissen, die dadurch entstehen, dass Clouddienste genutzt werden, denen die Gerichtsbarkeit eines anderes Staates zugrundeliegt, kann somit entgegengewirkt werden. Gleichzeitig wird die digitale Infrastruktur des Staatenverbundes aufgrund der Nutzung gefördert.

Erfolgen kann dies durch Unternehmen oder Organisationen selbst. Alternativ eröffnet sich Marktpotenzial für neue Unternehmen innerhalb des Staatenverbundes,

indem diese Komplettpakete in Form von *Software as a Service* (SaaS) anbieten, die dementsprechend in ihrer Gesamtheit den hiesigen Gesetzen unterliegen und somit die angestrebte gerichtsbare Reichweite erhöhen.

Auch sind Ausgestaltungen denkbar, bei denen auf lokales Hosting zurückgegriffen wird [32]. Softwareanbieter, die anderen gesetzlichen Bestimmungen unterliegen, können *On-Premises* Software liefern, welche es den Serverbetreibern ermöglicht, die Software zu betreiben, ohne einen für diese ungewollten Datenabfluss befürchten zu müssen. Bei Installationen auf Servern, die mit dem Internet verbunden sind, wie dies etwa unter Rückgriff auf IaaS-Provider der Fall ist, kann es ratsam sein, Datenabflüsse zu überprüfen oder auf vertrauenswürdige Zertifizierer zurückzugreifen.

Beschriebene Hindernisse, die durch die Speicherung von Daten auf Servern entstehen können, deren Betreiber mehreren Gesetzgebern unterstehen, können in einigen Fällen durch den Einsatz von Verschlüsselungen ausgeräumt werden. Diese sollten entsprechend so angelegt sein, dass der Serverbetreiber selbst die Daten nicht auslesen kann.

Die Idee bei der Nutzung von sogenannten *Ende-zu-Ende* (E2E) verschlüsselten Anwendungen liegt darin, dass selbst bei einer Weitergabe von Daten immer noch eine entsprechende Entschlüsselung vorgenommen werden müsste [55]. Je nachdem, wie das entsprechende E2E-Verschlüsselungssystem ausgestaltet ist, variiert die Stärke des gewährten Schutzes. Darüber hinaus lassen sich Metadaten in vielen Fällen weiterhin auslesen [56]. Es wird allerdings auch an Lösungen gearbeitet, die auch eine Verschlüsselung für Metadaten umsetzen [57].

Core Network, Radio Access Network, User Equipment Die den Rechenzentren zugrundeliegende Infrastruktur basiert auf Komponenten von Netzwerkausrüstern. Weisen diese ihren Hauptsitz in dem Staat auf, in dem die digitale Souveränität hergestellt bzw. erhalten werden soll, unterliegen diese der dort herrschenden Gesetzgebung. Wie erläutert, können diese, falls Niederlassungen und Geschäftstätigkeiten im Ausland bestehen, im Falle bestimmter Regularien von anderen Staaten zur Herausgabe von Daten aufgefordert werden. Dies ist beispielsweise beim CLOUD-Act der Fall. Zur Gewährleistung einer gesetzgeberischen Reichweite bis auf die Basisstufe der Reichweitenhierarchie sind ansässige Netzwerkausrüster zu fördern und ggf. ist anzustreben, weitere Hersteller aufzubauen. Hierbei kann es auch vorteilhaft sein, Unternehmenseinheiten derart voneinander zu trennen, dass Gesetzgebungen anderer Staaten keinen Einfluss auf jede dieser Einheiten ausüben können [32]. Eine pragmatische Alternative lässt sich in Kooperationen mit Netzwerkausrüstern sehen, von denen anzunehmen ist, dass die staatlichen Regularien längerfristig äquivalent zu den Hiesigen sind und sein werden. Gleichzeitig ist es,

um Fairness zu garantieren, ratsam, jegliche Technologieanbieter einzuladen, sich am Wettbewerb um Aufträge zu beteiligen, solange die Sicherheitsanforderungen erfüllt werden. Parallelen lassen sich auf Endgeräte übertragen.

Den anstehenden 5G-Netzausbau hat die Europäische Union als „wichtige Voraussetzung für künftige digitale Dienste" identifiziert [58]. Um 5G-Cybersicherheit zu garantieren, wurde mit der „5G networks EU Toolbox" daher ein EU-Instrument geschaffen, mit dem Sicherheitsrisiken gemindert werden sollen, indem diese als „Orientierungshilfe bei der Auswahl und Priorisierung von Maßnahmen dienen" soll [59]. Diese beruhen „ausschließlich auf Sicherheitserwägungen".

Freiheitsgradeübergreifende Ansätze Denkbar wäre auch der Einsatz entsprechender Siegel, die aufzeigen, dass das jeweilige Unternehmen Daten ausschließlich in der EU verarbeitet [60]. Somit könnten Verbraucher Marktsituationen schneller erfassen. Bei der Realisierung ist, wie bereits beim Sicherheitskatalog für kritische Telekommunikations- und Datenverarbeitungssysteme der Bundesnetzagentur erwähnt, besonders darauf zu achten, wie die Kriterien der Siegelvergabe gestaltet werden. Orientierungspunkt kann hierzu das Siegel der *TeleTrusT*-Zeicheninitiative „IT Security made in Germany" bieten [61].

Bestrebungen hinsichtlich des Aufbaus einer dem Staatenverbund unterstehenden Dateninfrastruktur werden vom *BMWi* (Bundesministerium für Wirtschaft und Energie) mit dem Projekt *GAIA-X* gefördert [62–64]. Die Zielsetzung von GAIA-X besteht in der Schaffung eines offenen digitalen Ökosystems zum Datenaustausch mittels einer vernetzten Dateninfrastruktur zur Stärkung der digitalen Souveränität. Dieses Projekt zielt darauf ab, dass der Staat nur als neutraler Mittler auftritt, wobei die konkrete Entwicklungsarbeit durch private Unternehmen umgesetzt wird. Bei der Kreierung des entsprechenden Projekts sollte jedoch darauf geachtet werden, inwieweit Unternehmen, die nicht ausschließlich den Gesetzgebungen des Staatenverbunds unterliegen, hinsichtlich sicherheitsrelevanter Abwägungen beteiligt werden. Kritische Stimmen, wie etwa die des Jurists und Ex-Unternehmers Mayer-Schönberger, sehen Lösungsansätze – statt in entsprechenden staatlich finanzierten Projekten – in einer Grundverordnung zur Datennutzung, die einer monopolistischen Datennutzung entgegenwirken soll [65]. Indem Sachdaten, die in Unternehmen erzeugt werden, mit anderen Unternehmen geteilt werden, steige der Nutzen exponentiell.

Darüber hinaus ist in Erwägung zu ziehen, die Leitmaßstäbe, die bei der Bewilligung durch den Staat hinsichtlich Unternehmensverkäufen zurate gezogen werden, zu überdenken. Die *Brainloop AG* aus München bietet für den Austausch sensibler Dokumente sichere Datenräume an und konnte vor dem Verkauf im Jahr 2018 70 %

der Dax-Konzerne zu seinen Kunden zählen [66, 67]. Der Verkauf an die Softwarefirma *Diligent* mit Sitz in New York wurde seitens der deutschen Regierung nicht eingeschränkt [68].

Die Kombination der vorgeschlagenen Maßnahmen zielt auf die Förderung einer stärkeren Wirkungstiefe gesetzgeberischer Regularien ab. Digitale Souveränität soll in diesem Sinne die Reichweite der Gesetze, die von der hiesigen Legislative beschlossen werden, erhöhen. Wie eine zielführende Gesetzgebung hinsichtlich der Formulierung auszugestalten ist, ist ein Thema für sich.

5 Fazit

Ausgehend von einer Gesetzgebung eines Staates wurde ein Modell entwickelt, das die Limitationen gesetzgeberischer Reichweite verdeutlicht. Mit dem Modell der Reichweitenhierarchie wurden Bedingungen aufgezeigt, die erfüllt werden müssen, um die Reichweite gesetzlicher Initiativen beurteilen und darauf aufbauend verstärken zu können. Anhand des Modells lassen sich Problemfelder und Lösungsansätze strukturiert adressieren.

Für die entsprechenden Bereiche wurden Vorschläge zur Stärkung der digitalen Souveränität eines Staates erarbeitet. Auf diesen aufbauend ist sowohl eine vertiefte Diskussion der Gestaltung als auch deren Realisierung in Folgearbeiten anzustreben. Hierbei sind auch entsprechende Hindernisse wie beispielsweise kritische Einschätzungen der Wirtschaftlichkeitsbetrachtung von Open-Source-Software oder Netzwerkeffekte beim Aufbau alternativer Plattformen zu adressieren.

Es wäre im thematischen Kontext nicht angebracht Staaten, die ihrerseits ihre digitale Souveränität ausbauen, für deren gesetzgeberische Wirkungstiefe zu diskreditieren. Die Regierungen der Vereinigten Staaten von Amerika und die Volksrepublik China, als die in diesem Paper angeführten beispielhaften Staaten, welche zu derzeitigem Stand in manchen Konstellationen die Reichweite europäischer Gesetzgebung limitieren können, sollten nicht als Ursache mangelnder europäischer digitaler Datensouveränität (oder auch eines anderen Staates) angesehen werden.

Vielmehr ist es den europäischen Bürgern anzuraten (oder auch den Bürgern eines anderen Staates), gestalterische Initiativen zu ergreifen, die der hiesigen Legislative den Weg bereiten, die notwendige Reichweite zu erhalten, um den Wesenskern der Gesetzgebung umsetzen zu können.

Literatur

1. Geminn, C., Roßnagel, A.: „Privatheit“ und „Privatsphäre“ aus der Perspektive des Rechts – Ein Überblick. JuristenZeitung **14**(2015), 703–708 (2015). https://doi.org/10.1628/002268815X14346427046980
2. Bundesministerium für Wirtschaft und Energie.: Leitplanken Digitaler Souveränität. Nationaler IT Gipfel, Berlin, (2015). https://www.de.digital/DIGITAL/Redaktion/DE/Downloads/it-gipfel-2015-leitplanken-digitaler-souveraenitaet.pdf?__blob=publicationFile&v=1. Zugegriffen: 20. Okt. 2020
3. Bundesministerium für Wirtschaft und Energie.: Kompetenzen für eine digitale Souveränität. (2017). https://www.de.digital/DIGITAL/Redaktion/DE/Downloads/it-gipfel-2015-leitplanken-digitaler-souveraenitaet.pdf?__blob=publicationFile&v=1. Zugegriffen: 20. Okt. 2020
4. Craddock, R. Watson, D., Saunders, W.: Generic Pattern of Life and Behaviour Analysis. In: IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, IEEE (2016)
5. Biltgen, P., Ryan, S.: Activity-Based Intelligence: Principles and Applications. Artech House, Boston (2016)
6. Biltgen, P., Bacastow, T., Kaye, T., Young, J.: Activity-Based Intelligence: Understanding Patterns-of-life. In: USGIF´s State & Future of GEOINT Report (2017)
7. Schmidt, A., Männel, T.: Potenzialanalyse zur Mobilfunkdatennutzung in der Verkehrsplanung, Fraunhofer IAO Homepage. https://www.iao.fraunhofer.de/lang-de/images/iao-news/telefonica-studie.pdf. Zugegriffen: 20. Okt. 2020
8. Kenneth, L.: AT&T Is Spying on Americans for Profit, DAILY BEAST Homepage (2017). https://www.thedailybeast.com/atandt-is-spying-on-americans-for-profit. Zugegriffen: 22. Okt. 2020
9. Neuer Comscore Report “Die mobile Bedürfnispyramide“ enthüllt globale Mobile-Trends, Comscore Pressemitteilung (2017). https://www.comscore.com/ger/Insights/Pressemitteilung/2017/3/Neuer-comScore-Report-Die-mobile-Beduerfnispyramide-enthuellt-globale-Mobile-Trends?cs_edgescape_cc=DE. Zugegriffen: 22. Okt. 2020
10. Smartphone Usage Has Doubled in the Past Three Years, Comscore Homepage (2017). https://www.comscore.com/Insights/Blog/Smartphone-Usage-Has-Doubled-in-the-Past-Three-Years. Zugegriffen: 22. Okt. 2020
11. Bitkom-Research. https://www.bitkom-research.de/system/files/document/20190620_Bitkom_Research_Studien_2019.pdf. Zugegriffen: 22. Okt. 2020
12. Konsumenten punktgenau erreichen – Basisinformationen für fundierte Mediaentscheidungen, VuMa Touchpoints (2020). https://www.vuma.de/fileadmin/user_upload/PDF/berichtsbaende/VuMA_Berichtsband_2020.pdf. Zugegriffen: 22. Okt. 2020
13. Apps und Datenschutz: Verbraucherzentrale Homepage (2020). https://www.verbraucherzentrale.de/wissen/digitale-welt/mobilfunk-und-festnetz/apps-und-datenschutz-6431. Zugegriffen: 20. Okt. 2020
14. Biselli, A.: Kleine Anfrage – Bundespolizei speichert Bodycam-Aufnahmen weiter bei Amazon, Netzpolitik Homepage (2019). https://netzpolitik.org/2019/bundespolizei-speichert-bodycam-aufnahmen-weiter-bei-amazon/. Zugegriffen: 22. Okt. 2020

15. Lückoff, J.: Fotos aus Facebook und Co. Gesichterdatenbank – Traum oder Albtraum? (2020). https://www.tagesschau.de/inland/gesichtserkennung-147.html. Zugegriffen: 22. Okt. 2020
16. Privacy Shield schützt nicht vor US-Spionage via Cloud Act (2020). https://www.it-daily.net/it-sicherheit/datenschutz-grc/24008-privacy-shield-schuetzt-nicht-vor-us-spionage-via-cloud-act. Zugegriffen: 22. Okt. 2020
17. Ghoroghy, S.: CLOUD Act, DSGVO, E-Evidence-VO – aktuelle Entwicklung und Auswirkungen, Haufe Homepage (2019). https://www.haufe.de/recht/weitere-rechtsgebiete/strafrecht-oeffentl-recht/behoerdenzugriff-auf-nutzerdaten-cloud-act-dsgvo-e-evidence-vo_204_500808.html. Zugegriffen: 22. Okt. 2020
18. Microsoft veröffentlicht sechs Grundsätze zum CLOUD Act (2019). https://www.board-portal-software.de/artikel/microsoft-veroeffentlicht-sechs-grundsaetze-zum-cloud-act-95/. Zugegriffen: 22. Okt. 2020
19. Haar, T.: US CLOUD Act regelt internationalen Datenzugriff (2018). https://www.heise.de/select/ix/2018/7/1530927567503187. Zugegriffen: 22. Okt. 2020
20. PlusMinus über die Übernahme von Brainloop durch den US-Riesen Diligent: Industriespionage durch den CLOUD Act? (2019). https://www.board-portal-software.de/artikel/plusminus-ueber-die-uebernahme-von-brainloop-durch-den-us-riesen-diligent-industriespionage-durch-de/. Zugegriffen: 22. Okt. 2020
21. Sokolov, D.: Eine Frage des Vertrauens – Welche Rolle Huawei im Handelskrieg der USA gegen China spielt (2019). https://www.heise.de/select/ct/2019/5/1551439898501617. Zugegriffen: 22. Okt. 2020
22. National Security Law of the People´s Republic of China (2015). https://en.pkulaw.cn/display.aspx?cgid=250527&lib=law#. Zugegriffen: 22. Okt. 2020
23. BVerfGE 65, 1 – Volkszählung.https://www.servat.unibe.ch/dfr/bv065001.html. Zugegriffen: 22. Okt. 2020
24. Schrems, M.: Der Gerichtshof erklärt die Entscheidung der Kommission, in der festgestellt wird, dass die Vereinigten Staaten von Amerika ein angemessenes Schutzniveau übermittelter personenbezogener Daten gewährleistet, für ungültig. Gerichtshof der Europäischen Union, Pressemitteilung Nr. 117/15. (2015)
25. Document 62014CJ0362. https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A62014CJ0362. Zugegriffen: 22. Okt. 2020
26. Bleich, H.: FAQ: Das Ende des Privacy Shields. https://www.heise.de/ratgeber/FAQ-Das-Ende-des-Privacy-Shields-4906737.html. Zugegriffen: 22. Okt. 2020
27. Art. 48 DSGVO Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung. https://dsgvo-gesetz.de/art-48-dsgvo/. Zugegriffen: 22. Okt. 2020
28. The High Court Judicial Review – Facebook Ireland Limited and Data Protection Commission (2020). https://www.dropbox.com/s/yngcdv99irbm5sr/Facebook%20DPC%20filing%20Sept%202020-rotated.pdf?dl=0. Zugegriffen: 22. Okt. 2020
29. Martin-Jung, H.: Streit um Datenschutz – Facebook bringt Abschied aus EU ins Spiel (2020). https://www.sueddeutsche.de/digital/datenschutz-safe-harbor-abkommen-privacy-shield-max-schrems-datenschutzaktivist-1.5041160. Zugegriffen: 22. Okt. 2020
30. Hertig, D. CAS Information Security & Risk Management 2017: Sicherheit von SOA Services, Fachhochschule Nordwestschweiz Hochschule für Wirtschaft Homepage. https://www.fhnw.ch/plattformen/iwi/2017/12/07/cas-information-security-risk-man

agement-2017-sicherheit-von-soa-service-oriented-architecture-services/. Zugegriffen: 22. Okt. 2020
31. Microsoft Lizenzprogramme: Azure über Cloud Solution Provider vs. Enterprise Agreement. https://cloud.telekom.de/de/blog/cloud-infrastruktur/microsoft-lizenzprogramme. Zugegriffen: 22. Okt. 2020
32. Yared, P.: How to manage global data under CLOUD Act governance (2020). https://iapp.org/news/a/how-to-manage-global-data-given-the-cloud-act/. Zugegriffen: 22. Okt. 2020
33. Scheffler, M.: DSGVO vs. CLOUD Act: EU-Unternehmen im Spannungsfeld (2019). https://www.datensicherheit.de/dsgvo-cloud-act-eu-unternehmen-spannungsfeld. Zugegriffen: 22. Okt. 2020
34. Neuerer, D.: CLOUD ACT Bundesjustizministerium warnt Unternehmen vor Rechtsrisiken bei US-Datenzugriff (2019). https://www.handelsblatt.com/politik/deutschland/cloud-act-bundesjustizministerium-warnt-unternehmen-vor-rechtsrisiken-bei-us-datenzugriff/24351610.html?ticket=ST-4553710-Ue29xVzV1NP5Wr16pfCJ-ap2. Zugegriffen: 22. Okt. 2020
35. Internet standards – RFCs. https://www.ietf.org/standards/rfcs/. Zugegriffen: 22. Okt. 2020
36. iana – Internet Assigned Numbers Authority – About us. https://www.iana.org/about. Zugegriffen: 22. Okt. 2020
37. Raising the world´s standards. https://standards.ieee.org/transformation/index.html. Zugegriffen: 22. Okt. 2020
38. Lewis, J.: How will 5G shape Innovation and Security: A Primer (2018). Center for Strategic & International Studies Homepage. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181206_Lewis_5GPrimer_WEB.pdf. Zugegriffen 22. Okt. 2020
39. Neuerer, D.: 5G-Debatte (2020). https://www.handelsblatt.com/politik/deutschland/5g-debatte-verfassungsschutz-sieht-5g-ausbau-als-ziel-chinesischer-spionage/25995726.html?ticket=ST-2055731-uZW7AeLyqwT9prOKoKAH-ap2. Zugegriffen: 22. Okt. 2020
40. Koch, M.: "Smoking gun": Streit um Beweise gegen Huawei (2020). https://www.handelsblatt.com/politik/deutschland/5g-debatte-smoking-gun-streit-um-beweise-gegen-huawei/25484764.html. Zugegriffen: 22. Okt. 2020
41. Ein Telekom-Roboter steht im Zentrum der Vorwürfe gegen Huawei (2019). https://www.wiwo.de/unternehmen/it/t-mobile-us-ein-telekom-roboter-steht-im-zentrum-der-vorwuerfe-gegen-huawei/23924980.html. Zugegriffen: 22. Okt. 2020
42. Heide, D., Hua, S., Karabasz, I.: Für Huawei wird es im Spionage-Streit eng (2019). https://www.handelsblatt.com/unternehmen/it-medien/technologiekonzern-fuer-huawei-wird-es-im-spionage-streit-eng-/23923326.html?ticket=ST-2198441-cStneudEhhRVFoMscwtu-ap2. Zugegriffen: 22. Okt. 2020
43. Justice News, (2019) Department of Justice Homepage. https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade. Zugegriffen: 22. Okt. 2020
44. Lahiri, T.: The full list of crimes the US accuses Huawei of committing (2019). https://qz.com/1535995/the-full-list-of-crimes-huawei-is-accused-of-committing-by-the-us/. Zugegriffen: 22. Okt. 2020

