Friedewald | Roßnagel | Geminn | Karaboga [Hrsg.]

Freiheit in digitalen Infrastrukturen

Nomos

Privatheit und Selbstbestimmung in der digitalen Welt

Privacy and Self-Determination in the Digital World

herausgegeben von | edited by
Dr. Michael Friedewald
Prof. Dr. Alexander Roßnagel

Band | Volume 5

Michael Friedewald | Alexander Roßnagel
Christian L. Geminn | Murat Karaboga [Hrsg.]

Freiheit in digitalen Infrastrukturen

Nomos

Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

Gestaltung Titelmotiv: Magdalena Vollmer

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

1. Auflage 2025

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-7560-3000-2
ISBN (ePDF): 978-3-7489-5337-1

DOI: https://doi.org/10.5771/9783748953371

Onlineversion
Nomos eLibrary

Vorwort

In der modernen Welt sind digitale Infrastrukturen – nicht nur Netze, sondern auch Suchmaschinen, soziale Medien und andere digitale Angebote – von entscheidender Bedeutung für die Ausübung von Freiheit. Unternehmen wie Alphabet, Apple, Meta, Amazon und Microsoft bieten Plattformen, die derzeit als Grundlagen für die digitale Freiheitsausübung dienen. Aber auch Anbieter traditioneller Infrastrukturen und der Staat bauen digitale Systeme auf, die Machtgefüge und Freiheitsräume verändern. Was bedeutet Freiheit in der digitalen Welt, wie wird sie sie geschützt oder eingeschränkt und welche Rolle spielen dabei die digitalen Infrastrukturen?

Um sich diesen Herausforderungen im Rahmen eines über die Wissenschaft hinausweisenden Diskurses zu stellen, veranstaltete die vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) geförderte „Plattform Privatheit" am 17. und 18. Oktober 2024 in Berlin die Konferenz „Freiheit in digitalen Infrastrukturen". Der vorliegende Band stellt die wichtigsten Vorträge vor und reflektiert die dort angestoßenen Diskussionen.

Die Plattform Privatheit vernetzt interdisziplinäre wissenschaftliche Projekte, die vom BMFTR im Rahmen der Förderlinie „Plattform Privatheit – Bürgerinnen und Bürger bei der Wahrnehmung des Grundrechts auf informationelle Selbstbestimmung unterstützen" gefördert werden. Diese Projekte werden vom Fraunhofer-Institut für System- und Innovationsforschung (ISI) in Karlsruhe und der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel wissenschaftlich koordiniert und kommunikativ begleitet. Die Plattform Privatheit versteht sich als ein Forum für den fachlichen Austausch und erarbeitet Orientierungswissen für den öffentlichen Diskurs in Form wissenschaftlicher Publikationen, Tagungen, White- und Policy-Paper. Ziel ist es, allen Bürger:innen einen reflektierten und selbstbestimmten Umgang mit ihren Daten, technischen Geräten und digitalen Anwendungen zu ermöglichen. Sie bereitet aktuelle Forschungsergebnisse für Zivilgesellschaft, Politik, Wissenschaft und Wirtschaft auf und berät deren Akteur:innen zu sozialen, rechtlichen und ethischen Aspekten von Privatheit, Datenschutz und informationeller Selbstbestimmung.

Die Plattform Privatheit ist 2021 aus dem „Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt" hervorgegangen. Das „Forum Privat-

heit“ arbeitete seit 2013, mit Förderung des BMBF und ausgehend von technischen, juristischen, ökonomischen sowie geistes- und gesellschaftswissenschaftlichen Ansätzen, an einem interdisziplinär fundierten, zeitgemäßen Verständnis von Privatheit und Selbstbestimmung. Hieran anknüpfend hat es Konzepte zur (Neu-) Bestimmung und Gewährleistung informationeller Selbstbestimmung und des Privaten in der digitalen Welt erstellt und öffentlich kommuniziert. Die Plattform Privatheit führt diese Arbeiten auf breiterer Basis mit mehr Projekten fort. In dieser Tradition hat sie auch die Konferenz „Freiheit in digitalen Infrastrukturen“ durchgeführt.