45. Australia keeps China out of internet cabling for Pacific neighbor (2018). https://fr.reuters.com/article/us-australia-solomonislands-internet-idUSKBN1J90JY. Zugegriffen: 22. Okt. 2020
46. Huawei Deepens Cooperation with Duisburg to Transform Germany´s Industrial Heartland into a Smart City (2018).. https://www.huawei.com/en/news/2018/9/huawei-duisburg-germany-smartcity. Zugegriffen: 22. Okt. 2020
47. The geopolitics of 5G (2020). https://www.economist.com/briefing/2020/07/16/americas-war-on-huawei-nears-its-endgame. Zugegriffen: 22. Okt. 2020
48. Vielfalt statt Abhängigkeit (2020). https://www.telekom.com/de/blog/konzern/artikel/telekom-setzt-auf-multi-vendor-strategie-603466. Zugegriffen: 22. Okt. 2020
49. Sicherheitskatalog: Bund stellt bei 5G die Vertrauensfrage (2020). https://www.heise.de/news/Sicherheitskatalog-Bund-stellt-bei-5G-die-Vertrauensfrage-4867966.html?seite=2. Zugegriffen: 22. Okt. 2020
50. Aktualisierung Sicherheitsanforderungen. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/aktualisierung_sicherheitsanforderungen/aktualisierung_sicherheitsanforderungen-node.html. Zugegriffen: 22. Okt. 2020
51. Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystem sowie für die Verarbeitung von personenbezogenen Daten nach § 109 Telekommunikationsgesetz (TKG) Version 2.0, Bundesnetzagentur (2020)
52. Metzger, G., Heger, D., Höwer, D., Licht, G.: High-Tech-Gründungen in Deutschland – Hemnisse junger Unternehmen. Zentrum für Europäische Wirtschaftsforschung GmbH (2010)
53. Sarasvathy, D.: Causation and effectuation: Toward a theoretical shift from economic inevitability to entrepreneurial contingency. Acad. Manag. Rev. **26**(2), 243–263 (2001)
54. Fragen & Antworten zu Open Source Software, Bundesamt für Sicherheit und Informationstechnik Homepage. https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/EinrichtungSoftware/OpenSource/OpenSource.html. Zugegriffen: 22. Okt. 2020
55. Nabeel, M.: The Many Faces of End-to-End Encryption and Their Security Analysis (2017), IEEE International Conference on Edge Computing (EDGE), Honolulu, HI, 2017, S. 252–259, doi: https://doi.org/10.1109/IEEE.EDGE.2017.47
56. Wolf, F., Gebara, D.: Verschlüsselung erschwert die Strafverfolgung (2016). https://archiv.technikjournal.de/cms/front_content.php?idcat=59&idart=1470&lang=1. Zugegriffen: 22. Okt. 2020
57. Steinhausen, I.: Der nicht verschlüsselbare Rest, IT-Zoom Homepage. https://www.it-zoom.de/sn/eset/e/der-nicht-verschluesselbare-rest-10131/. Zugegriffen: 22. Okt. 2020
58. Sichere 5G-Netze: Fragen und Antworten zum EU-Instrumentarium (2020). Europäische Kommission Homepage. https://ec.europa.eu/commission/presscorner/detail/de/qanda_20_127. Zugegriffen: 22. Okt. 2020
59. Cybersecurity of 5G networks EU Toolbox of risk mitigating measures, CG Publication (2020)
60. Datenschutz ist europäisch – EU-Anbieter müssen gestärkt werden (2020). https://www.pressetext.com/news/datenschutz-ist-europaeisch-eu-anbieter-muessen-gestaerkt-werden.html. Zugegriffen: 22. Okt. 2020
61. TeleTrusT-Initiative: Zeichen “IT Security made in Germany”. https://www.teletrust.de/itsmig/kriterien-und-antrag/. Zugegriffen: 22. Okt. 2020

62. Schuster, H.: Was ist Gaia-X? (2019). https://www.it-business.de/was-ist-gaia-x-a-932306/. Zugegriffen: 22. Okt. 2020
63. Klein, M.: Eine Cloud für Europa soll´s jetzt richten (2019). https://www.it-business.de/eine-cloud-fuer-europa-solls-jetzt-richten-a-887177/. Zugegriffen: 22. Okt. 2020
64. Strocke, D., Witmer-Goßner, E.: Europäische Dateninfrastruktur kommt politisch und praktisch voran (2020). https://www.it-business.de/bmwi-sieht-gaia-x-durch-eugh-gestaerkt-a-962645/. Zugegriffen: 22. Okt. 2020
65. Mayer-Schönberger, V., Ramge, T.: Gute Gründe für die digitale Allmende, FAZ vom 10.10.2020
66. Voss, O.: Amerikaner wollen deutschen Online-Datentresor kaufen (2018). https://www.tagesspiegel.de/wirtschaft/brainloop-amerikaner-wollen-deutschen-online-datentresor-kaufen/22783182.html. Zugegriffen: 22. Okt. 2020
67. Seeger, J.: Sicherheitsspezialist Brainloop von US-Firma übernommen (2018). https://www.heise.de/ix/meldung/Sicherheitsspezialist-Brainloop-von-US-Firma-uebernommen-4132342.html. Zugegriffen: 22. Okt. 2020
68. Höpner, A., Heide, D., Schlautmann, C.: Der Geheimnisträger der deutschen Wirtschaft wird verkauft (2018). https://www.handelsblatt.com/unternehmen/it-medien/it-spezialist-brainloop-der-geheimnistraeger-der-deutschen-wirtschaft-wird-verkauft/22874290.html?ticket=ST-214970-cLY3MPdAWG6CMAIP3ZWm-ap1. Zugegriffen: 22. Okt. 2020

Let the Computer Say NO! The Neglected Potential of Policy Definition Languages for Data Sovereignty

Jan Bartsch, Tobias Dehling, Florian Lauf, Sven Meister and Ali Sunyaev

Abstract

During interaction with today's internet services and platform ecosystems, consumer data is often harvested and shared without their consent; that is, consumers seized to be the sovereigns of their own data with the proliferation of the internet. Due to the rapid and abundant nature of interactions in today's platform ecosystems, manual consent management is impractical. To support development of semi-automated solutions for reestablishing data sovereignty, we investigate the use of policy definition languages as machine-readable and enforceable mechanisms for fostering data sovereignty. We conducted a realist

J. Bartsch (✉) · T. Dehling · A. Sunyaev
Institute of Applied Informatics and Formal Description Methods (AIFB), Karlsruhe Institute of Technology (KIT), Karlsruhe, Germany
E-Mail: jan.bartsch@kit.edu

T. Dehling
E-Mail: dehling@kit.edu

A. Sunyaev
E-Mail: sunyaev@kit.edu

F. Lauf
Fraunhofer Institute for Software and System Engineering ISST, Dortmund, Germany
E-Mail: florian.lauf@isst.fraunhofer.de

S. Meister
Witten/Herdecke University Faculty of Health/School of Medicine, Witten, Germany
E-Mail: sven.meister@uni-wh.de

T. Dehling · A. Sunyaev
KASTEL Security Research Labs, Karlsruhe, Germany

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_22

literature review of the capabilities of policy definition languages developed for pertinent application scenarios (e.g., for access control in cloud computing). We consolidate extant literature into a framework of the chances and challenges of leveraging policy definition languages as central building blocks for data sovereignty in platform ecosystems.

Keywords

Policy languages • Data sovereignty • Digital platforms • Policy driven management • Platform ecosystems

1 Introduction

By using a single internet application, consumers usually indirectly connect themselves with a full ecosystem of third-party platforms [1–3]. For consumers, platform applications are usually provided cheap or for free; instead of requiring monetary fees, consumer data is harvested [4]. However, consumers gain little to no insight into the storage, sharing, processing, and use of their data in platform ecosystems [5, 6]. As it is today, consumers cease to be the sovereign of their data once they start using an internet application, since they lose influence over the flow of their information [4, 7]. Until consumers can influence the flow of their information, their privacy demands will not be met [8] and a sustainable data economy cannot be established [9].

The literature on data sovereignty is still evolving, predominantly driven by sociological and politically oriented literature streams [10–12]. On a technical level, little research investigates support for data sovereignty [13]. However, it is important to emphasize the technical side of data sovereignty since, by 2025, six billion consumers are expected to have a data interaction at least every eighteen seconds [14, 15]. By then, it will be impossible for humans to manually decide on consents for data sharing and handling.

To cope with the rapid digitalization, communication of consumer preferences and policies for the use of their data needs to be, at least, semi-automated and machine-enforceable. A far-spread solution for the fast handling of policies of multiple parties is the use of machine-readable languages that specify policies on a technical level to guide system components in their actions [16]. To avoid ambiguity, we use the term policy definition language (PDL) for the language and policy rule for the instantiation of a specific policy. Existing PDLs are quite diverse and address a broad spectrum of different concepts in various domains.

The quantity of available PDLs is not the issue; a sufficiently large portion of PDLs seems to work well in their target domains [16, 17]. As we see it, the more pressing challenge is to realize the chances and master the challenges of combining PDLs in a sensible way to establish data sovereignty. Accordingly, the intriguing question is why data sovereignty has not yet been established with PDLs as central building blocks: PDLs could offer exactly the functionalities consumers need for data sovereignty–they will say 'NO!' if the user wants them to and they can do it fast.

The goal of our research is to understand the key considerations for the use of PDLs as central building blocks for realizing data sovereignty in platform ecosystems. Since there are most likely already too many PDLs, we prioritize the state-of-the-art and extant solutions instead of adding language n + 1 to the ever-expanding list of PDLs. Hence, our research question is: What are the challenges and chances of using PDLs as a central building block for data sovereignty in platform ecosystems?

To answer our research question, we conducted a comprehensive literature review of PDLs [18, 19]. We harmonized extant quality criteria of PDLs and performed a thematic analysis to assess the key considerations for using PDLs to foster data sovereignty [20]. We organize our findings in abstract layers of relevant development and operation stages of PDL-supported systems with data sovereignty.

Our work contributes to the existing literature in two ways. First, we extend extant research on data sovereignty by investigating a key technology. Second, we contribute to the PDL literature by pointing out and synthesizing the desired capabilities of PDLs for establishing data sovereignty. Regardless of the field of application, PDLs are characterized by common concepts, thus, our findings support development and review of PDLs also beyond the data sovereignty context.

2 Information Flow Governance and Data Sovereignty

2.1 Policy-Based Management

Policy-based Management (PBM) emerged as computer networks grew in size and participants. To allow for flexible and dynamic adjustment of system behavior, policies were introduced to specify the conditions under which a set of predefined operations or actions can be invoked to provide desired functionality [21]. Policies allow to change the behavior of system components without changing or

reimplementing the mechanisms that execute the actions, due to the separation of management and mechanisms [22]. This is accomplished through specification of high-level requirements that are refined into low-level policies which are more related to the actual domain or device the policy applies to [16]. Today, PBM is used in multiple domains because it is faster and less error-prone than traditional, manual system management [16]. Dependent on its goals and development status, a PDL might include components beyond the language itself, for instance, a model for the deployment of policy rules, a policy execution engine and a policy decision point that intercept requests and validate them against policy rules, and monitoring and quality ensuring components [23, 24].

2.2 A Brief History of PDLs

For over two decades, PDLs for different application scenarios were developed, leading to a rich body of PDLs for different application scenarios. One of these scenarios is the use of PDLs to influence consumers' privacy perceptions, PDLs can represent a company's privacy practices, inform the company about consumer preferences for data handling, and adjust company practices to consumer preferences [25]. Privacy-focused PDLs did not find widespread adoption because they are either too complicated or too simplistic to cope with consumers' privacy preferences [26, 27]. Overall, the development of privacy PDLs shows a stronger focus on data controllers than consumers [26]. Due to the ability of some privacy PDLs to restrict access to resources, comparisons with security PDLs are common [28]. Security PDLs are specialized on access control rules [16] and less common on usage control rules, due to harder system requirements [29]. The capabilities of access control languages are especially important in large applications [16]. In large applications, a fast retrieval of policy rules, written in a standard format with formal foundations to specify event-based rules, role-based access control, and obligations are desired properties of a PDL [16]. Besides access control in large applications, security PDLs can support network management [16]. Related to security applications is the use of PDLs for trust negotiation between strangers over the internet, where the handling of credentials is a key concern [30–32].

Tim Berners-Lee's vision of a semantic web [33] spurred the search and development of PDLs for the specification of (access control) rules in multi-agent systems on the semantic web [34, 35]. Famous PDLs in this context are KAoS and Rei, which utilize ontologies as a knowledge base to reason about policy rules. No PDL has a clear edge in all situations [34]. PDLs for data protection in the semantic web have shortcomings in addressing the principle of minimal

information disclosure and the control of data after disclosure [35]. PDLs suited for data protection need to be able to specify obligations, time constraints, and to be formalizable [36]. Fulfilling all these criteria still poses a challenge for most PDLs. Other studied PDL application areas are their suitability in service-oriented systems [23] and their capabilities for access control, privacy policies and preferences, transparency, data trading, and service level agreements [17]. However, PDLs are not necessarily bound to an application area; Ponder [37] and A-PPL [38] are, for instance, holistic PDLs. In the technical context of data sovereignty, usage control architectures for business ecosystems, designed to encompass traditional access control, were studied [13]. Albeit PDLs are part of the investigated architectures and data sovereignty is addressed, this work differs from our research. We focus on one part of the architecture because PDLs are a very relevant technology suitable for (re-)establishing data sovereignty for individuals and not only for organizations.

2.3 Data Sovereignty

There are several, interchangeably used, concepts of digital sovereignty [39] that share notions of independence, control, and autonomy [10]. The essential distinction in data sovereignty concepts is who is seen as the sovereign. States are the most commonly mentioned data sovereigns, as they strive to control the data generated or passing through their national internet infrastructures [11]. Other definitions see data sovereignty as self-determined data use by companies and individuals [13, 40] or focus on individuals and society as a whole along with individuals' ability to have comprehensive knowledge on data flows [41]. For individual consumers, this translates into the ability to articulate, monitor, and enforce how to handle their data [7]. Our research builds on a consumer-centered definition of data sovereignty. Consumers should have the freedom to change the platform and migrate their data whenever desired.

However, full control of one's data and full understanding of the involved mechanisms is not practical in modern platform ecosystems. We instead define data sovereignty as consumers' ability to determine what information is and is not shared, influence the flow of their data/information, trace data flows across the involved platforms, and check for compliance with their preferences. PDLs appear to be a feasible technology to address these requirements since the governance of information flows is their key strength.

3 Study Design

To answer our research question, we conducted a realist literature review [19]. To reduce out of scope search results and narrow down the vast literature on PBM, we chose a snowballing approach [18]. A preliminary search was conducted to compile a starting set of surveys, taxonomies, typologies, and reviews targeting PDLs. Relevant literature was identified through iterative and purposive forward and backward search [42, 43]. We included conceptual and empirical scientific papers and technical reports. Preferred snowballing objects were all kinds of literature performing quality appraisals or providing requirements for PDLs. Non-English sources and sources with a sole focus on technical means for connecting platforms, technical mechanisms to enforce policies, or user behavior were excluded. In contrast to extant studies, we rather stay on an abstract level and put a strong emphasis on the capabilities and open issues of PDLs that one could interpret as requirements for building a new PDL for data sovereignty.

To establish an overview of the capabilities of extant PDLs, a thematic analysis was performed [20]. After familiarization with the identified literature, an initial coding of PDL features was performed in parallel with a harmonization of terminology and concepts. After refinement of the codes, themes representing multiple codes were derived, iteratively refined, and named. We based our themes and codes on the full spectrum of PDLs, leading to results that were too abstract to address data sovereignty. Thus, we conducted an extra refinement step to compress and filter our findings by performing another thematic analysis [20]. A code was included if a direct (e.g., a prohibition operation) or indirect (e.g., policy rules leaking information) (dis-)advantage for consumer's data sovereignty was present and labeled as chance or challenge accordingly. We excluded codes with little fit to data sovereignty despite their technical relevance for PDLs in general (e.g., trigger paradigms for policy rules). The second thematic analysis yielded overarching themes forming our model's layers and grouping the remaining themes to inform the key considerations for using PDLs to design and operate PDL-supported systems allowing for data sovereignty.

4 Results

The ability of consumers to use a PDL to say 'NO!' and to regain data sovereignty, requires a system concept that can represent such rules while ensuring the security of the system. Finally, policy rules can be entered and enforced at runtime. Table 1 offers an overview of the key considerations in these three layers.

Tab. 1 Layers where PDLs directly or indirectly support consumer data sovereignty

Layer	Key Considerations	Decisions to be made
Concept	Policy rules for data sovereignty	What policy rules supported by extant PDLs are useful to protect data sovereignty?
	Syntax and semantics	How to represent policy rules in the system?
	Supported operations	What operations should the PDL support to implement data sovereignty rules?
Security	Access control	How to ensure that not everyone can access shared data?
	Usage control	How to ensure appropriate use after access?
	Protecting policies	How to protect the information in policy rules?
Runtime	Usability	How easy is it to specify and assess policy rules?
	Storage and deployment of policy rules	How to associate a policy rule with the corresponding data?

4.1 The Concept Layer

The concept layer deals with conceptual decisions to decide what kind of policy rules are important, how to represent rules in the system, and what operations need to be expressed in the rules.

4.1.1 Policy Rules for Data Sovereignty

PDLs have been used for over two decades to communicate privacy expectations of consumers and match them with company practices [44]. The first privacy policy language was P3P, which was designed to tackle online privacy concerns of consumers that arise due to difficulties in obtaining information on the privacy practices of websites [45]. Consumers could match P3P rules with the related preference PDLs APPEL-P3P and XPref to avoid websites with P3P policy rules that mismatched their privacy preferences, data use consents, or disclosure conditions [27, 46]. Despite P3P's abandonment in 2018, provision of information on the privacy practices of a company [45] is still relevant for modern PDLs to address data protection [17, 36, 47]. Modern PDLs do not only consider purposes

for data collection, data use, and processing, but also rules for data anonymization [47], location of processing [38, 48], and data retention times that specify how long data should reside at a location [36, 47, 49]. Additionally, it is beneficial for data protection when PDLs (e.g., AAL/A-PPL) already support accountability and auditing [17, 38, 48]. Data protection PDLs are not limited to companies, for instance, the preference language YaPPL is used to formulate consumers' data protection requirements in IoT contexts [50]. Ideally, the company and consumer side is addressed in system design to realize a semi-automated exchange of consents [27, 44, 46, 51].

However, a few challenges remain. A rule for retention times must, for instance, go beyond the data itself and delete it out of log files without impeding system performance [49]. Since platform ecosystems are built to facilitate data exchange, secondary data use poses a risk for data sovereignty. Only a few PDLs are designed to support auditing, handle secondary data use, facilitate data trading, or support tracing of data flows [17]. The ability of consumers to trace the provenance of their data within and across platform ecosystems is one prerequisite to achieve data sovereignty, while auditing is necessary to ensure compliance with policy rules. Here, the challenge lies in invoking rights and claims after the data has been anonymized and transferred across multiple parties [47]. So far, LPL is the only proposed PDL that addresses these requirements. Extant literature shows that a few PDL proposals address these challenges and that solutions can be found. Chances arise from further adapting and circulating these solutions and combining them with the years of scientific knowledge published on PDLs and associated possibilities for rule specification in the privacy and data protection context. This can result in PDLs allowing to formulate rules for machine-readable exchange of consent.

4.1.2 Syntax and Semantics

Policy rules predominantly follow a declarative paradigm. They state constraints on operations and boundaries but do not describe how the system has to satisfy these constraints. From the different options to write down policy rules (e.g., via an own syntax or functional languages), standardized data description languages are often used [e.g., XML or JSON, 27, 46] and use of such languages is a commonly found PDL quality criteria in the literature. While XML is predominantly used, more recent PDLs tend to support JSON due to its less verbose notation and lower storage consumption [50, 52]. The semantics of a PDL can be based on mathematical formalisms [e.g., mathematical logic by an ex ante or post hoc formalization, 16] or on ontologies [e.g., the PDL KaOS, 34, 53]. Ontologies are the foundation of the semantic web and provide computers with access to a

structured collection of information, relations between concepts, and can include inference rules to perform automated reasoning [33]. Such semantics allow for a better analysis of the policy rules [16, 54] without needing the PDL [53], since mathematical formalisms [30, 32] and ontologies [34] allow investigation and alteration of rules independent of the particular implementation of a PDL. However, it is more difficult to implement PDLs with a mathematical formalism [54].

Depending on the syntax and semantics, PDLs show design properties that make them ideal candidates for communicating consent to heterogeneous parties, which constitutes a chance for implementing data sovereignty. PDLs were designed to facilitate interplay and dynamic changes to system components through commonly understandable rules that emphasize 'what to do' and not 'how to do' something [21, 22]. PDLs build upon XML or other standard notations that are used beyond the PDL context and allow for readability by machines and humans [16]. Formalisms can help to avoid ambiguities in the reasoning process and yield useful properties based on the underlying logical system [e.g., monotonicity, 30–32]. Understanding data handling is an important part for establishing data sovereignty [7, 41] and can be fostered by ontology-based PDLs [34]. Such PDLs can help consumers in their decision-making as they offer them a chance to understand their data's properties and, more importantly, relationships between their data. Moreover, ontologies are helpful to understand relationships between policy rules, which improves system analysis and error handling capabilities.

4.1.3 Supported Operations

After considering how to represent policy rules in computer systems, we take a deeper look at the of content of rules; in particular, at two operations that are especially useful for implementing data sovereignty: prohibitions and obligations. Prohibitions are negative authorization policies to explicitly state forbidden actions [37]. Despite sounding simple, prohibitions are not part of every PDL as they can create conflicts, rule violations, or wrong attestations of rights and increase the complexity of policy analysis, but this can be mitigated with standard error-detection techniques [24 at 9.1.7, 37]. Obligations represent a more complex operation. In the PDL-context an obligation is an action that must be performed when certain events occur [37, 49]. That is, the ability of a PDL to trigger actions prior to, during, or after data access [16, 55]: Pre-obligations are actions that the requester must perform before access [49, 55]. For instance, handling of payment requirements before enabling access to resources in digital rights management [DRM, 55] or enabling provisional authorizations [56]. Provisional authorizations are feedback-mechanisms that refer to the issued access request. For instance, the binary return message 'access denied' could be changed into the more informative

provisional authorization message 'provide a valid certificate to gain access' [56]. Peri(ongoing)-obligations need to be performed during use; otherwise, access will be revoked [55]. For instance, logging of access (attempts), performed actions, or error messages during the session [55]. Post-obligations are the most common obligations and specify actions that need to be performed after access [55]. Post-obligations can be used to support policy rules that cover legal requirements, for instance, data retention times, usage conditions, and notifications [36, 49, 55].

Considering both operations in PDL design is a chance for (re-)establishing data sovereignty for consumers. Prohibitions are a high-level and intuitive operation to specify actions users disapprove of [37], are included in modern preference languages [e.g., YaPPL, 50], and are the operation that enables consumers to say 'NO'. The different types of obligations constitute multiple chances for implementing data sovereignty or to foster platform economy. Provisional authorizations are beneficial for all users as they offer suggestions, explanations, and decision support in contrast to PDLs that just reply with uninformative binary error messages [25, 28, 32, 48, 56]. Obligations are important for sensitive data [e.g., in health IT, 55] or to implement data protection rules. However, not every PDL supports obligations to protect the data of consumers [36]. The first challenge is to specify legal obligations ('liabilities') as obligations in a policy rule since the gap between convoluted legal language and clear PDLs needs to be bridged [49]. The second challenge is to design and implement a system that can handle and enforce different obligation types [55, 57]. The policy enforcement point must, for instance, understand obligations and act accordingly [28] while being consistent with conclusions of the policy decision point [55]. Sophisticated obligation rules that can be used in practical applications are still an open issue in current research [57].

4.2 The Security-Layer

For unprotected data, all claims to data sovereignty are in vain as they can be simply ignored. To restrict unwanted leakage or manipulation of data, security mechanisms are required. While security is a vast field, we outline the key considerations for PDLs.

4.2.1 Access Control

PDLs for access control are part of access control systems for many years and are predominantly specified and executed on the company side [16]. They are used to express rules to authorize the actions a requester or other participating party can perform with resources [28, 37]. Before authorization, requesters must verify

their claimed identity, for instance, by providing evidence in form of a digital certificate [30, 31, 58]. What evidence is needed and how to submit it should be stated in policy rules. The logic behind the access control process and its policy rules are specified by access control schemes, which are usually based on roles or attributes [16, 52], dependent on application requirements.

For many years, PDLs have been successfully used to specify policy rules in access control systems [e.g., XACML for over 15 years, 24]. This provides a great chance for the implementation of data sovereignty as rules can be stated and communicated to restrict access to consumer data.

4.2.2 Usage Control

To state how sensitive data should be handled by the receiving party while allowing for dynamic changes of permissions, traditional access control is encompassed by usage control [59]. Variations of usage control that make extensive use of obligations in their policy rules are used to protect the full lifecycle of data in different applications [13, 29, 59, 60]. Usage control rules can, for instance, be expressed in the PDL OSL, a formalized language that is translatable into two common DRM-PDLs to use their enforcement mechanisms [61].

Usage control and data provenance tracking work well together [62], thereby, providing a chance with respect to controlling and tracking data flows. Approaches for implementing data sovereignty [13, 60] can build on extant usage control technologies [e.g., LUCON, 63] provided, for instance, by the International Data Spaces (IDS) initiative [40, 64]. Challenges of PDLs for usage control, besides the specification of suitable policy rules, are, especially, conflict resolution between rules [65], harder requirements for the rest of the system [29], and requirements for cryptographically trusted soft- or hardware systems [66]. Usage control is a promising chance for establishing data sovereignty, but recent developments tend to focus on the business-to-business context and need to be modified for the consumer-to-business context.

4.2.3 Sensitive Policies and Credentials

A policy rule, written in a PDL, might contain information, for instance, on credentials or processes, that can be considered sensitive and needs to be handled and released with care [30, 31, 35, 56]. For instance, security policies aim to protect the asset they are written for and do not necessarily protect the private credentials to be inferred out of the policy rules [24 at 9.2.7]. Protection of sensitive rules can be done during their specification or at runtime [30]. PDLs themselves can protect sensitive policies by using policies about policies [metapolicies; 23, 56, 58] or by

simply treating the policy rules like all other protected resources [35]. Additionally, PDLs for 'trust negotiation' can be used when policy rules or credentials cannot be fully disclosed at the beginning of an interaction [30, 32, 56, 67]. In this context, 'negotiation' is a stateful step-by-step exchange of credentials and partial results between two foreign parties that reason together about their distinct policy rules until they reach an agreement or terminate the process [32, 56, 58].

Trust negotiations can help to minimize disclosure, foster interplay, and provide consumers with the ability to demand further evidence from the other party before proceeding with the negotiation. The disadvantage is that the negotiation of trust in large distributed systems is a challenge for most PDLs [67]. Overall, the handling of sensitive policies can be considered a challenge for consumer privacy. Despite the existence of mechanisms to handle sensitive policies [31, 35], the policy must first be considered as sensitive and the mechanisms (e.g., for trust negotiation) must be implemented by administrators [24 at 9.2.7].

4.3 The Runtime-Layer

The focus of the runtime layer are the different stages for handling a policy rule, from its instantiation to execution.

4.3.1 Usability

Policy rules are created and managed by users with different backgrounds and skills. For instance, a logic-based language might require some literacy in mathematical logic. In general, a PDL needs to be readable, writable, comprehensible, and easily manageable for users with different experience levels to enable them to express a policy rule quickly and easily [26, 27, 37, 47, 51, 56]. The users' job in writing policies can be simplified by tools to read, write, modify, visualize, and analyze policy rules. For instance, the PDL KaOS [53] offers a graphical user interface for writing and applying policies and can load ontologies and check them for conflicts [34]. Ponder offers a toolkit for administrative tasks and the analysis of policy specifications and conflicts [34]. Especially for preference languages, graphical tools should be available [17]. An early tool to support consumers was Privacy Bird, a P3P user agent that indicated the fit between consumer preferences and a website's privacy policy with a color-changing icon with the option to let the consumer gain more background information [68].

User-friendly tools do not exist for all PDLs [26, 54], but should be a key consideration in system design since access to (refined) information is a prerequisite for an individual to (re-)establish data sovereignty [7, 41]. There are multiple

chances [e.g., information provision, specification, analysis, 54] where tools can be combined with PDLs (e.g., with XML bindings) to benefit consumers.

4.3.2 Storage and Deployment of Policy Rules

After policy rules are specified, they need to be deployed. This can be done centrally via a policy repository or retrieval point [24] allowing for optimization through specialized indexes [16]. The decentralized option is to stick policy rules to cryptographically secured data [69]. Sticky policies are useful for data protection rules [48]. What option to choose depends on the application.

While sticky policies appear useful for implementing data sovereignty in a platform ecosystem, they face certain challenges with respect to different versions of policy rules, user roles, and jurisdictions [70]. Additionally, policy rules can contain constraints what data should not be released together [35] or context-dependent information [71]. There could be errors or ambiguities in the reasoning about policy rules when related data is released independently of each other in a platform ecosystem without a central component that checks the logical applicability of policy rules. On the upside, the potential problems of sticky policies can be mitigated by an ecosystem that includes such central component and/or defines clear boundaries to avoid ambiguities for data in the ecosystems [e.g., by LUCON or IDS components, 40, 63, 64]. Then, sticky policies are a chance to realize data sovereignty by connecting consumer preferences with encrypted data.

5 Discussion

We identified the key considerations and corresponding chances and challenges for using PDLs to support data sovereignty in platform ecosystems. On the concept layer, extant PDL-research based on privacy and data protection offers a valuable foundation to specify policy rules that support data sovereignty. However, we could not identify a PDL that addresses all challenges impeding data sovereignty and PDLs for the consumer side (preference languages) are rather underrepresented. The syntax and semantics of PDLs are ideal for communicating consent in standardized human- and machine-readable formats that represent rules and build upon a semantic foundation. Out of the supported operations, prohibitions can be seen as a trade-off between security and practicability. Obligations can be considered as the most valuable operation for protecting data, but realizing and enforcing post-obligations in practice is challenging. Security in the form of access control can be realized by well-established PDLs. While usage

control is already considered valuable for establishing data sovereignty, it is complex in implementation and does not primarily focus on the needs of consumers. The protection of policy rules and credentials by classifying them as sensitive and protecting them accordingly (e.g., by negotiations or metapolices) should be part of security considerations. Good usability, especially for consumers, in form of assessable and easy to specify policy rules can be fostered by tool support or guidance material but is not included in every PDL. For the deployment and association of policy rules with data, a central repository or sticky policies can be used. To prevent the loss of context-sensitive information and relations between data, both approaches should be combined.

It can be assumed that data ecosystems will grow in popularity. Therefore, challenges, for instance, with secondary data use and provenance tracking, will manifest even more often and more regularly in the future, which results in the need for new mechanisms to protect data sovereignty. The identified key considerations are informed by a plethora of distinct PDLs. One could interpret these considerations as requirements for building a new PDL for data sovereignty. However, we see the development of a new holistic data sovereignty PDL with skepticism since we encountered a vast amount of abandoned PDLs in our literature review that were never used in practice. Due to the heterogeneous requirements for establishing data sovereignty, we consider improving the interplay of extant or new PDLs a more promising chance to implement data sovereignty with PDLs than the development of yet another PDL; for instance, by translating between languages [e.g., OSL to DRM PDLs, 61], refining high-level PDLs into more technical languages, or by creating bindings to established PDLs (e.g., XACML).

To address the problem of low adoption and high abandonment of PDLs, the perspective of practitioners needs to be considered; otherwise, there is a risk that PDLs suitable for (re-)establishing data sovereignty will never be used in practice. For practitioners, the adoption of PDLs for data sovereignty can be beneficial to demonstrate legal compliance, increase the usability of their platform ecosystem, or improve the interplay of participating parties (e.g., provisional authorizations). The adoption of PDLs in a data economy that is driven by a decentralized community appears also promising. PDLs could help with the communication between peers and data transfers (e.g., sticky policies), while the decentralized design prevents clustering of data under the control of one authority. Thus benefitting autonomy and data sovereignty.

Despite the various applications PDLs are used for, they are not a cure-all technology. The purpose of PDLs is to specify rules that describe policies or preferences. Without a working enforcement mechanism, those rules can be ignored or

bypassed. Since we did not focus on enforcement-mechanisms and also reviewed PDLs in early design stages without implemented enforcement-mechanisms, some of our identified chances might, for now, only exist in theory. Due to space limitations, we had to focus on the most important considerations and exclude other considerations that should not be neglected, for instance, interoperability, extensibility, scalability, context-sensitivity, and some operations [e.g., filters or delegations, 37]. Moreover, we focused on PDLs and did not address various other technologies that might be suitable for implementing data sovereignty in platform ecosystems. We could only scratch the surface for the well-studied research fields of usability and security and their mechanisms, theories, and principles, which are directly or indirectly connected with the reported key considerations.

In future research, we will further investigate ontologies as a representation of knowledge to help consumers understand their data, relationships between their data, and data provenance. Another promising research direction is the assessment of what characteristics of distributed ledger technologies [DLT, 72, 73] could be useful to enhance certain parts of data sovereignty, for instance, data provenance or use of DLT as an enforcement mechanism for policy rules. To address provenance tracking and secondary data use, the extension of extant systems, for instance, with a usage control system, a suitable preference language, and tools to support consumers seems helpful and promising to ensure free but safe movement of consumer data.

6 Conclusions

We started our manuscript with the question whether PDLs can enable consumers to let their computer say 'NO!' since this will become a necessity in the future. To extend the literature on data sovereignty on a technical level, we conducted a review of the old and vast field of PDLs. The identified key considerations for using PDLs as central building blocks to implement data sovereignty indicate certain challenges that need to be overcome. Still, solution strategies are already offered in extant literature and by implementing them, the chances PDLs offer for (re-)establishing data sovereignty outweigh the challenges they are facing. By building our layer model, we contribute towards seizing these chances and offer a building block for future PDL development and for the development of technologies that (re-)establish data sovereignty for consumers. To conclude, the answer to the question whether PDLs are a beneficial technology to (re-)establish consumers' data sovereignty is 'YES!'.

Acknowledgements This research was partially funded by the German Federal Ministry of Education and Research (BMBF) within the scope of the research project DaWID (Data-driven value creation platform for interactive, assisting service systems; funding reference number: 16SV8383). This work was supported by funding from the topic Engineering Secure Systems of the Helmholtz Association (HGF) and by KASTEL Security Research Labs.

References

1. Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T., Shadbolt, N.: Third party tracking in the mobile ecosystem. In: Proceedings of the 10th ACM Conference on Web Science. pp. 23–31. ACM, Amsterdam, Netherlands (2018)
2. Libert, T.: An automated approach to auditing disclosure of third-party data collection in website privacy policies. In: Proceedings of the 2018 World Wide Web Conference. pp. 207–216. International World Wide Web Conferences Steering Committee, Lyon, France (2018)
3. Razaghpanah, A., Nithyanand, R., Vallina-Rodriguez, N., Sundaresan, S., Allman, M., Kreibich, C., Gill, P.: Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. In: Network and Distributed Systems Security Symposium 2018. NDSS, Sab Duegi, California, USA (2018)
4. De Filippi, P., McCarthy, S.: Cloud computing: Centralization and data sovereignty. Eur. J. Law Technol. **3** (2012)
5. Sunyaev, A., Dehling, T., Taylor, P.L., Mandl, K.D.: Availability and quality of mobile health app privacy policies. J. Am. Med. Inform. Assoc. **22**, e28–e33 (2015)
6. Zuboff, S.: Big other: Surveillance capitalism and the prospects of an information civilization. Journal of Information Technology. **30**, 75–89 (2015)
7. Hummel, P., Braun, M., Augsberg, S., Dabrock, P.: Sovereignty and data sharing. ITU Journal: ICT Discoveries. **25**, (2018)
8. Westin, A.: Privacy and Freedom. Atheneum, New York (1967)
9. Ochs, C., Büttner, B., Lamla, J.: Trading social visibility for economic amenability: Data-based value Translation on a "Health and fitness platform." Sci. Technol. Human Values **46**, 480–506 (2021)
10. Couture, S., Toupin, S.: What does the notion of "sovereignty" mean when referring to the digital? New Media & Soc, **21**, 2305–2322 (2019)
11. Polatin-Reuben, D., Wright, J.: An Internet with BRICS Characteristics: Data sovereignty and the balkanisation of the Internet. In: 4th USENIX Workshop on Free and Open Communications on the Internet. USENIX Association, San Diego, California, USA (2014)
12. Amoore, L.: Cloud geographies: Computing, data, sovereignty. Prog. Hum. Geogr. **42**, 4–24 (2018)
13. Zrenner, J., Moeller, F.O., Jung, C., Eitel, A., Otto, B.: Usage control architecture options for data sovereignty in business ecosystems. J. Enterp. Inf. Manage. **32**, 477–495 (2019)
14. Culnan, M.J.: Policy to avoid a privacy disaster. Journal of the Association for Information Systems. **20**, 848–856 (2019)

15. Reinsel, D., Gantz, J., Rydning, J.: The digitization of the world from edge to core. White Paper #US44413318. Framingham: International Data Corporation (2018).
16. Han, W., Lei, C.: A survey on policy languages in network and security management. Comput. Netw. **56**, 477–489 (2012)
17. Becher, S., Gerl, A., Meier, B., Bölz, F.: Big picture on privacy enhancing technologies in e-Health: A holistic personal privacy workflow. Information. **11**, 356 (2020)
18. Wohlin, C.: Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: Proceedings of the 18th international conference on evaluation and assessment in software engineering. pp. 1–10. ACM, London, England (2014).
19. Paré, G., Trudel, M.-C., Jaana, M., Kitsiou, S.: Synthesizing information systems knowledge: A typology of literature reviews. Information & Management. **52**, 183–199 (2015)
20. Braun, V., Clarke, V.: Using thematic analysis in psychology. Qual. Res. Psychol. **3**, 77–101 (2006)
21. Sloman, M., Lupu, E.: Security and management policy specification. IEEE Network **16**, 10–19 (2002)
22. Sloman, M.: Policy driven management for distributed systems. J. Netw. Syst. Manage. **2**, 333–360 (1994)
23. Phan, T., Han, J., Schneider, J.G., Erbinger, T., Rogers, T.: A survey of policy-based management approaches for service oriented systems. In: 19th Australian Conference on Software Engineering. IEEE, Perth, Australia (2008)
24. Oasis, eXtensible Access Control Markup Language (XACML) Version 3.0, https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html#_Toc325047205. Accessed: 8. 10. 2020
25. Kumaraguru, P., Cranor, L., Lobo, J., Calo, S.: A survey of privacy policy languages. In: Proceedings of the 3rd symposium on Usable privacy and security. ACM (2007)
26. Zhao, J., Binns, R., Van Kleek, M., Shadbolt, N.: Privacy languages: Are we there yet to enable user controls? In: Proceedings of the 25th International Conference Companion on World Wide Web. pp. 799–806. ACM, Montréal, Québec, Canada (2016)
27. Kasem-Madani, S., Meier, M.: Security and privacy policy languages: A survey, categorization and gap identification. arXiv:1512.00201. (2015)
28. Anderson, A.: A comparison of two privacy policy languages: EPAL and XACML. In: Proceedings of the 3rd ACM workshop on secure web services. pp. 53–60. ACM, Alexandria, Virginia, USA (2006)
29. Lazouski, A., Martinelli, F., Mori, P.: Usage control in computer security: A survey. Comput. Sci. Rev. **4**, 81–99 (2010)
30. Seamons, K.E., Winslett, M., Yu, T., Smith, B., Child, E., Jacobson, J., Mills, H., Yu, L.: Requirements for policy languages for trust negotiation. In: Proceedings Third International Workshop on Policies for Distributed Systems and Networks. pp. 68–79. IEEE, Monterey, California, USA, (2002).
31. Bertino, E., Ferrari, E., Squicciarini, A.: Trust negotiations: concepts, systems, and languages. Comput. Sci. Eng. **6**, 27–34 (2004)
32. Coi, J.D., Olmedilla, D.: A review of trust management, security and privacy policy languages. In: Proceedings of the International Conference on Security and Cryptography. pp. 483–490. INSTICC PRess, Porto, Portugal (2008)
33. Berners-Lee, T., Hendler, J., Lassila, O.: The semantic web. Sci. Am. **284**, 34–43 (2001)

34. Tonti, G., Bradshaw, J.M., Jeffers, R., Montanari, R., Suri, N., Uszok, A.: Semantic web languages for policy representation and reasoning: A comparison of KAoS, Rei, and Ponder. In: International Semantic Web Conference. pp. 419–437. Springer, Sanibel Island, Florida, USA (2003)
35. Duma, C., Herzog, A., Shahmehri, N.: Privacy in the semantic web: What policy languages have to offer. In: Eighth IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY'07). pp. 109–118. IEEE, Bologna, Italy (2007)
36. Leicht, J., Heisel, M.: A survey on privacy policy languages: Expressiveness concerning data protection regulations. In: 2019 12th CMI Conference on Cybersecurity and Privacy (CMI). pp. 1–6. IEEE, Copenhagen, Denmark (2019)
37. Damianou, N., Dulay, N., Lupu, E., Sloman, M.: The ponder policy specification language. In: International Workshop on Policies for Distributed Systems and Networks. pp. 18–38. Springer, Bristol, United Kingdom (2001)
38. Azraoui, M., Elkhiyaoui, K., Önen, M., Bernsmed, K., De Oliveira, A.S., Sendor, J.: A-PPL: an accountability policy language. In: Data privacy management. autonomous spontaneous security, and security assurance, pp. 319–326. Springer, Wroclaw, Poland (2014)
39. Adonis, A.A.: Critical engagement on digital sovereignty in international relations: Actor transformation and global hierarchy. Glob. J. Polit. Int. **21**, 262–282 (2019)
40. Otto, B., Auer, S., Cirullies, J., Jürjens, J., Menz, N., Schon, J., Wenzel, S.: Industrial Data Space Digitale Souveränität über Daten. Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e. V und Industrial Data Space e. V. (2016)
41. Posch, R.: Digital sovereignty and IT-security for a prosperous society. In: Informatics in the Future. pp. 77–86. Springer, Cham (2017)
42. Harzing, A.-W.: Publish or perish. https://harzing.com/resources/publish-or-perish. Zugegriffen: 27. Mai. 2020
43. Webster, J., Watson, R.T.: Analyzing the past to prepare for the future: Writing a literature review. MIS Q. **26**, 13–23 (2002)
44. Henze, M., Hiller, J., Schmerling, S., Ziegeldorf, J.H., Wehrle, K.: Cppl: Compact privacy policy language. In: Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society. pp. 99–110. ACM, New York, NY, USA (2016)
45. Reagle, J., Cranor, L.F.: The platform for privacy preferences. Commun. ACM **42**, 48–55 (1999)
46. van de Ven, J., Dylla, F.: Qualitative privacy description language. In: Annual Privacy Forum. pp. 171–189. Springer, Frankfurt a. M. (2016)
47. Gerl, A., Bennani, N., Kosch, H., Brunie, L.: LPL, towards a GDPR-compliant privacy language: Formal definition and usage. In: Hameurlain, A., Wagner, R. (Hrsg.) Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVII, pp. 41–80. Springer, Berlin (2018)
48. Benghabrit, W., Grall, H., Royer, J.-C., Sellami, M., Azraoui, M., Elkhiyaoui, K., Önen, M., De Oliveira, A.S., Bernsmed, K.: A Cloud Accountability Policy Representation Framework. In: Proceedings of the 4th International Conference on Cloud Computing and Services Science. pp. 489–498. SCITEPRESS, Barcelona, Spain (2014).
49. Guarda, P., Zannone, N.: Towards the development of privacy-aware systems. Inf. Softw. Technol. **51**, 337–350 (2009)