Als Herausgeber freuen wir uns, nun diesen Konferenzband präsentieren zu können. Wir danken insbesondere den Autor:innen für die Überarbeitung ihrer Vorträge und die Beisteuerung der jeweiligen Fachaufsätze. Ebenso zum Dank verpflichtet sind wir dem wissenschaftlichen Beirat der „Plattform Privatheit“ sowie Kolleg:innen, die die in diesem Band veröffentlichten Texte begutachtet haben. Die Konferenz wäre ohne die vielfältige Unterstützung durch das interdisziplinäre Kollegium nicht möglich gewesen. Wir danken insbesondere all jenen, die organisatorisch oder inhaltlich an der Vorbereitung und Durchführung der Konferenz mitgewirkt haben, darunter vor allem Susanne Ruhm, Greta Runge, Dr. Frederik Metzger, Sabine Muhr, Yuwen Zhang, Marvin Dobke und Gvantsa Zakariadze (Fraunhofer ISI). Darüber hinaus danken wir besonders Barbara Ferrarese (Fraunhofer ISI) für die professionelle und engagierte Wissenschaftskommunikation und Hendrik Kafsack (F.A.Z.) für die lebendige Moderation. Für die angenehme und zielführende Zusammenarbeit mit dem Nomos-Verlag danken wir Dr. Sandra Frey.

Unser besonderer Dank gilt Dr. Heike Prasse und Dr. Steffen Lohmann (BMFTR) für die Förderung der Plattform Privatheit sowie die engagierte Unterstützung unserer Forschungsthemen. Auch danken wir Florian Till Patzer, der für den Projektträger VDI/VDE-IT die Forschungsarbeiten der Plattform Privatheit, die Vorbereitung der Konferenz und das Erscheinen des Bandes konstruktiv begleitet hat.

Die Herausgeber:innen und das Team der „Plattform Privatheit“

Karlsruhe und Kassel, im Juli 2025

Inhaltsverzeichnis

Alexander Roßnagel, Michael Friedewald, Christian L. Geminn und Murat Karaboga
Freiheit in digitalen Infrastrukturen – eine Einleitung in die Thematik 9

Ingrid Schneider
Der geopolitische Kampf um digitale Souveränität: Zur Digital-Governance der EU in der Rivalität zwischen den USA und China und der Wirkung des „Brüssel-Effekts" im Globalen Süden 19

Marit Hansen, Andreas Baur und Felix Bieker
Freiheit by Design in digitalen Infrastrukturen 53

Leopold Beer, Paul C. Johannes, Huda Koulani, Christian L. Geminn, Matthias Söllner und Stefan Voigt
Ein offener Webindex: Anwendungen, rechtlicher Rahmen, Akzeptanz 77

Luisa Schmied und Maxi Nebel
Digitale Vulnerabilität und Selbstbestimmung – Vorgaben zur Sicherstellung der Selbstbestimmung vulnerabler Nutzendenden durch informierte Einwilligung und Rechtspflichten im Behinderten- und Datenrecht 107

German Neubaum
Algorithmen-Transparenz und -Kompetenz als Säulen der informationellen Selbstbestimmung: Ein nutzerzentrierter Blick 149

Johanna Möller, Lukas Schmitz und Sebastian Rehms
Das *Privacy Fabric Model*: Ein Vorschlag für interdisziplinäre Verständigung in der Privatheitsforschung 167

Carsten Ochs, Andreas Bischof, Mario Göbel, Simon Hensellek, Delphine Reinhardt und Ina Schiering
Freiheit und Selbstbestimmung in digitalen Infrastrukturen? Zur Kontroverse um den Gemeinwohlnutzen soziodigitaler Infrastrukturen 187

Heiner Koch, Clara Strathmann, Martin Hennig, Luisa Schmied, Christian L. Geminn, Jessica Heesen, Nicole Krämer und Karoline Reinhardt
Diversitätsgerechter Privatheitsschutz in digitalen Umgebungen 223