50. Ulbricht, M.-R., Pallas, F.: YaPPL-a lightweight privacy preference language for legally sufficient and automated consent provision in IoT scenarios. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology. pp. 329–344. Springer (2018)
51. Becker, M.Y., Malkis, A., Bussard, L.: S4P: A generic language for specifying privacy preferences and policies. Technical Report, Microsoft Research (2010)
52. Jiang, H., Bouabdallah, A.: JACPoL: a simple but expressive JSON-based access control policy language. In: IFIP International Conference on Information Security Theory and Practice. pp. 56–72. Springer, Crete, Greece (2017)
53. Uszok, A., Bradshaw, J.M., Jeffers, R., Tate, A., Dalton, J.: Applying KAoS services to ensure policy compliance for semantic web services workflow composition and enactment. In: The Semantic Web–ISWC 2004. pp. 425–440. Springer, Hiroshima, Japan (2004)
54. Morel, V., Pardo, R.: Three dimensions of privacy policies. arXiv preprint arXiv:1908.06814. (2019)
55. Li, N., Chen, H., Bertino, E.: On practical specification and enforcement of obligations. In: Proceedings of the second ACM conference on Data and Application Security and Privacy. pp. 71–82. ACM, San Antonio, Texas, USA (2012)
56. Bonatti, P.A., Duma, C., Fuchs, N., Nejdl, W., Olmedilla, D., Peer, J., Shahmehri, N.: Semantic web policies–a discussion of requirements and research issues. In: ESWC 2006: The Semantic Web: Research and Applications. pp. 712–724. Springer, Budva, Montenegro (2006)
57. Ferguson, D., Albright, Y., Lomsak, D., Hanks, T., Orr, K., Ligatti, J.: PoCo: A Language for specifying obligation-based policy compositions. In: Proceedings of the 2020 9th International Conference on Software and Computer Applications. pp. 331–338. ACM, Langkawi, Malaysia (2020)
58. Bonatti, P.A., Olmedilla, D.: Rule-based policy representation and reasoning for the semantic web. In: Reasoning Web 2007: Reasoning Web. pp. 240–268. Springer, Dresden, Germany (2007)
59. Sandhu, R., Park, J.: Usage control: A vision for next generation access control. In: Gorodetsky, V., Popyack, L., Skormin, V. (Eds.) Second International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security, pp. 17–31. Springer, St. Petersburg, Russia (2003)
60. Gil, G., Arnaiz, A., Diez, F.J., Higuero, M.V.: Evaluation methodology for distributed data usage control solutions. In: 2020 Global Internet of Things Summit. pp. 1–6. IEEE, Dublin, Ireland (2020)
61. Hilty, M., Pretschner, A., Basin, D., Schaefer, C., Walter, T.: A policy language for distributed usage control. In: Biskup, J., López, J. (Hrsg.) Computer Security – ESORICS 2007, pp. 531–546. Springer, Dresden, Germany (2007)
62. Bier, C.: How usage control and provenance tracking get together - a data protection perspective. In: 2013 IEEE Security and Privacy Workshops. pp. 13–17. IEEE, San Francisco, California, USA (2013)
63. Schuette, J., Brost, G.S.: LUCON: Data flow control for message-based IoT systems. In: 2018 17th IEEE International Conference On Trust. Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp. 289–299. IEEE, New York, NY, USA (2018)

64. Otto, B., Steinbuß, S., Teuscher, A., Lohmann, S., et. al.: IDS reference architecture model version 3.0. International Data Spaces Association (2019)
65. Karafili, E., Lupu, E.C.: Enabling data sharing in contextual environments: Policy representation and analysis. In: Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies. pp. 231–238. ACM, Indianapolis, Indiana, USA (2017)
66. Pretschner, A., Hilty, M., Basin, D.: Distributed usage control. Commun. ACM **49**, 39–44 (2006)
67. Kolar, M., Fernandez-Gago, C., Lopez, J.: Policy languages and their suitability for trust negotiation. In: DBSec 2018: Data and Applications Security and Privacy XXXII. pp. 69–84. Springer, Bergamo, Italy (2018)
68. Cranor, L.F., Guduru, P., Arjula, M.: User interfaces for privacy agents. ACM Transactions on Computer-Human Interaction. **13**, 135–178 (2006)
69. Mont, M.C., Pearson, S., Bramhall, P.: Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services. In: 14th International Workshop on Database and Expert Systems Applications. pp. 377–382. IEEE, Prague, Czech Republic (2003)
70. Karjoth, G., Schunter, M., Waidner, M.: Platform for enterprise privacy practices: Privacy-enabled management of customer data. In: PET 2002: Privacy Enhancing Technologies. pp. 69–84. Springer, San Francisco, California, USA (2002)
71. Kapitsaki, G.M.: Reflecting user privacy preferences in context-aware web services. In: 2013 IEEE 20th International Conference on Web Services. pp. 123–130. IEEE, Santa Clara, California, USA (2013)
72. Sunyaev, A.: Distributed ledger technology. In: Sunyaev, A. (Hrsg.) Internet computing: Principles of distributed systems and emerging internet-based technologies, pp. 265–299. Springer International Publishing, Cham (2020)
73. Kannengießer, N., Lins, S., Dehling, T., Sunyaev, A.: Trade-offs between distributed ledger technology characteristics. ACM Comput. Surv. **53**, 42:1–37 (2020)

Entwurfsmuster für die interdisziplinäre Gestaltung rechtsverträglicher Systeme

Ernestine Dickhaut, Laura Friederike Thies, Andreas Janson, Jan Marco Leimeister und Matthias Söllner

Zusammenfassung

Durch die Digitalisierung werden immer mehr Technologien entwickelt. Dabei gewinnt die soziotechnische Systementwicklung zunehmend an Bedeutung, in deren Rahmen nicht nur das technische System isoliert betrachtet wird, sondern auch der Nutzer und sein Umfeld. Insbesondere bei der Entwicklung rechtsverträglicher Systeme stehen Entwickler häufig aufgrund fehlenden rechtlichen Fachwissens vor großen Herausforderungen. Dies gilt insbesondere dann, wenn es um intelligente, selbstlernende Systeme geht. Diese Systeme

E. Dickhaut (✉) · J. M. Leimeister
Fachgebiet Wirtschaftsinformatik & Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Universität Kassel, Kassel, Deutschland
E-Mail: ernestine.dickhaut@uni-kassel.de

J. M. Leimeister
E-Mail: janmarco.leimeister@unisg.ch; leimeister@uni-kassel.de

L. F. Thies
Institut für Wirtschaftsrecht & Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Universität Kassel, Kassel, Deutschland
E-Mail: l.thies@uni-kassel.de

A. Janson · J. M. Leimeister
Institut für Wirtschaftsinformatik (IWI-HSG), Universität St.Gallen, St.Gallen, Schweiz
E-Mail: andreas.janson@unisg.ch

M. Söllner
Fachgebiet Wirtschaftsinformatik und Systementwicklung & Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG), Universität Kassel, Kassel, Deutschland
E-Mail: soellner@uni-kassel.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_23

sammeln, um die Qualität ihrer Dienste zu optimieren und Nutzerbedürfnissen zu entsprechen mithilfe leistungsfähiger Technologien große Mengen an personenbezogenen Daten, was Risiken für die informationelle Selbstbestimmung der Nutzer mit sich bringt. Um diesen Risiken entgegenzuwirken nutzen wir Anforderungs- und Entwurfsmuster. Ziel des Beitrags ist daher mittels eines multi-methodischen Ansatzes aufzuzeigen, welchen Beitrag interdisziplinäre Anforderungs- und Entwurfsmuster für die Entwicklung rechtsverträglicher und qualitativ hochwertiger KI-basierter Systeme leisten können. Um die Wirksamkeit der Muster zu untersuchen wurde mithilfe der Muster ein Lernassistent entwickelt und durch die Methode der Simulationsstudie evaluiert.

Schlüsselwörter

Entwurfsmuster • Interdisziplinäre Gestaltung • Rechtsverträglichkeit

1 Rechtsverträgliche Lernassistenten im universitären Einsatz

Smarte persönliche Assistenten (SPA), wie beispielsweise Alexa und Siri, werden immer beliebter [1]. Dabei kommen sie nicht nur in der privaten Nutzung im Alltag zum Einsatz, sondern auch vermehrt im Lernkontext [2, 3]. Die Entwicklung smarter Lernassistenten für den universitären Einsatz stellt Entwickler vor Herausforderungen. Sowohl datenschutzrechtliche Vorgaben als auch die didaktische Umsetzung der Technologie müssen den Anforderungen der Universität genügen. Der Einsatz eines Lernassistenten im Lehr-Lern-Kontext impliziert bei den Studierenden, dass die Technologie ganzheitlich durch die Lehrperson, aber auch durch die Universität geprüft wurde. Daher sind bei der Entwicklung smarter Lernassistenten verschiedene Disziplinen beteiligt, die sich von Didaktik, über Psychologie, Rechtswissenschaft bis hin zur Informatik erstrecken [4]. Dabei entstehen mehrdimensionale Anforderungen an den Lernassistenten, die während der Entwicklung berücksichtigt werden müssen.

Eine Lehrperson hat vor dem Einsatz eines smarten Lernassistenten in der Lehre zwei Möglichkeiten, was in der Systementwicklung als „make or buy“ bezeichnet wird. Entweder wird eine Technologie verwendet, die durch einen Drittanbieter entwickelt wurde (buy), oder die Lehrperson bzw. die Universität entwickelt ein eigenes System (make). Die „make-Entscheidung“ hat den Vorteil, dass den mehrdimensionalen Anforderungen individuelle Aufmerksamkeit

gewidmet werden kann und so die Technologie für den individuellen Anwendungsfall der Universität bestmöglich adaptiert werden kann. In der Praxis zeigt sich besonders, dass in der Vereinigung rechtlicher Anforderungen und Anforderungen der Dienstleistungsqualität häufig große Kompromisse eingegangen werden müssen [5]. Für die Anpassungsfähigkeit der Systeme an den Nutzer werden häufig große Datenmengen erforderlich, ohne deren Nutzung die Qualität des Systems leidet [6]. Eine Unterstützung der Entwickler, die ganzheitlich die Entwicklung von der Anforderungserhebung bis hin zur praktischen Evaluation begleitet, ist erforderlich. In der Informatik haben sich Anforderungs- und Entwurfsmuster etabliert, die Entwicklern bei wiederkehrenden Problemen mit bewährten Lösungen unterstützen [7]. In ihrer bisherigen Darstellung enthalten die Muster jedoch kein interdisziplinäres Gestaltungswissen und können Entwickler nicht bei interdisziplinären Problemstellungen unterstützen [8]. Daraus entsteht folgende Forschungsfrage:

Wie kann die Entwicklung eines rechtsverträglichen smarten Lernassistenten durch interdisziplinäre Anforderungs- und Entwurfsmuster unterstützt werden?

Um die Forschungsfrage zu beantworten und einen Beitrag zur Schließung der Forschungslücke zu leisten, haben wir einen interdisziplinären Musterkatalog bestehend aus Anforderungs- und Entwurfsmuster für die Entwicklung von smarten persönlichen Assistenten entwickelt. Dabei haben wir ein besonderes Augenmerk auf die Disziplinen Recht und Dienstleistungsqualität gelegt.

In diesem Beitrag legen wir dar, wie ein solcher Musterkatalog zur erfolgreichen Entwicklung eines rechtsverträglichen und qualitativ hochwertigen smarten Lernassistenten beitragen kann. Dabei beschränken wir uns nicht allein auf den Entwicklungsprozess, sondern stellen auch einen Ansatz für die interdisziplinäre Evaluation vor, in der der prototypisch entwickelte Lernassistent sowohl mit Nutzern als auch auf seine Rechtmäßigkeit hin evaluiert wird. Hierfür verwenden wir die Methodik der Simulationsstudie, die in der Rechtswissenschaft etabliert ist und uns frühzeitig im Entwicklungsprozess die Möglichkeit bietet, Aussagen über die Rechtmäßigkeit des Systems zu treffen und mögliche Gestaltungsverbesserungen abzuleiten.

2 Bisherige Forschung

2.1 Gestaltung smarter persönlicher Assistenten

SPA können das tägliche Leben auf vielfältige Weise unterstützen, z. B. auf Smartphones, im Auto, bei Dienstleistungsbegegnungen, in intelligenten häuslichen Umgebungen oder als Unterstützung für ältere Menschen. Nach Knote et al. lassen sich SPA in fünf Archetypen unterscheiden: Adaptive Voice-(Vision-)Assistenten, Chatbot-Assistenten, verkörperte virtuelle Assistenten, passiv-pervasive Assistenten und natürliche Konversationsassistenten. Einen smarten Lernassistenten ordnen wir demnach als Unterklasse von SPA ein, die sich auf eine spezielle Nutzergruppe und einen spezifischen Anwendungsfall spezialisiert hat. Aus technischer Perspektive unterscheiden sich smarte Lernassistenten nicht von Chatbot-Assistenten, da auch die Verarbeitung der Spracheingabe und -verarbeitung ähnlich abläuft [4]. Ein wichtiges Merkmal hierbei ist die individuelle Adaption an den Lernenden und seinen aktuellen Lernstand [9]. Die individuelle Anpassungsfähigkeit des Lernassistenten an den Nutzer ermöglicht es, sowohl schnell, als auch individuell Feedback zu geben [10].

Um SPA zu entwickeln, müssen wir Anforderungen aus verschiedenen Disziplinen Beachtung schenken. Schlüsselaspekte beziehen sich z. B. auf ihre Usability und User Experience, die wir als Gesamtqualität der Dienstleistung zusammenfassen können. Der Dienstleistungsqualität wird während des Entwicklungsprozesses häufig große Aufmerksamkeit geschenkt. Insbesondere die direkte Interaktion mit dem Nutzer erfordert große Beachtung. Gleichzeitig wächst aber beispielsweise die Besorgnis dahingehend, dass diese Systeme ihre Nutzer abhören, ohne durch ein Wake-Word aktiviert worden zu sein, was zeigt, dass hohe Qualitätswahrnehmungen mit diesen Geräten nur schwer zu erreichen sind. Hinzu kommt, dass gesetzliche Anforderungen oft nur in einem Mindestmaß erfüllt werden, um den Minimalanforderungen des Rechts zu genügen [11]. In diesem Zusammenhang fehlt es den Systementwicklern oft am notwendigen Fachwissen, um rechtliche Anforderungen zur Entwicklung eines SPA derart umzusetzen, dass die rechtlichen Vorgaben über das beschriebene Mindestmaß hinaus adressiert werden. In diesem Zusammenhang gibt es große Unsicherheiten in der Forschung darüber, wie Entwickler bei der Gestaltung von SPA unterstützt werden können [12].

Daher stellen wir einen Ansatz für die Entwicklung von smarten Lernassistenten vor, der neben Qualitätsaspekten die rechtlichen Vorgaben gleichwertig, bereits während der Entwicklung berücksichtigt. Der Ansatz basiert auf Anforderungs- und Entwurfsmustern, die in der Systementwicklung bereits ein

etabliertes Werkzeug darstellen, um komplexes Wissen für Anforderungsanalysten und Systementwickler zugänglich und somit auch anwendbar zu machen [13]. Die Muster kommen in der Systementwicklung an verschiedenen Zeitpunkten zu tragen. Anforderungsmuster verfolgen das Ziel, eine Sammlung von Wissen und Erfahrungen zu schaffen, die Softwareentwicklern helfen (sollen) wiederkehrende Probleme zu lösen [14]. Demnach ist ein Anforderungsmuster ein wiederverwendbares Rahmenwerk aus Erfahrungen, das für die Identifizierung von Anforderungen verwendet werden kann [14]. Dabei decken Anforderungsmuster nicht alle denkbaren Problembereiche ab und lösen aufgrund ihrer Abstraktion in der Regel mehrere Problemstellungen durch gemeinsame Entwurfsmuster. Entwurfsmuster kommen zu einem späteren Zeitpunkt zum Einsatz und lösen konkrete Problemstellungen indem sie mögliche Lösungsansätze zur Verfügung stellen. Durch Entwurfsmuster wird der Anwender[1] nicht in seiner Kreativität eingeschränkt, bekommt mögliche Lösungsansätze präsentiert, die auf das individuelle Problem angewendet werden können.

2.2 Simulationsstudie

Die Simulationsstudie wurde seit ihrer Entwicklung vielfach, in verschiedenen Konstellationen, eingesetzt [15–17]. Die Methode der Simulationsstudie dient dazu, relevante soziale Voraussetzungen und Folgen einer Technik zu bewerten und anwendungsnahe Gestaltungsvorschläge zu entwickeln, bevor die Technik in der Praxis eingesetzt wird [15].

Dazu werden realitätsnahe Anwendungsszenarien kreiert, die auch kritische Nutzungssituationen umfassen können, die in der Realität selten auftreten [18]. Der Vorteil dieser Methode liegt darin, dass auf diese Weise riskante Nutzungssituationen provoziert werden können, ohne dass die Teilnehmer realen Gefahren ausgesetzt werden [19].

Um, wie in diesem Fall möglichst realitätsnahe zu erproben, wie eine Technik vor Gericht in Hinblick auf ihre Vereinbarkeit mit rechtlichen Vorgaben beurteilt werden würde, werden echte Richter und Rechtsanwälte in die Studie eingebunden, die die realitätsnahen, nachgestellten Fälle bearbeiten [16, 20, 21]. Diese sachverständigen Testpersonen werden während der Simulation wissenschaftlich beobachtet und teilen ihre Erfahrungen mit den Wissenschaftlern. Die Ergebnisse

[1] Zur besseren Lesbarkeit des Textes wird auf die Aufzählung mehrerer Geschlechter verzichtet. Die Begriffe „Entwickler“ oder „Nutzer“ und ähnliche Begriffe umfassen immer auch alle Personen anderen Geschlechts.

können dann direkt in die Gestaltung der Technik einfließen, welche im nächsten Abschnitt vor dem Hintergrund interdisziplinärer Anforderungsmuster beleuchtet wird.

3 Anforderungen der Rechtsverträglichkeit und Dienstleistungsqualität

Vor der Entwicklung des smarten Lernassistenten wird eine ausführliche Anforderungserhebung durchgeführt. Dabei werden die beiden Disziplinen zunächst größtenteils getrennt voneinander analysiert und anschließend Anforderungen konsolidiert, die für die Entwicklung als Leitfaden dienen sollen. Die Erhebung der Anforderungen wird durch interdisziplinäre Anforderungsmuster unterstützt [22].

3.1 Anforderungen der Rechtsverträglichkeit

Für die Entwicklung werden – basierend auf den Chancen und Risiken, die smarte persönliche Assistenten in der Lehre für die Grundrechte der Nutzer mit sich bringen – die Grundlagen „Zweckbindung“, „Datensparsamkeit und Datenvermeidung“, „Speicherbegrenzung“, „Transparenz“, „Einwilligung“, „Kontrollierbarkeit“, „Intervenierbarkeit“, „Verhaltensfreiheit“, „Verfügbarkeit“, „Vertraulichkeit“, „Integrität“, „Identifizierung des Nutzers“, „Keine Verarbeitung sensitiver Daten“, „Kernbereichsschutz“, „Keine Profilbildung“ und „Schutzvorkehrungen für Heranwachsende“ als relevante Grundlagen für die Auswahl der Anforderungsmuster eingestuft. Im nächsten Schritt werden die auf den genannten Grundlagen basierenden Anforderungsmuster in Hinblick auf das konkrete Einsatzszenario des Lernassistenten hin ausgewertet und die dafür relevanten Anforderungsmuster ausgewählt.

Jedes Anforderungsmuster hat die gleiche Struktur aufgebaut und beinhaltet zum besseren Verständnis des Musters Informationen zu dem Ziel der Anforderungen, sowie eine User Story, die den Anwendungskontext spezifizieren. Für den Einsatz im Entwicklungsprozess werden außerdem Informationen zur Systemeigenschaft des anzuwendenden Systems bereitgestellt. Um einen Eindruck zu vermitteln, ist hier ein beispielhaftes Anforderungsmuster aus dem Bereich des Rechts abgebildet (siehe Abb. 1).

Aus der Analyse der rechtlichen Anforderungsmuster gehen für smarte persönliche Assistenten in der Lehre 25 relevante Anforderungen hervor. In Tab. 1 sind fünf wichtige rechtliche Anforderungen exemplarisch dargestellt.

Anforderungsmuster Rechtsverträglichkeit				
	Name	**Löschroutinen**		**RV7**
	Ziel	Das System verarbeitet wenig personenbezogene Daten des Nutzers.		
	Grundlage	K1, K2, K3, K17, K18	**Priorität**	Hoch
	Systemeigenschaften	Alle		
	Abhängigkeiten	RV1, RV3, RV5		
	Verknüpfungen	RV2, RV5, RV34		
	Konflikte	DLQ8, DLQ18, DLQ19, DLQ22, DLQ25, DLQ26		
	Anforderung	**Das System prüft regelmäßig, welche personenbezogenen Daten noch zur Zweckerreichung erforderlich sind.**		
	User Story	Als Nutzer möchte ich, dass das System nur solche Daten von mir verarbeitet, die für das Funktionieren des Systems nötig sind		
	Hinweise	Mechanismen für regelmäßig Überprüfungen. Löschkonzepte. Keine Schattendatenbanken. Entfernung des Personenbezugs durch Anonymisierung oder Pseudonymisierung.		

Abb. 1 Beispielhaftes Anforderungsmuster Rechtsverträglichkeit

Tab. 1 Übersicht der Anforderungen der Rechtsverträglichkeit

ID	Grundlage	Anforderung Lernassistent
RV1	Zweckbindung	Die Verwendungszwecke werden, unter Einräumung von granularen Einwilligungsmöglichkeiten, präzise und differenziert angegeben
RV2	Datensparsamkeit und Datenvermeidung	Das System verarbeitet nur solche Daten, die zur Erreichung des Verarbeitungszwecks erforderlich sind
RV3	Kernbereichsschutz	Das System verarbeitet keine Daten, die die Privat- oder Intimsphäre des Nutzers betreffen
RV4	Keine Profilbildung	Das System legt kein umfassendes Persönlichkeitsprofil des Nutzers an
RV5	Keine Profilbildung	Das System fällt auf Basis von Daten mit Diskriminierungspotential keine Entscheidungen

3.2 Anforderungen Dienstleistungsqualität

Für die Anforderungserhebung der Anforderungen aus Sicht der Dienstleistungsqualität (DLQ) werden Anforderungsmuster genutzt, wie auch bei der Erhebung rechtlicher Anforderungen. Ein beispielhaftes Anforderungsmuster, dass für die Entwicklung des rechtsverträglichen Lernassistenten verwendet wurde, ist in Abb. 2 zu sehen.

Zunächst werden die Kategorien der Grundlagen der dargestellten Anforderungen analysiert. Für die Erstellung des Lernassistenten werden die Kategorien „Kompetenz“, „Lernfähigkeit“, „Wohlwollen“, „Empathie“, „Komfort“, „Design“, „Spaß“, „Personalisierung“ und „Funktionalität“ als relevant angesehen. Nach der Analyse aller Grundlagen werden die einzelnen Grundlagen genauer betrachtet. Jede Grundlage beinhaltet zwei bis sechs Anforderungsmuster, die nun für den konkreten Anwendungsfall genauer analysiert werden, um so genaue Anforderungen extrahieren zu können. Für den Einsatz im Entwicklungsprozess werden außerdem Informationen zur Systemeigenschaft des anzuwendenden Systems bereitgestellt.

Das Ergebnis der Analyse sind 13 Anforderungen, die aus Sicht der Dienstleistungsqualität im zu entwickelnden Lernassistenten umgesetzt werden müssen. In

Anforderungsmuster Dienstleistungsqualität				
	Name	**Meiden sensibler Themen**		**DLQ20**
	Ziel	Der Nutzer weiß, dass er mit dem System nicht zu sensiblen Themen kommunizieren kann.		
	Grundlage	Empathie	**Priorität**	Mittel
	Systemeigenschaften	Ausrichtung: zweiseitig Kommunikation: primitive NL, compound NL		
	Abhängigkeiten			
	Verknüpfungen	RV5, RV22, RV23		
	Konflikte	RV1		
	Anforderung	**Das System soll den Nutzer dazu ermutigen, sensible Themen zu meiden, indem er keine tiefgreifenden Dialoge zu diesen Themen zulässt.**		
	User Story	Als Nutzer möchte ich wissen, dass ich mit dem System nicht tiefergehend über sensible Themen kommunizieren kann, damit ich mich auf die wesentlichen Themen konzentrieren kann.		
	Hinweise	Für Kategorisierung siehe z.B. Art 9 DSGVO		

Abb. 2 Beispielhaftes Anforderungsmuster Dienstleistungsqualität

Tab. 2 Übersicht der Anforderungen der Dienstleistungsqualität

ID	Grundlage	Anforderung Lernassistent
DLQ1	Empathie	Das System soll dem Nutzer durch wohlwollende Dialoggestaltung vermitteln, dass es sich um seine Belange kümmert
DLQ2	Empathie	Das System soll auf emotionale Sprache adäquate Antworten formulieren
DLQ3	Komfort	Das System bietet dem Nutzer möglichst einfache Anfrage- und Antwortmöglichkeiten
DLQ4	Personalisierung	Das System soll den Nutzer nach erstmaliger Nutzung wiedererkennen
DLQ5	Lernfähigkeit	Das System soll auf Basis der Relevanzbewertungen des Nutzers mit fortschreitender Nutzungsdauer relevantere Informationen für den Nutzer ausgeben

diesem Beitrag wollen wir die praktische Umsetzung anhand einer Auswahl der Anforderungen genauer beschreiben und wählen hierfür die in Tab. 2 dargestellten fünf Anforderungen aus.

3.3 Verknüpfung der Anforderungen

Jedes Anforderungsmuster enthält neben inhaltlichen Details zu den Anforderungen auch weitere Informationen, die sich auf die Interaktion zwischen den verschiedenen Anforderungsmustern beziehen. So werden beispielsweise Abhängigkeiten, Verknüpfungen oder mögliche Konflikte dargelegt. Da die Anforderungen nicht isoliert voneinander betrachtet werden können, werden in einem nächsten Schritt alle erhobenen Anforderungen auf mögliche Interaktionen hin geprüft.

In vielen Fällen stehen sich die Anforderungen aus dem Bereich der Dienstleistungsqualität und die aus dem Bereich des Rechts diametral entgegen [5]. So ist die Personalisierung der Funktionalitäten ein entscheidendes Merkmal für die Zufriedenheit der Nutzer mit dem Dienst [23]. Aus rechtlicher Sicht ist es jedoch stets geboten, so wenige personenbezogene Daten wie möglich zu verarbeiten, was einer ausgeprägten Personalisierung entgegensteht [6]. Auch Kontextsensitivität und Selbstlernfähigkeit, beides Grundvoraussetzungen für die Bereitstellung vieler personalisierter Dienste, erfordern die Verarbeitung vieler personenbezogener Daten. Eine rechtsverträgliche Gestaltung jedoch verlangt die Vermeidung

der Verarbeitung von Daten mit persönlichem Bezug [24]. Diese Zielkonflikte zeigen sich bei der Entwicklung des Lernassistenten. Wenn sich der Lernassistent an den individuellen Lernstatus des Nutzers anpasst, können ihm genau für ihn notwendigen Materialien bereitgestellt werden. Vergleichbar ist dies mit Individualunterricht in einem 1:1 Lehrszenario. Während ein Lernassistent, der nicht an den Lernenden angepasst ist, lediglich ein 1:n Szenario abbilden kann. Hierbei fehlt der Bezug zu dem individuellen Lernenden. Für die Anpassungsfähigkeit werden jedoch Daten des Lernenden benötigt. Um solchen Konflikten entgegen zu wirken und letztendlich eine für alle Bereiche zufriedenstellende Lösung zu finden, wurden die erhobenen Anforderungskataloge im Gesamten betrachtet und mögliche Konflikte zur Suche nach Lösungen vermerkt.

4 Gestaltung rechtsverträglicher smarter persönlicher Lernassistenten

Als Grundlage für die Gestaltung des rechtsverträglichen smarten Lernassistenten dienen zum einen die zuvor durchgeführte Anforderungserhebung, sowie Interviews mit Dozierenden und Didaktik-Experten (N = 7), zum anderen aber auch Entwurfsmuster, die bei der Lösung möglicher Konflikte in der Entwicklung unterstützen.

Das verwendete Lehrmaterial basiert auf den Inhalt der Lehrveranstaltung und wird gemeinsam mit dem Dozierenden und weiteren Lehrpersonen der Lehrveranstaltung aufbereitet und in den Lernassistenten integriert. Während der iterativen Entwicklung wurden die Dozierenden immer wieder einbezogen. Das Lehrmaterial wird in Form eines Quiz dargestellt. Der Lernassistent wird für eine universitäre Lehrveranstaltung als ergänzende Klausurvorbereitung entwickelt, um gemeinsam mit dem Nutzer den Lehrstoff der Veranstaltung spielerisch zu wiederholen. In dem Lernquiz stellt der Lernassistent dem Nutzer eine Frage und bietet vier mögliche Antworten, wovon genau eine Antwort richtig ist.

Wichtige Anforderungen aufseiten der Dienstleistungsqualität an den smarten Lernassistenten basieren auf den Grundlagen „Personalisierung“ und „Lernfähigkeit“. So wäre es aus Qualitätssicht wünschenswert, dass der Lernassistent den Nutzer nach erstmaliger Nutzung wiedererkennen kann. Wünschenswert wäre außerdem, dass der Lernassistent auf Basis der Relevanzbewertungen des Nutzers mit fortschreitender Nutzungsdauer relevantere Informationen für den Nutzer ausgeben kann (siehe Tab. 2).

Die auf den Grundlagen „Datensparsamkeit und Datenvermeidung“, „Kernbereichsschutz“ und „Keine Profilbildung“ basierenden rechtlichen Anforderungen

an den Lernassistenten verlangen hingegen, dass nur solche personenbezogenen Daten verarbeitet werden, die zur Erreichung des Verarbeitungszwecks erforderlich sind, dass kein umfassendes Persönlichkeitsprofil des Nutzers angelegt wird und das auf Basis von Daten mit Diskriminierungspotential gehören, keine Entscheidungen gefällt werden (siehe Tab. 2).

Zu Beginn der Entwicklung werden die erhobenen Anforderungen betrachtet, um einen genauen Überblick über das zu entwickelnde System zu erhalten. Danach werden die Anforderungen abgeglichen und Zielkonflikte identifiziert. Um diese Zielkonflikte aufzulösen und zufriedenstellenden Lösungen zuzuführen, kommen interdisziplinäre Entwurfsmuster zum Einsatz, die die konfliktären Anforderungen des Rechts und der Dienstleistungsqualität adressieren und mögliche Lösungswege aufzeigen.

Bei der Umsetzung der erhobenen Anforderungen, zeigen sich klare Konflikte zwischen den beiden Disziplinen auf. Würde man alle Anforderungen der Dienstleistungsqualität voll verwirklichen, würde gegen rechtliche Anforderungen verstoßen werden. Würden alle rechtlichen Anforderungen vollumfänglich umgesetzt, würde hingegen die Dienstleistungsqualität des Lernassistenten leiden. Ein beispielhafter Konflikt zwischen den Anforderungen „Personalisierung“ der Dienstleistungsqualität und „Datensparsamkeit und Datenvermeidung“ der Rechtsverträglichkeit, lassen sich nicht gleichermaßen umsetzen, da sie einander widersprechen. Um die beschriebenen Konflikte bestmöglich aufzulösen und einer qualitativ hochwertigen wie rechtsverträglichen Lösung zuzuführen, kommt das Entwurfsmuster „Datenschutzfreundliches Nutzerprofil“ zum Einsatz (siehe Abb. 3).

Das Entwurfsmuster „Datenschutzfreundliches Nutzerprofil“ löst den beschriebenen grundlegenden Zielkonflikt, indem es spezifiziert, welche personenbezogenen Daten des Nutzers auf welche Art und Weise vom Lernassistenten verarbeitet und im Nutzerprofil gespeichert werden dürfen. Dabei wird in der Lösung unter anderem vorgeschlagen, dass personenbezogene Daten mit Bezug zur Privat- und Intimsphäre, sowie sensible Daten nicht zur Profilbildung genutzt werden dürfen. Eine strenge Einhaltung des Zweckbindungsgrundsatzes stellt sicher, dass nur solche personenbezogenen Daten verarbeitet werden, die zur Zweckerreichung erforderlich sind. Gleichzeitig garantiert diese Lösung auch, dass die Anforderungen aufseiten der Dienstleistungsqualität umgesetzt werden. Eine personalisierte Art der Dienstleistungserbringung wird ermöglicht, wenn es sich nicht um Daten, die zur Privat- oder Intimsphäre des Nutzers gehören oder um sensible Daten, handelt. Um dabei die informationelle Selbstbestimmung des Nutzers zu gewährleisten, erfolgt eine Personalisierung nur, wenn der Nutzer aktiv einwilligt. Sollte keine Einwilligung erfolgen, wird kein Nutzerprofil angelegt. Außerdem wird im

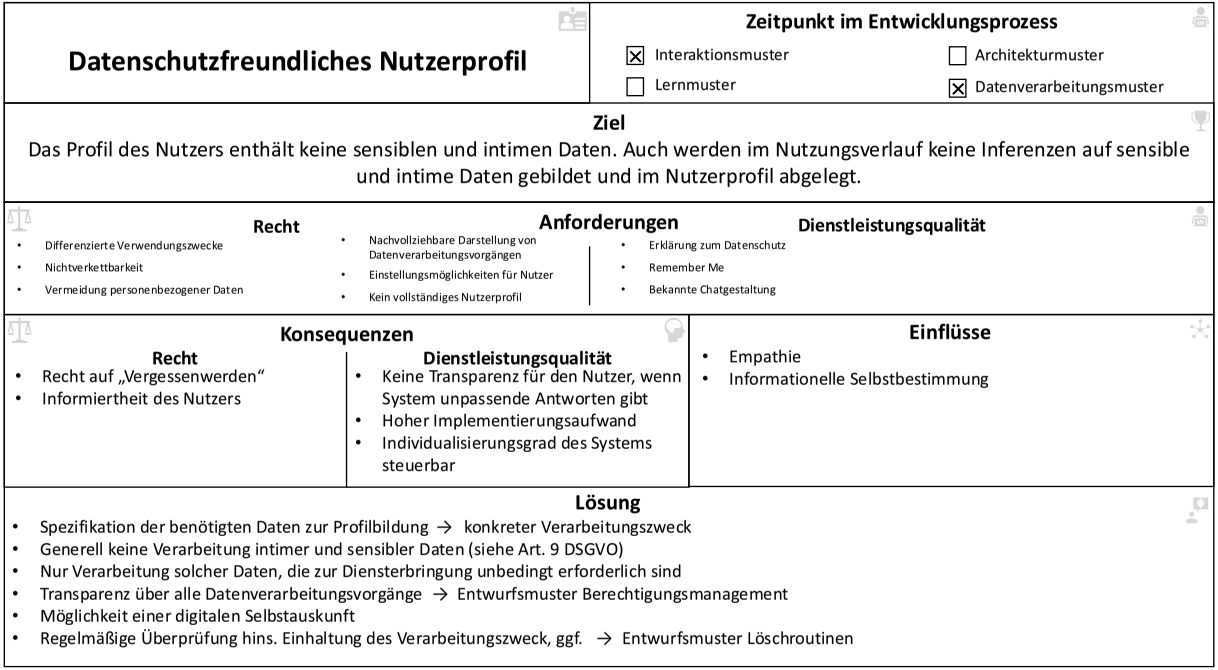


Abb. 3 Entwurfsmuster Datenschutzfreundliches Nutzerprofil

Entwurfsmuster vorgeschlagen, eine Identifizierung des Nutzers auf dem Endgerät auf Basis eines selbstgewählten Pseudonyms zu ermöglichen. Durch die Pseudonymisierung wird kein Nutzerprofil angelegt, das Rückschlüsse auf die Person selbst zulässt. Dennoch wird erreicht, dass der Nutzer eine Möglichkeit zur Identifizierung hat und der Lernassistent dadurch immer wieder auf den aktuellen Lernfortschritt zugreifen kann, um die Lehrinhalte daran anzupassen. Dadurch werden zum einen die Anforderungen RV3 und RV5 der Rechtsverträglichkeit umgesetzt, indem kein umfassendes persönliches Nutzerprofil angelegt wird und auf deren Basis keine Diskriminierungen erfolgen können. Zum anderen wurden durch die Umsetzung des Entwurfsmusters auch die konfliktäre Anforderung DLQ4 der Dienstleistungsqualität umgesetzt, die besagt, dass das System den Nutzer nach erstmaliger Nutzung wiedererkennen soll.

Des Weiteren besagt das Entwurfsmuster, dass der Verwendungszweck der Datenverarbeitung präzise und differenziert angegeben werden muss. Außerdem wird hierfür eine granulare Einwilligungsmöglichkeit vorgeschlagen. Die Lösungsvorschläge aus dem Entwurfsmuster werden bei der Entwicklung des Lernassistenten umgesetzt und in den Voreinstellungen eine Personalisierung zunächst deaktiviert. So kann der Nutzer bei der Anmeldung genau auswählen, welcher Datenspeicherung er zustimmt. Hierfür erhält er außerdem zusätzliche Informationsmöglichkeiten, die genau darlegen, warum die jeweilige Datenspeicherung notwendig ist, und welchen Mehrwert diese für die Erreichung der Dienstleistungsqualität hat. Außerdem wird, um die Transparenz hinsichtlich aller Datenverarbeitungen, die im Muster empfohlen wird, den Lernassistenten derart gestaltet, dass die Nutzer situationsadäquat über stattfindende Datenverarbeitungsvorgänge informiert werden. Ihnen werden nicht nur bei der ersten Nutzung, sondern immer dann, wenn relevante Datenverarbeitungen stattfinden, entsprechende Informationen geboten. Um einen Ausgleich zwischen Transparenz und störungsfreier Nutzung zu gewährleisten, haben wir den Nutzern in den Einstellungen die Möglichkeit eingeräumt, auszuwählen, wie oft und wie detailliert sie über Datenverarbeitungen informiert werden möchten. Ergänzend dazu hat der Nutzer, wie im Entwurfsmuster empfohlen, zu jedem Zeitpunkt die Möglichkeit in den Einstellungen eine digitale Selbstauskunft über die Speicherung seiner Daten einzusehen. Dies unterstützt die Transparenz der Datenspeicherung.

Um den Anforderungen des Rechts zur Zweckbindung gerecht zu werden, empfiehlt das Entwurfsmuster die regelmäßige Prüfung, welche personenbezogenen Daten noch zur Zweckerreichung erforderlich sind. Hierfür können beispielsweise Löschroutinen einen Lösungsansatz darstellen. Im Lernassistenten wird nach Abschluss eines Semesters die Möglichkeit solche automatisierten Löschroutinen durchzuführen umgesetzt.

5 Evaluation des digitalen Lernassistenten

Um den entwickelten Lernassistenten zu evaluieren, wird eine zweiteilige Simulationsstudie durchgeführt, mit der die Technologie auf Dienstleistungsqualität, wie auf Rechtsverträglichkeit hin überprüft werden kann. Im ersten Teil wird die Technologie in einer praktischen Evaluation mit Nutzern auf Usability, User Experience und mögliche Anwendungsprobleme untersucht. Der zweite Teil der Simulationsstudie dient zur Evaluation der Rechtmäßigkeit des Lernassistenten. In diesem zweiten Teil der Studie wird eine simulierte Gerichtsverhandlung durchgeführt, in der das System unter Mitwirkung echter Richter und Anwälte in simulierten Gerichtsprozessen auf seine Rechtmäßigkeit hin evaluiert wird.

Um das primäre Ziel des ersten Teils der Simulationsstudie zu untersuchen, ist die Verwendung des Lernassistenten in der Praxis durch echte Nutzer unabdingbar. Für die Evaluation wird der Lernassistent in einer universitären Grundlagenveranstaltung für Wirtschaftswissenschaften als ergänzende Klausurvorbereitung eingesetzt.

Die Teilnehmer können an drei Terminen in einem Zeitraum von zwei Wochen eine Stunde lang gemeinsam mit dem Lernassistenten für die Klausur lernen und das erworbene Wissen aus der Lehrveranstaltung wiederholen. Das Angebot findet auf freiwilliger Basis statt. Anschließend werden in Fragebögen die Zufriedenheit der Studierenden mit dem Lernassistenten erfragt und insbesondere Aspekte der Rechtsverträglichkeit und Dienstleistungsqualität in den Fokus gestellt. Außerdem wird in einer qualitativen Befragung nach Verbesserungsvorschlägen gefragt.

Um den mithilfe der Anforderungs- und Entwurfsmuster entwickelten prototypischen Lernassistenten von rechtlicher Seite aus zu evaluieren, wird die Methode der Simulationsstudie angewendet. Ziel der Simulation ist es, zu evaluieren, wie der von uns mithilfe von Anforderungs- und Entwurfsmustern entwickelte Lernassistent in der Praxis in Hinblick auf seine Rechtmäßigkeit beurteilt wird und dabei schwerpunktmäßig herauszufinden, inwiefern die Anforderungs- und Entwurfsmuster dazu geeignet sind, die vollständige Umsetzung der datenschutzrechtlichen Vorgaben zu beweisen. Daneben prüfen wir auch andere Gestaltungsmerkmale, wie unsere Implementierung der Betroffenenrechte oder der Transparenzvorgaben aus der DSGVO, richterlich prüfen lassen.

Dazu werden insgesamt vier Fälle entworfen, von denen zwei verwaltungsrechtlicher Art und zwei zivilrechtlicher Art sind. Dabei wird darauf geachtet, dass die Fälle zum einen realitätsnah sind und zum anderen darauf, dass prozessrechtliche Fragen, wie etwa die der Zuständigkeit des Gerichts, und andere für uns weniger relevante Aspekte wie die exakte Schadenshöhe, nicht zu viel Raum einnehmen. Alle Fälle werden derart konstruiert, dass Studierende sich,

aus verschiedensten Gründen, gegen den Einsatz des von uns entwickelten Lernassistenten in der Lehre wenden.

Auf Basis der konstruierten Fälle erstellen Anwälte realitätsnahe Klageschriften und Klageerwiderungen sowie weitere vorprozessliche Korrespondenz, die die Grundlage für den nachfolgenden Prozess bilden. Der Anwalt der Beklagtenseite, also der Universität, stützt seine Argumentationen in den Klageerwiderungen in allen Fällen maßgeblich auf die verwendeten Anforderungs- und Entwurfsmuster. In der Klageerwiderung geht er ausführlich darauf ein, welche datenschutzrechtlichen Vorgaben die Muster umsetzen und wie die Lösungsvorschläge aus den Mustern programmiert wurden. Die Muster wurden mithin dazu verwendet, zu beweisen, dass der entwickelte Lernassistent unter Einhaltung aller datenschutzrechtlichen Vorgaben entwickelt wurde.

Im Anschluss an die Vorverfahren werden die verwaltungsrechtlichen Gerichtsprozesse aufgrund der covid-19 Pandemie in einer Videokonferenz verhandelt, während die zivilrechtlichen Prozesse im schriftlichen Verfahren durchgeführt werden. Dabei wird besonders darauf geachtet, das Szenario so realitätsnah wie möglich durchzuführen, weshalb unter anderem auch Roben getragen werden und den Ablauf der Gerichtsverhandlung unter Leitung der Richterin entsprechend den einschlägigen prozessrechtlichen Vorgaben gestaltet.

6 Ergebnisse

Der Einsatz interdisziplinärer Anforderungs- und Entwurfsmuster hilft in der Systementwicklung fachfremdes Domänenwissen zu kodifizieren und in einem System umzusetzen. Die Unterstützung eines Katalogs, der im Entwicklungsprozess von Anfang, der Anforderungserhebung, bis zum Ende, der eigentlichen Gestaltung des Systems, unterstützt, hat sich in unserer Evaluation als geeignetes Verfahren herausgestellt, um einen rechtsverträglichen Lernassistenten zu entwickeln. In den Prozessen, die unter Leitung von Richtern aus der Praxis durchgeführt werden, stehen die Anforderungs- und Entwurfsmuster im Fokus. Die Muster werden in den mündlichen Verhandlungen vom Anwalt der Universität herangezogen, um seine Ausführungen hinsichtlich der Einhaltung der datenschutzrechtlichen Vorgaben zu untermauern. Die Verwaltungsrichterin, die den Lernassistenten in ihrem Urteil im Anschluss an die mündliche Verhandlung als rechtmäßig einstuft, hält die Muster für sehr hilfreich, die Einhaltung rechtlicher Vorgaben bei einer Technik zu beweisen. Als Ergebnis dieser Simulationsstudie lässt sich festhalten, dass die Anforderungs- und Entwurfsmuster zum einen ein geeignetes Mittel sind, Technik rechtskonform zu entwickeln. Zum

anderen lassen sie sich gut dafür verwenden, vor Gericht die Rechtmäßigkeit einer Technik zu beweisen.