Maximilian Lukat und Volkan Sayman
Personalisierung von Werbung – wer, was, warum und wie? Eine soziologische Perspektive darauf, wie Betroffene datenverarbeitende Organisationen personifizieren 243

Lennart Kiss, Rachelle Sellung, Björn Hanneke und Lorenz Baum
Erkenntnisse zur Verbesserung von Datenschutz in Plattformökonomien: Transparenz, Intervenierbarkeit und User Experience im Fokus 263

Tom Hubert, Felix Büning, Marwan El-Rifaai, Florian Franke, Michael Kern, Sara Elisa Kettner, Otmar Lell, Markus Meyer, Runjie Xie, Benedikt Morschheuser, Christian Thorun und Andreas Wiebe
Privacy by Design: Schutz der Privatheit im Metaverse durch Designpraktiken am Beispiel ausgewählter Gefahren für Datenschutz und Persönlichkeitsrechte 285

Mitarbeiterinnen und Mitarbeiter dieses Bandes 319

Freiheit in digitalen Infrastrukturen – eine Einleitung in die Thematik

Alexander Roßnagel, Michael Friedewald, Christian L. Geminn und Murat Karaboga

Freiheit als Abwehr von ungerechtfertigter Machtausübung und Schutz vor Machtmissbrauch ist Voraussetzung für individuelle Selbstentfaltung und kollektive Selbstbestimmung. Grundrechte und Demokratie sollen diese Freiheit gewährleisten. Sie sollen die Ausübung unter anderem von Meinungsfreiheit, Informationsfreiheit, Gewissensfreiheit, Wissenschaftsfreiheit und Wahlfreiheit ermöglichen und vor Diskriminierung schützen. Auch das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts, die Achtung des Privat- und Familienlebens und der Schutz personenbezogener Daten sind Bedingungen von Freiheit. Wie individuelle und kollektive Freiheit gelebt werden kann, ist abhängig von den gesellschaftlichen, technischen, ökonomischen und kulturellen Bedingungen, unter denen sie ausgeübt werden soll. Diese Freiheiten sind aktuell gefährdet und müssen verteidigt werden. Damit auch die Forschung ihren Beitrag zu ihrer Erhaltung leistet, hat das Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) „Freiheit" in den Mittelpunkt des Forschungsjahres 2024 gestellt.

In der modernen Welt sind für die Freiheitsausübung die gesellschaftlichen Infrastrukturen von entscheidender Bedeutung. Diese verändern sich aktuell dynamisch und damit auch die Bedingungen von Freiheit.

1. Digitale Infrastrukturen

Infrastrukturen sind netzartige sozio-technische Systeme die verlässlich einen einheitlichen Satz von Leistungen anbieten, die von Interessierten als Grundlagen des menschlichen Zusammenlebens, als Eröffnung von Handlungsmöglichkeiten und als Schutz gegenüber Lebensrisiken genutzt werden können – wie für Kommunikation, Energieversorgung, Güteraustausch, Mobilität oder Unterhaltung. Infrastrukturen sind daher Grundlagen für die Ausübung von Freiheit. Sie können aber auch durch die Abhän-

gigkeit von ihren Leistungen, durch die Machtsteigerung ihrer Anbieter und die Rigidität ihres Angebots die Freiheitsausübung einschränken oder gefährden.

Digitale Infrastrukturen sind die Basis für Digitalisierung. Sie sind Bedingungen für das Leben in der digitalen Welt. Ohne sie wären digitale Kommunikation, Informationssuche, -verbreitung und -verarbeitung, sozialer Austausch, Handel, Mobilität sowie Hardware- und Softwarenutzung nicht möglich. Vor allem die Infrastrukturnetze und -plattformen von Alphabet (Google), Apple, Meta (Facebook), Amazon und Microsoft bieten Leistungen, die derzeit Grundlagen für Freiheitsausübung in der digitalen Welt sind. Aber auch die Anbieter „alter" Infrastrukturen wie Automobilhersteller, Energieversorger, Finanzdienstleister, Gesundheitsdienstleister, Logistikunternehmen, Telekommunikationsanbieter oder Bahnbetreiber bauen digitale Infrastrukturen auf, ohne die ihre Leistungen nicht mehr genutzt werden können. Selbst der Staat errichtet neue Infrastrukturen wie Bürgerkonten, elektronische Akten, elektronische Register und elektronische Zugänge zur Verwaltung. Alle diese digitalen Infrastrukturen verändern Machtgefüge und Freiheitsspielräume.