Gerade der Einsatz der Entwurfsmuster hat sich für die Umsetzung konfliktärer Anforderungen als hilfreich erwiesen. Dadurch, dass die Lösungsansätze auf der einen Seite abstrakt sind, aber auch konkrete Vorschläge geben, die praktisch umgesetzt werden können, schränken sie insbesondere die Kreativität nicht ein, aber helfen dennoch Lösungen für die Problemstellungen zu identifizieren [25].

Durch die Evaluation mit Nutzern wurde ein Einblick in die Praxistauglichkeit der Lösungen gewonnen und die Lösungsansätze konnten auf ihre Usability und User Experience beleuchtet werden. Dabei kam insbesondere heraus, dass die Möglichkeit eines pseudonymen Profils positiv angenommen wurde. Ergänzend zu der Evaluation des Systems mit Nutzern, hat die durchgeführte Simulationsstudie die Erkenntnis erbracht, dass ein smarter Lernassistent durch die Verwendung der interdisziplinären Anforderungs- und Entwurfsmuster dazu führte, dass das System von Rechtsexperten als rechtmäßig bewertet wurde. In der mündlichen Verhandlung wird vorwiegend auf Basis des in der Entwicklung verwendeten Musterkatalogs debattiert. Die Anforderungs- und Entwurfsmuster geben der Richterin und den beteiligten Anwälten eine Möglichkeit, den Systementwicklungsprozess nachzuvollziehen, ohne dabei Vorwissen aus der Systementwicklung zu besitzen. Diese Ergebnisse zeigen das Potenzial für die interdisziplinäre Systementwicklung und Ansätze, wie die Zusammenarbeit durch Anforderungs- und Entwurfsmuster unterstützt werden kann.

7 Limitierungen und weitere Forschung

Um Entwickler bei der Gestaltung eines rechtsverträglichen Lernassistenten zu unterstützen, wird ein Musterkatalog bestehend aus Anforderungs- und Entwurfsmuster eingesetzt. Dies Muster vereinen die interdisziplinäre Systementwicklung in einem gemeinsamen Katalog und können so bei der soziotechnischen Systementwicklung unterstützen. Unsere Studie hat einige Limitierungen, die Ansätze für zukünftige Arbeiten vorgeben. In diesem Zusammenhang ist es wichtig anzumerken, dass es bei der Entwicklung des Lernassistenten kein professionelles Entwicklerteam beteiligt war, sondern Wissenschaftler mit einer technischen Ausbildung. Daher ist es wichtig, weitere Studien mit professionellen Entwicklerteams durchzuführen, um konkrete Aussagen zu der Anwendbarkeit unseres Musterkatalogs treffen zu können. Bei der Anwendung des Musterkatalogs sind wir auf einige Verbesserungsmöglichkeiten hinsichtlich der Anforderungs- wie auch Entwurfsmuster gestoßen, die in einer folgenden Überarbeitung der

Anforderungs- und Entwurfsmuster berücksichtigt werden müssen. Dabei hat sich auch herausgestellt, dass an einigen Punkten der Grad der Abstraktion der Muster überdacht werden sollte, sodass diese einen höheren Mehrwert für den Entwicklungsprozess bieten können. Hier sind entsprechend auch Fragestellungen zu adressieren, die sich mit Aspekten der kognitiven Last bei der Musternutzung befassen [26, 27].

Bei den simulierten Gerichtsprozessen sind wir ebenfalls zu wertvollen Erkenntnissen hinsichtlich der Anforderungs- und Entwurfsmuster gelangt. Wir haben festgestellt, dass sich die Muster, sofern nachvollziehbar dargelegt wird, wie sie implementiert wurden, sehr gut dafür eignen, die Vereinbarkeit mit datenschutzrechtlichen Vorgaben von Technik in Gerichtsprozessen nachzuweisen. Es handelte sich zwar nicht um echte Gerichtsprozesse, jedoch haben wir durch die Konzeption der Fälle und die Teilnahme von Richtern und Anwälten aus der Praxis sichergestellt, dass die Prozesse echten Verfahren nahekommen. Ferner wurde durch Beteiligung der Praktiker auf die Möglichkeit hingewiesen, die Anforderungs- und Entwurfsmuster auch für Datenschutzfolgenabschätzungen oder Zertifizierungsprozesse einzusetzen.

Insgesamt konnte durch unsere Studie gezeigt werden, wie Anforderungs- und Entwurfsmuster in einer interdisziplinären Systementwicklung gebündelt einen Mehrwert bringen können. Sie ermöglichen dem Systementwickler, fachfremdes Gestaltungswissen zu verstehen und in einem System umzusetzen. Wir sehen großes Potenzial für die soziotechnische Systementwicklung und einen Mehrwert für den Endnutzer, dessen Anforderungen an neuartige Produkte durch die Unterstützung von Anforderungs- und Entwurfsmuster im Entwicklungsprozess noch besser umgesetzt werden können.

8 Danksagung

Die Autoren danken den Studienteilnehmern, welche maßgeblich zur Entwicklung der hier vorgestellten Anforderungs- und Entwurfsmuster beigetragen haben. Der hier vorliegende Beitrag wurde im Rahmen des von der Deutschen Forschungsgemeinschaft (DFG) geförderten Projekts AnEkA (Projektnummer: 348084924) erarbeitet.

Literatur

1. Knote, R., Janson, A., Söllner, M., Leimeister, J.M.: Value co-creation in smart services: a functional affordances perspective on smart personal assistants. J. Assoc. Inf. Syst. (JAIS) **22**, 5 (2020)
2. Hobert, S., von Wolff, R.M.: Say Hello to Your New Automated Tutor–A Structured Literature Review on Pedagogical Conversational Agents. ICIS (2019)
3. Song, D., Oh, E.Y., Rice, M.: Interacting with a conversational agent system for educational purposes in online courses. In: 10th International Conference on Human System Interactions (HSI), pp. 78–82 (2017)
4. Hobert, S.: How are you, chatbot? Evaluating chatbots in educational settings – results of a literature review, pp. 1617–5468 (2019)
5. Knote, R., Thies, L.F., Söllner, M., Jandt, S., Leimeister, J.M., Roßnagel, A.: Rechtsverträgliche und qualitätszentrierte Gestaltung für „KI made in Germany“. Inform. Spekt. **57**, 593 (2020)
6. Leeb, C.M., Liebhaber, J.: Grundlagen des Datenschutzrechts. Jus: Juristische Schulung, 534–537 (2018)
7. Gamma, E., Helm, R., Johnson, R., Vlissides, J.: Design Patterns: Elements of Reusable Object Oriented Software. AddisonWesley Professional, Boston (1994)
8. Dickhaut, E., Thies, L.F., Janson, A.: Die Kodifizierung von Gestaltungswissen in interdisziplinären Entwurfsmustern. Lösungen im Spannungsfeld zwischen Rechtsverträglichkeit und Dienstleistungsqualität. Datenschutz und Datensicherheit (DuD) (2020)
9. Chatti, M.A., Dyckhoff, A.L., Schroeder, U., Thüs, H.: A reference model for learning analytics. Int. J. Technol. Enhanc. Learn. 318–331 (2012)
10. Pereira, J.: Leveraging chatbots to improve self-guided learning through conversational quizzes. In: Proceedings of the Fourth International Conference on Technological Ecosystems for Enhancing Multiculturality, pp. 911–918 (2016)
11. Thies, L., Knote, R., Jandt, S., Söllner, M., Roßnagel, A., Leimeister, J.M.: Anforderungs- und Entwurfsmuster als Instrumente des Privacy by Design. Springer, Wiesbaden (2018)
12. Maedche, A., Morana, S., Schacht, S., Werth, D., Krumeich, J.: Advanced user assistance systems. BISE **58**, 367–370 (2016)
13. Roßnagel, A., Friedewald, M., Hansen, M. (Hrsg.): Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung. Springer, Wiesbaden (2018)
14. Wahono, C.: On the requirements pattern of software engineering. Proceedings of the Temu Ilmiah XI (2002)
15. Pordesch, V., Roßnagel, A., Schneider, M.: Simulation Study Mobile and Secure Communication in Healthcare. DuD, 76–80 (1999)
16. Fischer-Dieskau, S., Pordesch, V., Roßnagel, A.: Simulationsstudie. In:
17. Alexander, R.: Telekooperative Rechtspflege. In Computer Und Recht: Forum für die Praxis des Rechts der Datenverarbeitung, Information und Automation Vol. 10, No. 8, pp. 498–507 (1994)
18. Roßnagel, A., Sarbinowski, H.: Simulationsstudien zur Gestaltung von Telekooperationstechnik. GMD Spiegel Nr. 2 (1993)

19. Roßnagel, A., Nebel, M.: Beweisführung mittels ersetzend gescannter Dokumente. Neue Juristische Wochenschrift: NJW, 886–891 (2014)
20. Thies, L.F., Dickhaut, E., Janson, A., Roßnagel, A., Leimeister, J.M., Söllner, M.: Die Simulationsstudie als Evaluationsmethode. Interdisziplinäre Evaluation eines smarten persönlichen Assistenten. Datenschutz und Datensicherheit (DuD) (2020)
21. Dickhaut, E., Thies, L.F., Janson, A., Roßnagel, A., Leimeister, J.M.: Towards a new methodology to capture the legal compatibility of conversational speech agents. In: Proceedings of the 2nd Conference on Conversational User Interfaces. ACM, New York, NY, USA (2020)
22. Dickhaut, E., Janson, A., Roßnagel, A., Leimeister, J.M.: Interdisziplinäre Anforderungsmuster für smarte persönliche Assistenten. Mittel zu Erfassung divergenter Anforderungen aus Informatik und Recht. Datenschutz und Datensicherheit (DuD) (2020)
23. Knote, R., Thies, L.F., Söllner, M., Jandt, S., Roßnagel, A. & Leimeister, J. M.: Rechtsverträgliche und qualitätszentrierte Gestaltung für „KI made in Germany“. Informatik Spektrum (2019)
24. Dickhaut, E., Janson, A., Leimeister, J.M.: Wie können Systeme künstlicher Intelligenz ohne Qualitätsverlust rechtsverträglich gestaltet werden? WuM (Wirtschaftsinformatik & Management) (2020)
25. Dickhaut, E., Li, M.M., Janson, A.: Developing Lawful Technologies – A Revelatory Case Study on Design Patterns. HICSS 54 (2021 in Erscheinung)
26. Dickhaut, E., Janson, A., Leimeister, J.M.: Codifying Interdisciplinary Design Knowledge through Patterns – The Case of Smart Personal Assistants. DESRIST (2020)
27. Janson, A., Söllner, M., Leimeister, J.M.: Ladders for Learning: Is Scaffolding the Key to Teaching Problem Solving in Technology-mediated Learning Contexts? AMLE (2019)

Souveräne digitalrechtliche Entscheidungsfindung hinsichtlich der Datenpreisgabe bei der Nutzung von Wearables

Arvid Butting, Niel Conradie, Jutta Croll, Manuel Fehler, Clemens Gruber, Dominik Herrmann, Alexander Mertens, Judith Michael, Verena Nitsch, Saskia Nagel, Sebastian Pütz, Bernhard Rumpe, Elisabeth Schauermann, Johannes Schöning, Carolin Stellmacher und Sabine Theis

A. Butting · J. Michael (✉) · B. Rumpe
Software Engineering, RWTH Aachen, Aachen, Deutschland
E-mail: michael@se-rwth.de

A. Butting
E-mail: butting@se-rwth.de

B. Rumpe
E-mail: rumpe@se-rwth.de

N. Conradie · S. Nagel
Angewandte Ethik, RWTH Aachen, Aachen, Deutschland
E-mail: niel.conradie@humtec.rwth-aachen.de

S. Nagel
E-mail: saskia.nagel@humtec.rwth-aachen.de

J. Croll · C. Gruber
Stiftung Digitale Chancen, Berlin, Deutschland
E-mail: jcroll@digitale-chancen.de

C. Gruber
E-mail: cgruber@digitale-chancen.de

M. Fehler
Garmin Würzburg GmbH, Würzburg, Deutschland
E-mail: manuel.fehler@garmin.com

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_24

Zusammenfassung

Wearables unterstützen ihre Nutzer:innen in unterschiedlichen Kontexten. Dabei erzeugen und nutzen sie eine Vielzahl von oft sehr persönlichen (Gesundheits-) Daten, ohne dass Nutzer:innen über die notwendigen Kenntnisse und Erfahrungen verfügen, um reflektierte Entscheidungen über die Nutzung dieser Daten treffen zu können. In der aktuellen Forschung fehlen Konzepte, die einen unreflektierten Datenaustausch vermeiden und reflektierte Entscheidungen unterstützen. In diesem Beitrag diskutieren wir gesellschaftliche Herausforderungen der digitalen Souveränität und zeigen mögliche Wege der Visualisierung persönlicher (Gesundheits-)Daten und der Interaktion mit einem System, das transparente Informationen über die Nutzung von Wearable-Daten liefert. Wir zeigen Möglichkeiten zur Visualisierung rechtlicher und datenschutzrechtlicher Informationen auf und diskutieren unsere Ideen für einen erlebbaren Datenschutz mit Gamifizierungskonzepten. Die Bereitstellung interaktiver und visueller Datenräume kann die Fähigkeit zur eigenständigen Selbstbestimmung für Datenpreisgaben stärken.

D. Herrmann
Privatsphäre und Sicherheit in Informationssystemen, Universität Bamberg, Bamberg, Deutschland
E-mail: dominik.herrmann@uni-bamberg.de

A. Mertens · V. Nitsch · S. Pütz · S. Theis
Institut für Arbeitswissenschaft, RWTH Aachen, Aachen, Deutschland
E-mail: a.mertens@iaw.rwth-aachen.de

V. Nitsch
E-mail: v.nitsch@iaw.rwth-aachen.de

S. Pütz
E-mail: s.puetz@iaw.rwth-aachen.de

S. Theis
E-mail: s.theis@iaw.rwth-aachen.de

E. Schauermann
Gesellschaft für Informatik e. V, Berlin, Deutschland
E-mail: elisabeth.schauermann@gi.de

J. Schöning · C. Stellmacher
Human-Computer Interaction, Universität Bremen, Aachen, Deutschland
E-mail: schoening@uni-bremen.de

C. Stellmacher
E-mail: cstellma@uni-bremen.de

Schlüsselwörter

Digitale Souveränität • Datenschutz • Wearables • Fitnesstracker • Gesundheitsdaten • Visualisierung • InviDas

1 Motivation

Wearables sind allgegenwärtig [6]. Mit Wearables bezeichnet man eine Gruppe von mobilen Geräten, die Nutzer:innen direkt am Körper tragen und mit einer Vielzahl von Sensoren ausgestattet sind, um sie mobil zu unterstützen [32, 43]. Wearables können eine Vielzahl von Aktivitäten ihrer Nutzer:innen und deren Gesundheitsdaten aufzeichnen. Anwendungen existieren in einem breiten Spektrum von Bereichen, z. B. Gesundheit, Lebensstil, Arbeit, Fitness [4, 28, 36, 39, 40]. Diese Arbeit betrachtet Gesundheitsdaten aus Fitnesstrackern.

Gesundheitsdaten unterliegen nach der europäischen Datenschutzgrundverordnung (DSGVO [11]) einem besonderen Schutz und werden als besonders „sensibel" wahrgenommen. Entsprechend hoch ist der Bedarf an einer verlässlichen und transparenten Grundlage für die einfache, reflektierte Entscheidungsfindung bei der Erhebung, Verarbeitung und Weitergabe von mit Wearables erhobenen Gesundheitsdaten [15, 42]. Während z. B. Endanwender:innen durch die Verwendung eines Fitnesstrackers verstehen möchten, wie viel sie sich bewegen, wie viele Kalorien sie verbrennen und wie sich dies auf ihre Gesundheit auswirkt, könnten Hersteller und Drittanbieter aus diesen sensiblen Daten Rückschlüsse auf den Gesundheitszustand der Nutzer:innen ziehen, z. B. indem sie gemessene Bewegungsdaten mit weiteren persönlichen Krankheits- und Gesundheitsdaten kombinieren. Wenn Nutzer:innen z. B. die Begleitapplikation des Fitnesstrackers auf dem Smartphone installieren, können im Hintergrund zusätzliche Daten zwischen dem Smartphone, anderen Smartphone-Anwendungen und den Herstellern des Fitnesstrackers ausgetauscht werden. Oftmals sind diese Prozesse und deren Konsequenzen für Nutzer:innen nicht ausreichend transparent.

Dieser Beitrag diskutiert Probleme, auf die Menschen bei den aktuellen Formulierungen in Datenschutzerklärungen treffen und stellt erste Konzepte zum besseren Verständnis von ihrer Datenpreisgabe vor. Darüber hinaus zeigen wir erste Ideen für die Visualisierung der (Gesundheits-)Datennutzung von Fitnesstrackern, die im Rahmen des Projekts InviDas[1] entwickelt und umgesetzt werden. Im Projekt InviDas wird von einem interdisziplinären Expert:innenteam aus Informatik

[1] Beschreibung des vom BMBF geförderten Projekts InviDas unter https://technik-zum-menschen-bringen.de/projekte/invidas.

(Software Engineering, Sicherheit und Datenschutz, Human-Computer-Interaction), Kommunikationsdesign, Psychologie, Human Factors und Ergonomie, Ethik und Recht eine digitale Plattform entwickelt. Ziel der Plattform ist es, personenbezogene Daten, die ethischen und rechtlichen Implikationen ihrer Übermittlung und deren Verarbeitung für Nutzer:innen besser verständlich zu machen.

Im folgenden Abschnitt betrachten wir das Konzept digitale Souveränität und Herausforderungen für die Gesellschaft. Abschn. 3 beschreibt aktuelle Herausforderungen beim Verständnis von Datenschutzerklärungen und zeigt alternative Konzepte auf. Abschn. 4 diskutiert mögliche Visualisierungen zur Unterstützung der digitalen Souveränität. Abschn. 5 behandelt verwandte Arbeiten. Der letzte Abschnitt bietet einen Ausblick in zukünftige Entwicklungen.

2 Digitale Souveränität – eine gesellschaftliche Herausforderung

Es ist wichtig, das Verständnis und das Vertrauen in die Datenerfassung von Wearables zu verbessern, um die Nutzer:innen in die Lage zu versetzen, auf einfache und effiziente, aber verständliche Weise informierte Entscheidungen zu treffen, um ihre digitale Souveränität aufzubauen und zu erhalten. Beginnen wir zunächst mit einer Diskussion dieses Konzepts.

2.1 Das Konzept digitale Souveränität

Reflektierte Entscheidungen, die von den Entscheidungsträger:innen auch im Nachhinein getragen werden können, erfordern nachvollziehbare Information als Entscheidungsgrundlage. Entscheidungsträger:innen, die Zusammenhänge und Funktionsmechanismen eines Systems nicht ausreichend nachvollziehen können, haben häufig keine Möglichkeit, diese Entscheidung durchdacht und selbstbestimmt zu treffen. Um eine rationale Entscheidung zu treffen, ist es wichtig, nachzuvollziehen, wie ein Sachverhalt zustande kommt [38]. Erst wenn digitale Vorgänge und Entscheidungen wahrnehmbar und nachvollziehbar sind, können Nutzer:innen verstehen, wem ihre Daten übermittelt werden, wozu welche ihrer Daten mittelbar und unmittelbar genutzt werden, und dann auch bewerten, ob sie diesen Nutzungen zustimmen möchten oder nicht.

Floridis Konzept der *digitalen Souveränität* ist das legitimer Kontrolle über das Digitale [14]. Diese Kontrolle wird als eine Art „Steuerungskontrolle“ verstanden, wie sie vom Kapitän eines Schiffes ausgeübt wird. Das Digitale geht über Daten

hinaus und umfasst Elemente wie Prozesse und Standards. Diese Konzeption ist normativ zu verstehen, da es hier um eine legitime Kontrolle geht – nicht um die tatsächliche Kontrolle über das Digitale.

Wie in Kranich et al. [21] erklärt, stellt der Begriff der digitalen Souveränität häufig einen zivilrechtlichen und volkswirtschaftlichen Bezug her, obwohl die Handlungshoheit in digitalen Lebenswelten [41] mehr als das umfasst. Verfassungsrechtliche Interpretationen ergeben sich aus dem Begriff Souveränität: Er bezeichnet „oberste Gewalt" oder „Souveränität des Staates", aber auch die „Unabhängigkeit eines Staates vom Einfluss anderer Staaten". Diese wird durch individuelle Faktoren bestimmt, die mit den rechtlichen, wirtschaftlichen und sozialen Bedingungen zusammenhängen. Mertz et al. [23] haben das Konzept der digitalen Souveränität mit den begrifflichen Komponenten Kompetenz, Informiertheit, Werte, Wahlmöglichkeit, Freiwilligkeit, Entscheidungs- und Handlungsfähigkeit beschrieben. Darüber hinaus werden technische, soziokulturelle und persönliche Determinanten identifiziert, d. h. Bedingungen und Faktoren, die empirisch untersuchen, inwieweit eine Person digital selbstbestimmt ist.

Auf individueller Ebene erfordern reflektierte Entscheidungen ausreichende Informationen als Grundlage für die Entscheidungsfindung. Entscheidungsträger:innen, die die Zusammenhänge und Funktionsmechanismen eines Systems nicht wahrnehmen und verstehen, haben keine Möglichkeit, diese Entscheidung vernünftig und selbstbestimmt zu treffen. Nur wer verstehen und reflektieren kann, wie eine Situation tatsächlich abläuft, kann rationale, begründete Entscheidungen treffen. Nur wenn digitale Prozesse und Entscheidungen wahrnehmbar und nachvollziehbar sind, wenn Anwendungen nicht nur transparent sind, sondern auch den Nutzer:innen erklärt werden, können die Nutzer:innen verstehen, welche Daten gesammelt werden und wofür ihre Daten verwendet werden. Es ist ein wesentliches Merkmal zur Förderung der digitalen Souveränität, die Nutzer:innen in die Lage zu versetzen, die Informationen über ihre Daten zu verstehen und zu verarbeiten, und zwar in einer Weise, die für sie angemessen und aussagekräftig ist. In einer digitalisierten Gesellschaft ist die *digitale Souveränität* ein *wichtiger Aspekt* der *allgemeinen Souveränität,* zu der auch die Fähigkeit zur unabhängigen Selbstbestimmung in Bezug auf die Nutzung und Gestaltung der digitalen Systeme selbst, die in ihnen erzeugten und gespeicherten Daten und die Prozesse, die sie repräsentieren, gehört [34].

2.2 Digitale Souveränität und Wearables

Dies trifft in besonderem Maße auf Informationssysteme zu, die am Körper getragen werden. Solche so genannten Wearables zeigen nicht nur Benachrichtigungen vom

Smartphone an und messen den Puls, sondern sie analysieren das Schlafverhalten, zählen Schritte, zeichnen Ort und Dauer von Trainingseinheiten auf und berechnen den Kalorienverbrauch. Ein Vermessen des persönlichen Verhaltens in seinen vielen Facetten wird möglich („Quantified Self"). Die Daten diverser Endgeräte können auf Plattformen zusammengeführt werden, um ein komplexes Profil der Nutzenden und deren Umgebung zu erstellen. Anders als bei Nachrichten und Bildern, die in sozialen Medien geteilt werden, handelt es sich bei den durch Wearables erhobenen Daten oftmals um sensible biometrische Gesundheitsdaten. Entsprechend hoch ist der Bedarf der Nutzer:innen nach einer Grundlage für die erleichterte, reflektierte Entscheidungsfindung zur Sammlung, Verarbeitung und Weitergabe ihrer Daten. Während die Endverbraucher:innen durch die Nutzung eines Fitness-Armbandes beispielsweise verstehen möchten, wie viel sie sich bewegen, wie viele Kalorien sie verbrennen und wodurch ihr Bewegungsverhalten beeinflusst wird, könnten Hersteller:innen und Drittanbieter:innen z. B. durch die Kombination der dabei gemessenen Bewegungsdaten mit personenbezogenen Krankheits-und Gesundheitsdaten Rückschlüsse auf den Gesundheitszustand der Nutzer:innen ziehen. Installieren die Endverbraucher:innen die zum Fitness-Armband passende App auf ihrem Smartphone, können die Daten unter Umständen im Hintergrund mit anderen Apps und deren Anbietern ausgetauscht werden (vgl. ein aktuelles Experiment der Washington Post[2] zur iOS-Hintergrundaktivität). Diese digitalen Prozesse, aber auch rechtliche Zusammenhänge, bleiben jedoch oft unsichtbar und damit unverstanden.

Darüber hinaus haben auch bereits Versicherungen oder Arbeitgeber Interesse an diesen Daten geäußert[3]: Workplace-Wellness Programme sollen Mitarbeiter:innen sowie ihre Familienmitglieder dazu zu ermutigen, einen gesunden Lebensstil zu führen. Andere Überlegungen betreffen die Kopplung der Krankenversicherungsbeiträge an die Fitness der Versicherten. Wer seinen Gesundheitszustand verbessert wird mit Boni belohnt.

Ein Ziel der europäischen Datenschutzgrundverordnung (DSGVO) ist es, die Interessen der Nutzenden gegenüber datengetriebenen Plattformen und Technologien zu stärken. Diese wichtige rechtliche Schnittstelle zwischen Menschen und Technologie wird derzeit meist über lange, komplizierte und textuelle Datenschutzerklärungen und -einwilligungen abgebildet. Die Texte enthalten oft fachspezifische Formulierungen, die juristischen Anforderungen genügen müssen. Die für eine informierte Einwilligung notwendigen Informationen sind schwierig zu extrahieren.

[2] https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/. Letzter Zugriff: 23.10.2020.

[3] https://futurezone.at/digital-life/versicherungen-ueberwachen-kunden-per-fitnesstracker/48.932.295. Letzter Zugriff: 23.10.2020.

Das Lesen und kritische Hinterfragen ist aufwändig und selbst bei entsprechender Bereitschaft fehlt vielen die rechtliche und technische Expertise, um die Formulierungen ausreichend nachvollziehen und deren Bedeutung für die eigenen Daten interpretieren zu können. Oft wird daher dem Nutzungsinteresse Vorrang gegeben und den Bedingungen zugestimmt, ohne dass die Inhalte verstanden wurden: Entscheidungen über die Verarbeitung sensibler persönlicher Daten durch Wearables (z. B. Aufenthaltsort, Herzfrequenz, Schlaf-und Wachzyklen) werden so oft leichtfertig getroffen, da die vorliegende Information als zu lang und schwer rezipierbar wahrgenommen und deshalb ignoriert wird. Vulnerable Anwender:innen wie sehr junge Nutzer:innen oder Menschen mit kognitiven Beeinträchtigungen können häufig keine bewusste, reflektierte Einwilligung in die Nutzung ihrer Daten geben. Ältere Nutzer:innen hingegen lehnen die Nutzung ab, weil sie nicht nachvollziehen können, wie welche personenbezogenen Daten über sie erfasst werden und welche Konsequenzen dies für sie haben kann oder übertragen die Entscheidung dafür bei der Einrichtung der Systeme jüngeren, Technik-affineren Familienmitgliedern.

2.3 Ziele des Projekts InviDas

Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekt InviDas (Interaktive, visuelle Datenräume zur souveränen, datenschutzrechtlichen Entscheidungsfindung) möchte die individuelle Souveränität im digitalen Kontext durch interaktive Datenvisualisierungen persönlicher Gesundheitsdaten und datenschutzrechtlicher Informationen fördern. Derzeit liegen keine Erkenntnisse dazu vor, auf welcher Basis die Entscheidung zur Nutzung digitaler Endgeräte für ein aktiveres und gesünderes Leben getroffen wird, welche Kompetenzen und persönlichen Eigenschaften die Voraussetzung einer bewussten und zielführenden Entscheidung sind und wer die benötigten Kompetenzen wo und in welcher Form erwirbt. Um einer Spaltung in Menschen, die das Potenzial von gesundheitsfördernden digitalen Anwendungen nutzen, und weniger digital affine Menschen, die davon nicht profitieren können entgegenzuwirken, bedarf es der partizipativen Entwicklung von Konzepten, die allen potenziell Interessierten im Hinblick auf die Nutzung von digitalen Gesundheitssystemen und Endgeräten eine kontextbewusste Entscheidung ermöglicht.

Im Spannungsfeld zwischen verweigerndem Technikpessimismus und unreflektierter Datenfreigabe gibt es Innovationsraum für eine nutzergerechte Gestaltung der Mensch-Technik Interaktion mithilfe von interaktiver Datenvisualisierungen, die Potenzial für eine gemeinwohlorientierten Technikentwicklung europäischer Prägung birgt. Es gibt bereits Ideen, Einverständniserklärungen und Datennutzungs-

erklärungen mit statischen Icons zu bebildern[4], um diese besser verständlich zu machen. Das Projekt InviDas geht einen Schritt weiter und erforscht interaktive und visuelle Datenräume, um Einverständniserklärungen und Datennutzungserklärungen verständlich und erlebbar zu machen. Interaktive Visualisierungen sind in der Lage, komplexe Zusammenhänge durch grafische Darstellungen der gesammelten Daten abzubilden. Bisher nicht sichtbare Zusammenhänge werden dadurch nachvollziehbar. Im konkreten Anwendungsfall der Wearables soll unter Zuhilfenahme verschiedener nutzerzentrierter Datenvisualisierungen auf einen Blick dargestellt werden, wie umfangreich ein Datenprofil der Tragenden ist, welche Rückschlüsse beispielsweise auf Krankheiten gezogen werden können und welche Akteurinnen und Akteure auf welche Daten zugreifen können. Bisher existieren solche Nutzerprofil-Repräsentationen nur in nüchterner Textform, was die Verständlichkeit einschränkt und Interaktionsmöglichkeiten begrenzt. Rechtliche Informationen und Folgenabschätzung sind hierbei bisher noch nicht realisiert worden. Dazu werden innerhalb des Projektes rechtliche und ethische Parameter definiert und für die Nutzenden abgebildet, um ihnen eine bessere Entscheidungsgrundlage für souveränes digitales Handeln zu geben.

Das InviDas-Projekt entwickelt eine digitale Plattform, über die personenbezogene Daten sowie die datenschutzrechtlichen Implikationen ihrer Weitergabe und Verarbeitung verständlicher gestaltet werden. Menschen unterschiedlicher Technikgenerationen und Altersgruppen soll geholfen werden, abstrakte technische und rechtliche Zusammenhänge zu verstehen und folglich bewusste und reflektierte Entscheidungen zu treffen. Visuelles, interaktives Erleben der bisher unsichtbaren digitalen Prozesse soll das Technikverständnis, -vertrauen und die Souveränität digitalrechtlicher Entscheidungsfindungen verbessern. Dies wird durch einen visuellen spielerischen Zugang erreicht, der auf Nutzer:innenbedarfen basiert. Die Erkenntnisse und Instrumente aus InviDas sollen einer breiten Öffentlichkeit zur Verfügung stehen, den gesellschaftlichen Diskurs über digitale Souveränität bei Gesundheitsdaten voranbringen und mit Hinblick auf Übertragbarkeit und Generalisierbarkeit gesamtgesellschaftlich verwertet werden.

Zusammengefasst konzentriert sich das Projekt InviDas somit auf drei Ziele:

Z1) die Erforschung geeigneter Mechanismen zur Verbesserung der Übersicht über bzw. der Kontrolle über die Weitergabe der eigenen Daten bei der Nutzung von Wearables,

[4] https://netzpolitik.org/2007/iconset-fuer-datenschutzerklaerungen/. Letzter Zugriff: 23.10.2020.

Z2) das Entwickeln von Lösungen zum besseren Verständnis für und den Vergleich von Datenschutzerklärungen sowie
Z3) Lösungen zum Aufbau von digitaler Kompetenz zur Ermöglichung von reflektierten Nutzungsentscheidungen.

3 Analyse bestehender Datenschutzerklärungen

Um ein besseres Verständnis über die aktuelle Darstellung der Datenschutzerkärungen zu bekommen, haben wir für Deutschland geltende Datenschutzerklärungen namhafter Hersteller der meist verkauften Wearables (in alphabetischer Reihenfolge: Apple, FitBit, Fossil, Garmin, Huawei Samsung und Xiaomi) analysiert und hinsichtlich der enthaltenen Datenschutzkonzepte untersucht. Diese Analyse spiegelt jedoch nicht die Gesamtheit der Datenverarbeitung wider, weil Nutzer:innen während der Verwendung der Wearables der Verarbeitung weiterer Daten einwilligen können. Dies kann zum Beispiel geführt durch die Benutzerschnittstelle in der Menüführung oder durch die Anbindung an Drittanbieter-Software oder eine Companion App geschehen. Solche Entscheidungen sind nicht notwendigerweise Teil der Datenschutzerklärung.

Datenschutzerklärungen geben Auskunft über die *Datenart* der verarbeiteten Daten. Diese ist allerdings häufig nur exemplarisch angegeben und variiert in der Abstraktion. So werden Aussagen etwa teils im Bezug auf personenbezogene Daten getroffen und teils deutlich konkreter, zum Beispiel über das Geburtsdatum. Eine geeignete Darstellung und Kategorisierung der verschiedenen Datenarten stellt eine Herausforderung für das InviDas Projekt dar.

Die *Datenverarbeitungsform* bestimmt, was mit den erfassten Daten geschieht (siehe DSGVO Artikel 4(2)). Häufig erwähnte Formen der Datenverarbeitung in Datenschutzerklärungen beinhalten das Erheben, Verändern, Speichern, Weitergeben, und Löschen von Daten.

Die meisten Aussagen innerhalb von Datenschutzerklärungen werden über Daten getroffen, deren *„Dateneigentümer“* (wir verwenden der Verständlichkeit halber diesen Begriff wenngleich es ihn im juristischen Sinn nicht gibt) die jeweiligen Nutzer:innen sind. In einigen Ausnahmen werden aber auch Aussagen über Daten von dritten Personen, wie etwa durch freigegebene Kontakte getroffen.

Daten können aus verschiedenen *Datenquellen* erfasst werden. So kann etwa die manuelle Dateneingabe, die z. B. häufig für die Erfassung von Alter und Geschlecht verwendet wird, von der automatischen Erfassung von Daten über Sensoren (z. B. Position via GPS) unterschieden werden. Weiterhin gibt es Daten, die aus anderen (Roh-)Daten abgeleitet werden.

Der *Datenempfänger* ist meist das Unternehmen, welches Hersteller des Wearables ist oder wird als „Drittanbieter" angegeben. In einigen Fällen, zum Beispiel bei der Realisierung von Coaching Services, können auch andere Nutzer:innen bzw. andere Rollen von Nutzer:innen Datenempfänger sein.

Der *Verarbeitungszweck* begründet, warum Daten verarbeitet werden. Das „berechtigte Interesse" stellt hierbei die Rechtsgrundlage für die Datenverarbeitung Sinne der DSGVO dar. Ausprägungen hiervon sind etwa die Notwendigkeit zur Erbringung einer Dienstleistung oder zur Realisierung einer Funktion. Daten können aber auch z. B. für Marktforschung, dem Erstellen von Nutzerprofilen, oder zur Einhaltung von gesetzlichen Vorschriften verarbeitet werden.

In manchen Fällen gibt es eine *Nutzungsentscheidung,* die Nutzer:innen über die Verarbeitung der Daten treffen können. Wenn es eine Entscheidung gibt, basiert diese meist entweder auf dem Opt-In oder Opt-Out Prinzip. Opt-In ist zum Beispiel eine Funktion oder ein Dienst, der von Nutzer:innen aktiviert werden kann und durch den dann Daten verarbeitet werden. Dementgegen steht das Opt-Out für das Widerrufen einer Einerständniserklärung der Datenverarbeitung durch Nutzer, zum Beispiel durch das Deaktivieren einer Funktion oder das Abmelden aus Emailverteilern.

Datenschutzerklärungen enthalten unterschiedliche Aussagen zu den *Datenschutzmaßnahmen,* die das Unternehmen trifft. Zum Beispiel versprechen einige Anbieter, dass physische und technische Schutzmaßnahmen getroffen wurden, dass Daten verschlüsselt übertragen werden, oder dass Daten auf Servern innerhalb der EU gespeichert werden.

Die *Datenaufbewahrungsdauer,* sofern sie angegeben ist, bestimmt die Länge des Zeitraums zwischen Datenerfassung und -löschung. Häufig wird erwähnt, dass Daten nur so lange aufbewahrt werden, wie es für die Erfüllung von gesetzlichen Vorgaben erforderlich ist. In manchen Fällen werden Daten allerdings auch aufbewahrt, bis Nutzer:innen ihren Account explizit löschen.

Als *Rechtsgrundlage* für die Verarbeitung von Daten werden Buchstaben aus Artikel 6(1) der DSGVO herangezogen.

Insgesamt sind die Aussagen über die Datenverarbeitung in Datenschutzerklärungen häufig generell formuliert und beinhalten selten Zusammenhänge zwischen oben genannten Kategorien. So ist im Allgemeinen etwa nicht nachvollziehbar, für welche verschiedenen Zwecke jede Art von erhobenen Daten (z. B. Herzfrequenz) verwendet werden, an wen sie weitergegeben werden können, und wo sie verarbeitet werden. Zudem ist im Allgemeinen nicht nachvollziehbar, ob für eine konkrete Datenart z. B. die auf einem Fitness Armband ermittelte Herzfrequenz lokal auf dem Armband gespeichert, zu einem Mobiltelefon übertragen, oder auf einem Server hinterlegt wird. Somit ist aktuell in Datenschutzerklärungen nicht gut nachvollziehbar,

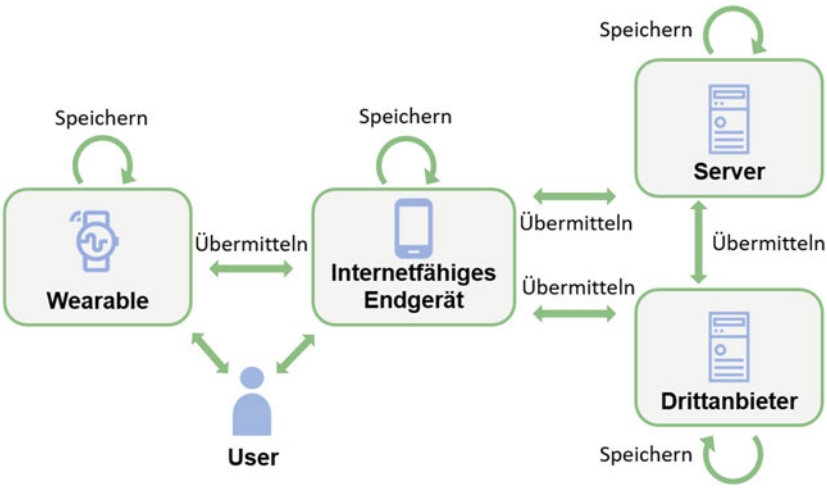


Abb. 1 Typische Konstellation von Datenverarbeitungsorten für Wearable-Anwendungen

welche Daten an welche beteiligten Orten, wie in Abb. 1 dargestellt, verarbeitet werden. Dies sind jedoch Informationen, die sich Nutzer:innen erwarten würden.

4 Be- und ergreifbarer Datenschutz

Aktuelle und zukünftige Nutzer:innen von Wearables können durch die in InviDas entwickelte Plattform mit unterschiedlichen Hilfestellungen bei der Entscheidungsfindung unterstützt werden: Übersichtliche Darstellungen von gesammelten Fitnessdaten ermöglichen den Vergleich unterschiedlicher Anbieter, textuelle Datenschutzrichtlinien werden zu einem interaktiven, visuellen Raum umgewandelt um sie verständlich zu machen und Auswirkungen von Datenschutzpräferenzen werden in einem virtuellen „Escape Room"-Spiel erlebbar.

Zunächst erhalten die Nutzer in der Komponente *myDataCockpit* (Ziel Z1) einen Überblick über die von Wearables gesammelten Daten. In diesem Zusammenhang verwenden wir einen modell-basierten Software-Engineering-Ansatz mit Code-Generierung [16], um die Plattform zu schaffen. Die Plattform wird sowohl personenbezogene Daten, Kontextinformationen [25] als auch datenschutzrechtliche Metadaten verarbeiten und sich insbesondere auf die Frage konzentrieren, welche Daten mit wem und zu welchem Zweck ausgetauscht werden [24]. So soll den

Nutzer:innen auch ermöglicht werden rückwirkend den Weg nachzuvollziehen, den ihre Daten im Verlauf der Verarbeitung durch andere Parteien genommen haben. Zu diesem Zweck wird ein geeignetes Metamodell erstellt und für die Generierung der Plattform verwendet, das aus einem Backend mit Datenspeicherung, einem Anwendungskern, einer Sicherheitsinfrastruktur und einem modernen visuellen Frontend besteht. Aufgrund des modell-basierten Entwicklungsansatzes können iterativ neue Daten und Metadaten eingebunden werden.

myDataCockpit kann entweder mit persönlichen Daten, die über ein Wearable gesammelt wurden, oder mit vordefinierten Daten von beispielhaften Nutzer:innen verwendet werden. Diese beispielhaften Nutzer sollten verschiedene Nutzer:innengruppen repräsentieren, z. B. ältere Menschen, die das Wearable zur Verfolgung ihrer täglichen Schritte verwenden, oder Marathonläufer, die sich auf einen Wettkampf vorbereiten. Welche Nutzer:innengruppen von Relevanz sind, bedarf weiterer Untersuchungen. Eine erste Grundlage bieten hierbei die Nutzer:innengruppen des D21-Index [1].

Abb. 2 zeigt eine mögliche Visualisierung von Datenverarbeitungsorten. Wählt man einen bestimmten Datensatz aus, wie z. B. die Herzfrequenz, so erhält man Informationen über (1) die Sensorik zur Erfassung, (2) die Speicherung und Verarbeitung in den unterschiedlichen Komponenten (Fitnesstracker, zugehörige lokale Fitness-App am Smartphone, Server des Anbieters, Drittanwendungen) oder (3) die simulierten Datenübermittlungen zwischen den Komponenten. Zur leichteren Vergleichbarkeit von unterschiedlichen Anbietern könnten deren Datenverarbeitungsorte auch gegenübergestellt werden.

myDataSim ermöglicht es den Nutzern, die Konsequenzen für die Akzeptanz von Datenschutzrichtlinien verschiedener Anbieter (Ziel Z2 und Z3) anhand von Visualisierungen verschiedener Datenschutzrichtlinien sowie von Gamifizierungskonzepten zu verstehen. Textuelle Datenschutzrichtlinien werden zu einem interaktiven, visuellen Raum, in dem das eigene Datenprofil in ein sich veränderndes physisches Objekt transformiert wird. Diese Räume werden speziell an die verschiedenen Nutzer:innengruppen angepasst, z. B. jüngere oder ältere, erfahrene oder unerfahrene, skeptische, gelegentliche oder leidenschaftliche Nutzer:innen.

Ein virtuelles „Escape-Room“-Spiel ermöglicht es den Nutzer:innen die Auswirkungen von Entscheidungen zu erfahren, die sich auf die Verwendung ihrer Daten beziehen (Ziel Z3). Jede Entscheidung in einer Datenschutzrichtlinie ist mit einem Rätsel oder einem Satz ähnlicher Rätsel verbunden z. B. die Auswahl „Weitergabe der GPS Daten“ mit einem Rätsel verbunden, das auf Basis solcher GPS Informationen raten lässt, wo eine Beispielperson wohnt bzw. wo sich die Person oft aufhält. Im „Escape-Room“ müssen mehrere Rätsel gelöst werden, um den Raum verlassen zu können - was von den Entscheidungen der Nutzer:innen in Bezug zu deren

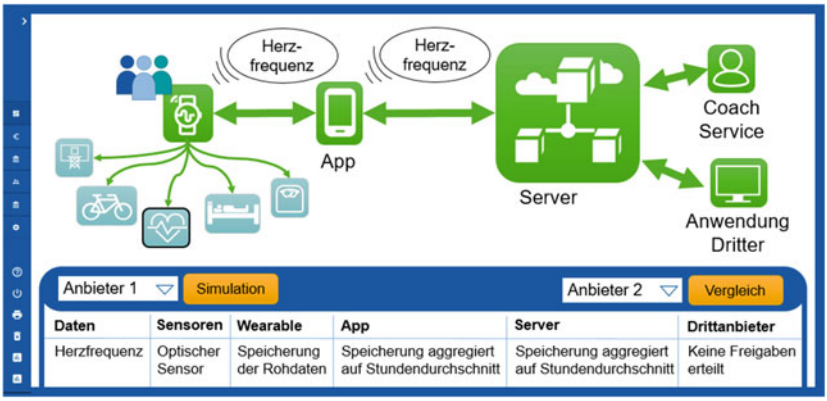


Abb. 2 Beispielhafte Anzeige: Graphische und tabellarische Darstellung von Verarbeitungsorten, Sensoren und Vergleich von Anbietern

Daten abhängt. Alle getroffenen Entscheidungen werden auf einer Skala bewertet. Diese Skala ist mit einer anderen „Welt“ verbunden, in der die Nutzer:innen den „Escape-Room“ verlassen können. Unterschiedliche Entscheidungen über die gemeinsame Nutzung tragbarer Daten wirken sich also auf die Welt aus, in die die Nutzer:innen den „Escape-Room“ verlassen. Abb. 3 zeigt diese Grundidee für das virtuelle „Escape-Room“-Spiel. Durch diese Form der Gamifizierung [19] können die Nutzer:innen trainieren, wie sie die Auswirkungen auf ihre Daten beeinflussen, z. B. wie sie sie vor Manipulation schützen können, und so auf spielerische Weise ihre digitale Souveränität entwickeln und verbessern können.

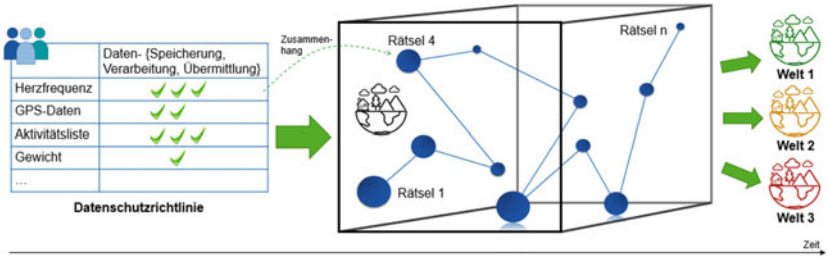


Abb. 3 Konzept des Escape-Room Spiels

myDataCockpit und myDataSim können unabhängig voneinander eingesetzt werden und ermöglichen (a) den Vergleich verschiedener Produkte hinsichtlich ihrer Datenschutzrichtlinien für InteressentInnen und (b) das bessere Verständnis für Datenschutzerklärungen an Hand eigener Daten. Wir gehen davon aus, dass eine adäquate Vergleichsmöglichkeit eine wichtige Voraussetzung darstellt, um langfristig einen Wettbewerb um datenschutzfreundlichere Produkte zwischen den Herstellern von Wearables voran zu treiben.

5 Verwandte Arbeiten zur Visualisierung der individuellen digitalen Souveränität

Im Prinzip können sich die Nutzer:innen digitaler Dienste und Technologien derzeit über Datenschutzerklärungen informieren, um zu verstehen, was mit den Daten geschehen ist. In der Praxis kommt das jedoch nicht sehr oft vor. In der Regel akzeptieren die Nutzer:innen ihre Vereinbarungen, ohne sie durchzulesen [12, 29]. Eine geeignete Visualisierung und strukturierte Präsentation kann ein Schlüsselfaktor zur Verbesserung dieser sein [3, 30]. Daher erörtern wir in diesem Abschnitt verwandte Arbeiten zur Visualisierung von Rechtsinformationen sowie zur Visualisierung von Datenschutzmaßnahmen im Allgemeinen. Daran schließt sich eine Skizze von Ideen an, die im Rahmen des InviDas-Projekts entwickelt wurden, wie neuartige und greifbare Wege zur Visualisierung der Nutzung von (Gesundheits-)Daten, insbesondere von Wearables, geschaffen werden können.

5.1 Visualisierung von Rechtlichen Informationen

Im Bereich des Rechts und der Rechtsprechung [3] sind textliche Informationsdarstellungen vorherrschend. Rechtsvisualisierungen und bildliche Darstellungen von Rechtsinformationen sollen, da sie oft mühsam zu verstehen sind, die Kommunikation zwischen Fachleuten und Laien verbessern, um Kommunikationsfehler zu vermeiden [30]. Obwohl es kein allgemeines Modell für die Visualisierung von Rechtsdaten gibt, machen bildliche Darstellungen von Rechtsinformationen bestimmte rechtliche Aspekte besser verständlich. Mögliche Rechtsbegriffe, die mit Hilfe von Visualisierungen veranschaulicht werden können, sind z. B. Gerichtsverfahren, Rechtsquellen und Rechtsnormen oder juristische Personen wie Kaufverträge [9, 22, 37]. Typische Visualisierungstypen, die in diesem Zusammenhang verwendet werden, sind Flussdiagramme, Prozessmodelle, Comics und Metamodelle [17, 31]. Wichtige Kriterien, die berücksichtigt werden müssen, sind u. a.

die logische Abfolge von Rechtsprozessen, die Einhaltung der Rechtsordnung, die Angemessenheit, die Erkennbarkeit sowie die Verbindung zwischen Text und Bild [37]. Insbesondere letzteres ist von zentraler Bedeutung, da juristische Visualisierungen in der Regel in hybrider Form auftreten, d. h. Text und Bild erscheinen kombiniert, um die Wirksamkeit der Kommunikation zu erhöhen [3]. Ein iterativer Gestaltungsprozess für eine Visualisierung in einem rechtlichen Kontext umfasst vier Aspekte: 1) die Identifizierung von Nutzerbedürfnissen durch Beobachtung und Einfühlungsvermögen; 2) eine Definition der Projektziele durch Kommunikation, Visualisierung und Prototyperstellung; 3) eine effektive Sprache durch vereinfachte Kommunikation; 4) Anpassung an Zielgruppen mit multiplen Bedürfnissen durch visuellen Diskurs und Unterstützung rechtlicher Funktionen durch einen optimalen Mix aus Sprache und Grafik [3, 31]. Lettieri et al. entwickelten die Webanwendung „Knowlex“ zur Visualisierung von Recherchen und zur Analyse juristischer Dokumente aus verschiedenen Quellen [22]. Die Ergebnisse der Studie ($n = 13$) zeigten, dass die auf einem grafischen Ansatz basierende Unterstützung die Nutzer:innen in die Lage versetzt, ihre Aufgaben schneller und effektiver zu erledigen. Darüber hinaus waren die persönliche Einstellung und der persönliche Nutzen wichtige Faktoren, um die Akzeptanz der Software zu erhöhen. Darüber hinaus stellten Burkhardt und Nazemi in einer Studie, die auf einer juristischen Konzeptontologie [7] basierte, einen Norm-Grafik-Visualisierungsansatz vor. Durch die enge Zusammenarbeit mit Nutzer:innen sowie Rechtsexperten erhielt die Einführung des Rahmenkonzepts konstruktives Feedback und sogar positive Rückmeldungen in Bezug auf Produktivität und Nutzen. Die empirische Evaluation dieses Ansatzes bleibt jedoch eine große Herausforderung.

5.2 Visualisierung von Persönlichen Informationen

Die Visualisierung von Sicherheitsdaten spielt in vielen Bereichen der Informationssicherheit eine Rolle, wie z. B. Sicherheitsmetriken, Sicherheitsüberwachung, Erkennung von Anomalien, Forensik und Malware-Analyse. Informationswissenschaft, maschinelles Lernen und explorative Datenanalyse untersuchen auch die Visualisierung von Sicherheitsdaten [2]. Ein Teilbereich der Visualisierung von Sicherheitsdaten ist die Visualisierung von Daten im Kontext der Cybersicherheit [27], die aufgrund der steigenden Zahl von Angriffen besondere Aufmerksamkeit erfährt [27, 33]. Hier werden Daten für die Logdaten-Analyse, Port-Scans und Schwachstellenbewertung durch Visualisierungstypen wie Koordinatensysteme und Baumstrukturen [8] verständlicher. Fan et al. [13] schlagen ein Echtzeit-Netzwerksicherheitssystem vor, das unbeaufsichtigtes Lernen und Visualisierungs-

technologie kombiniert, Netzwerk-Verhaltensmuster identifiziert und ein Visualisierungsmodul zur interaktiven Modellanpassung bereitstellt. Analyst:innen können mehrere Ansichten verwenden, um Erkennungsergebnisse schnell zu bewerten und Modelle anzupassen, um die Genauigkeit zu erhöhen [13].

Darüber hinaus gibt es Ansätze für die Visualisierung von datenschutzbezogenen Daten für Nutzer:innen, die oft als Transparenzverbessernde Tools (engl. Transparency Enhancing Tools, TETs) bezeichnet werden [26]. So entwickelten Kolter et al. z. B. eine Web-Browser-Erweiterung für die Visualisierung früherer Offenlegungen persönlicher Nutzerdaten, dargestellt in graphenbasierten Ansichten [20]. Bier et al. haben ein Privacy Dashboard entwickelt, das persönliche Daten entlang von Informationsflüssen visualisiert [5]. Van Kleek et al. visualisieren das Profil einer Person auf der Grundlage der Dauer ihrer App-Nutzung als navigierbare, gestapelte Balkendiagramme und von welchen Host-Server-Standorten diese Apps betrieben werden auf einer Weltkarte [35]. Kelley et al. [18] entwickelten ein Label ähnlich der Nährwertkennzeichnung auf Lebensmitteln um Datenschutzaspekte zu vermitteln. Emami-Naeini et al. [10] verfolgen einen ähnlichen Ansatz für ein IoT-Security-und-Privacy-Label.

6 Zusammenfassung und Ausblick

Die vielfältigen Herausforderungen und Spannungsfelder, die in diesem Projekt bearbeitet werden, erfordern einen inter- oder transdisziplinären Ansatz, um die sozio-technischen Systeme und Zusammenhänge in all ihren sozialen, rechtlichen und technischen Aspekten adäquat modellieren und interpretieren zu können. Mit einem entsprechend vielfältigen Methodenrepertoire, wie es vom Konsortium vertreten und in dieser Publikation diskutiert wird, ist es möglich, die vielfältigen Wechselwirkungen und Zusammenhänge bei der Entwicklung einer digitalen Plattform zu berücksichtigen, die visuelle, interaktive Erfahrungen ermöglicht, um den Nutzer:innen das Verständnis des Datenschutzes zu erleichtern.

Die Ziele, die hier verfolgt werden, wie Nutzerzentriertheit, technische Innovation, wirtschaftliche Konnektivität, digitale Politikreflexion, kontinuierliche ethische, soziale und rechtliche Analyse, sind so vielfältig wie die dafür erforderlichen Disziplinen. So müssen nicht nur die sozialen und rechtlichen Herausforderungen angegangen werden, sondern auch die Art und Weise, wie die Visualisierung rechtlicher Informationen oder von Informationen zum Schutz der Privatsphäre technisch umgesetzt wird, bedarf weiterer Forschung, denn nur eine effiziente methodologische und werkzeuggestützte Unterstützung wird es vielen Entwicklern soziotechnischer Systeme ermöglichen, ähnliche Visualisierungen einzubauen. Die Verwen-

dung geeigneter Modelle der Visualisierungstechnik sowie der visualisierten rechtlichen oder datenschutzrechtlichen Datenstrukturen und ihrer konkreten Daten wird ein Schlüssel zur Bewältigung solcher Entwicklungsherausforderungen sein.

Vielen bisher praktizierten sozio-technischen Lösungen mangelt es an Zugänglichkeit für die komplexen Entscheidungsprozesse und die Abschätzung der Auswirkungen auf die einzelne Person und schließt damit viele Menschen davon aus, reflektierte Entscheidungen über die Nutzung und Verarbeitung ihrer persönlichen Daten treffen zu können. Die in diesem Beitrag vorgestellten ersten Ideen und Konzepte leisten einen methodischen und operationellen Beitrag zur Verringerung dieser digitalen Kluft im Kontext Wearables. Aufgrund der zunehmenden Verbreitung von tragbaren Sport- und Gesundheitstechnologien, aber auch in der Fertigung und Produktion, ist davon auszugehen, dass die Nachfrage in Zukunft steigen und immer mehr Menschen betreffen wird. Aufgrund des integrierten Ansatzes werden die Ergebnisse eine Verallgemeinerung auf andere Anwendungsbereiche ermöglichen, so dass in Zukunft auch die Nutzer:innen anderer Technologien und Dienstleistungen von mehr Transparenz und digitaler Souveränität profitieren werden. Darüber hinaus werden die technologisch-technischen Projektergebnisse in allen vertretenen Disziplinen in die wissenschaftliche Forschung einfließen und stellen dank des hohen Innovationsgrades einen wichtigen Beitrag zum Diskurs dar. Letztlich soll damit ein Weg zwischen Technologiepessimismus und reflexionsfreiem Datenaustausch eröffnet werden, der den Raum für Innovationen für benutzerfreundliches Design weiter öffnet.

Literatur

1. Wie Digital Ist Deutschland? Initiative D21 e. V (2019), https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/wie-digital-ist-deutschland
2. Balakrishnan, B., et al.: Security data visualization. SANS Institute In-foSec Reading Room (2015). https://www.sans.org/reading-room/whitepapers/metrics/security-data-visualization-36387
3. Berger-Walliser, G., Barton, T.D., Haapio, H.: From visualization to legal design: a collaborative and creative process. Am. Bus. LJ **54**, 347 (2017)
4. Bernaerts, Y., Druwé, M., Steensels, S., Vermeulen, J., Schöning, J.: The office smartwatch: development and design of a smartwatch app to digitally augment interactions in an office environment. In: Proc. 2014 companion publication on Designing interactive systems, S. 41–44 (2014)
5. Bier, C., Kühne, K., Beyerer, J.: PrivacyInsight: The Next Generation Privacy Dashboard, In: Privacy Technologies and Policy. S. 135–152. Springer Int. (2016)
6. Billinghurst, M., Starner, T.: Wearable devices: new ways to manage information. Computer **32**(1), 57–64 (1999)

7. Burkhardt, D., Nazemi, K.: Visual legal analytics-A visual approach to analyze law-conflicts of e-Services for e-Mobility and transportation domain. Procedia Comput. Sci. **149**, 515–524 (2019)
8. Conti, G.: Security data visualization: graphical techniques for network analysis. No Starch Press (2007)
9. Čyras, V., Lachmayer, F., Hoffmann, H., Weng, Y.H.: Introduction to Legal Visualization (2018)
10. Emami-Naeini, P., Agarwal, Y., Cranor, L.F., Hibshi, H.: Ask the Experts: What Should Be on an IoT Privacy and Security Label? (2020)
11. Union, European: Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR). Official J. Eur. Union **L119**, 1–88 (2016)
12. Fabian, B., Ermakova, T., Lentz, T.: Large-Scale Readability Analysis of Privacy Policies. In: Proceedings of the International Conference on Web Intelligence. S. 18–25. WI '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3106426.3106427
13. Fan, X., Li, C., Dong, X.: A real-time network security visualization system based on incremental learning (ChinaVis 2018). J. Visu. **22**(1), 215–229 (2019)
14. Floridi, L.: The Fight for Digital Sovereignty: What It Is, and Why It Matters. Especially for the EU. Philos. Technol. **33**, 369–378 (2020)
15. Gabriele, S., Chiasson, S.: Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours. In: Proc. CHI Conference on Human Factors in Computing Systems. S. 1–12. CHI '20, ACM (2020)
16. Gerasimov, Arkadii and Michael, Judith and Netz, Lukas and Rumpe, Bernhard and Varga, Simon: Continuous transition from model-driven prototype to full-size real-world enterprise information systems. In: 25th Americas Conf. on Information Systems (AMCIS 2020). Association for Information Systems (AIS) (2020)
17. Haapio, H., Plewe, D., deRooy, R.: Next generation deal design: comics and visual platforms for contracting. In: Networks. Proc. 19th Int. Legal Informatics Symposium IRIS. S. 373–380 (2016)
18. Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.W.: A „Nutrition Label" for Privacy. In: 5th Symposium on Usable Privacy and Security. SOUPS '09, ACM (2009)
19. Koivisto, J., Hamari, J.: The rise of motivational information systems: a review of gamification research. Int. J. Inf. Manage. **45**, 191–210 (2019)
20. Kolter, J., Netter, M., Pernul, G.: Visualizing Past Personal Data Disclosures. In: Int. Conf. on Availability, Reliability and Security. S. 131–139 (2010)
21. Kranich, L., Hauth, P., Pols, A.: Kompetenzen einer Digitalen Souveränität (11022020), https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/kompetenzen-fuer-eine-digitale-souveraenitaet.html, Studie im Auftrag des BMWi
22. Lettieri, N., Altamura, A., Malandrino, D.: The legal macroscope: Experimenting with visual legal analytics. Inf. Vis. **16**(4), 332–345 (2017)
23. Mertz, M., Jannes, M., Schlomann, A., Manderscheid, E., Rietz, C., Woopen, C.: Digitale Selbstbestimmung (2016). https://kups.ub.uni-koeln.de/6891, Technical Report
24. Michael, J., Netz, L., Rumpe, B., Varga, S.: Towards Privacy-Preserving IoT Systems Using Model Driven Engineering. In: Ferry, N., Cicchetti, A., Ciccozzi, F., Solberg, A.,

Wimmer, M., Wortmann, A. (Hrsg.) Proc. of MODELS 2019. Workshop MDE4IoT. S. 595–614. CEUR Workshop Proceedings (2019)
25. Michael, J., Steinberger, C.: Context Modeling for Active Assistance. In: Cabanillas, C., España, S., Farshidi, S. (Hrsg.) ER Forum and Demo Track 2017 co-located with the 36th Int. Conf. on Conceptual Modelling (ER 2017). S. 221–234 (2017)
26. Murmann, P., Fischer-Hübner, S.: Tools for Achieving Usable Ex Post Transparency: A Survey. IEEE Access **5**, 22965–22991 (2017)
27. Nadeem, S.F., Huang, C.Y.: Data Visualization in Cybersecurity. In: Int. Conf. on Computational Science and Comp. Intelligence (CSCI). S. 48–52. IEEE (2018)
28. Päßler, S., Wolff, M., Fischer, W.J.: Food Intake Recognition Conception for Wearable Devices. In: Proc. 1st ACM MobiHoc Workshop on Pervasive Wireless Healthcare. MobileHealth '11, ACM (2011)
29. Proctor, R.W., Ali, M.A., Vu, K.P.L.: Examining usability of web privacy policies. Intl. J. Hum.-Comput. Interact. **24**(3), 307–328 (2008)
30. Schoormann, T., Hofer, J., Behrens, D., Knackstedt, R.: Rechtsvisualisierung in 20 Jahren IRIS–Eine multimethodische Literaturanalyse. In: Internationales Rechtsinformatik Symposium (IRIS). Bd. 20 (2017)
31. Schoormann, T., Knackstedt, R., Haapio, H.: Modeling and Visualization in Law: Past, Present and Future. In: Int. Rechtsinformatik Symposium IRIS (2017)
32. Seneviratne, S., Hu, Y., Nguyen, T., Lan, G., Khalifa, S., Thilakarathna, K., Hassan, M., Seneviratne, A.: A survey of wearable devices and challenges. IEEE Commun. Surv. Tutorials **19**(4), 2573–2620 (2017)
33. Sethi, A., Wills, G.: Expert-interviews led analysis of EEVi—A model for effective visualization in cyber-security. In: IEEE Symposium on Visualization for Cyber Security (VizSec 17). S. 1–8. IEEE (2017)
34. Stubbe, J., Schaat, S., Ehrenberg-Silies, S.: Digital souverän? Kompetenzen für ein selbstbestimmtes Leben im Alter, Bertelsmann Stiftung (2019)
35. Van Kleek, M., Binns, R., Zhao, J., Slack, A., Lee, S., Ottewell, D., Shadbolt, N.: X-Ray Refine: Supporting the Exploration and Refinement of Information Exposure Resulting from Smartphone Apps. In: Proc. CHI Conference on Human Factors in Computing Systems. S. 1–13. CHI '18, ACM (2018)
36. Vermeulen, J., MacDonald, L., Schöning, J., Beale, R., Carpendale, S.: Heartefacts: augmenting mobile video sharing using wrist-worn heart rate sensors. In: Proc. ACM Conf. on Designing Interactive Systems. S. 712–723 (2016)
37. Walser Kessel, C., Lachmayer, F., Čyras, V., Parycek, P., Weng, Y.H.: Rechtsvisualisierung als Vernetzung von Sprache und Bild – Anmerkungen zum Buch „Kennst Du das Recht?". In: Proc. of the 19th International Legal Informatics Symposium IRIS. S. 365–371 (2016)
38. Weis, R., Lucks, S., Grassmuck, V.: Technologien für und wider Digitale Souveränität. Studien und Gutachten im Auftrag des Sachverständigenrat für Verbraucherfragen (SVRV) (2016)
39. Wenig, D., Schöning, J., Hecht, B., Malaka, R.: Stripemaps: Improving map-based pedestrian navigation for smartwatches. In: Int. Conf. on Human-Computer Interaction with Mobile Devices and Services. S. 52–62 (2015)

40. Williams, L., Hayes, G.R., Guo, Y., Rahmani, A., Dutt, N.: HCI and MHealth Wearable Tech: A Multidisciplinary Research Challenge. In: Ext. Abstracts - CHI Conf. on Human Factors in Computing Systems. S. 1–7. CHI EA '20, ACM (2020)
41. Wittpahl, V.: Digitale Souveränität: Bürger. Unternehmen. Staat. Springer Vieweg, Berlin (2017)
42. Yan, T., Lu, Y., Zhang, N.: Privacy Disclosure from Wearable Devices. In: Workshop on Privacy-Aware Mobile Computing. S. 13–18. PAMCO '15, ACM (2015)
43. Yang, H., Yu, J., Zo, H., Choi, M.: User acceptance of wearable devices: an extended perspective of perceived value. Telematics and Inform. **33**(2), (2016)