Digitale Infrastrukturen bestimmen über den Grad der Freiheit von Individuen und Gesellschaft. Dies gilt nicht nur für ihre Betreiber. Vielmehr sind es die Infrastrukturen selbst, die durch ihre standardisierenden Effekte und ihre Plattform- und Netzwerkeffekte infrastrukturelle Macht ausüben. Da sie für ihr Funktionieren personenbezogene Daten verarbeiten müssen, können sie diese Datenverarbeitung nicht von unterschiedlichen individuellen Einwilligungen abhängig machen. Die individuelle Selbstbestimmung ist letztlich reduziert auf das grundsätzliche „Ja" oder „Nein" zum digitalen Leben. Digitale Infrastrukturen erzeugen einen eigenen virtuellen Sozialraum, in den nahezu alle Aktivitäten aus der körperlichen Welt übertragen wurden. In diesem hinterlässt jede Handlung Datenspuren, deren Erhebung und – letztlich weltweite – Verbreitung und Verwendung die betroffene Person nicht kontrollieren kann. Den damit verbundenen Risiken zu entgehen, würde voraussetzen, den virtuellen Sozialraum zu meiden – für viele keine realistische Alternative. Es besteht ein virtueller „Anschluss- und Benutzungszwang" für digitale Infrastrukturen, der oftmals auch mit dem Wegfall analoger Alternativen einhergeht.

Die großen digitalen Infrastrukturen sind global und durchdringen überall auf der Welt in intensiver Weise das digitale Leben. Ihre Marktanteile sind monopolartig und ihre Anbieter haben den mit Abstand höchsten Marktwert aller Unternehmen weltweit. Für diese ungeheure ökonomische

Macht gibt es vor allem zwei Gründe: Zum einen sind ihre Angebote für das digitale Leben hilfreich und verführerisch und zum anderen sind sie „umsonst". Die Abhängigkeit von ihnen ist hoch und nimmt weiter zu. Diese ökonomischen Erfolge erzielen sie vor allem durch die Verarbeitung der Daten ihrer Nutzenden. Mit deren Hilfe erstellen sie Personenprofile, beuten die Subjektivität der Betroffenen aus, verkaufen ihre Aufmerksamkeit, steuern ihre Informationen und beeinflussen ihr Denken. Mit ihrer Informationsmacht versuchen sie, ihr Verhalten zu beeinflussen oder gar zu steuern – bisher noch insbesondere für Konsumwahl und Kundenbindung, potenziell aber auch für andere Verhaltensformen wie z. B. Wahlentscheidungen. Politisches Micro-Targeting könnte auf der Grundlage der Personenprofile leicht zur Manipulation demokratischer Wahlen verwendet werden. Zahlreiche weitere Techniken der Verhaltensmanipulation wie z. B. Dark Patterns oder Nudging stehen zur Verfügung. Die personalisierten Dienstleistungen der Infrastrukturen werden über den gesamten Tagesverlauf hinweg in die individuellen Handlungsabläufe integriert und unmerklich Teil des Verhaltens und Handelns. Die gleichen Infrastrukturen, die Freiheit und Demokratie unterstützen können, entwickeln sich zu ihren Gefährdern.

Der ungeheure Reichtum, den die Anbieter der großen digitalen Infrastrukturen innerhalb kurzer Zeit erringen konnten, ermöglicht ihnen, ihre Macht immer weiter auszubauen. Ihnen gelang es innerhalb ihrer Infrastrukturen alle wesentlichen Bausteine zu integrieren – von Hardware über Rechenzentren, Cloud-Systemen, APIs und Software bis hin zu Plattformen, Suchmaschinen, Anwendungssystemen und Forschungszentren. Sie binden mit interessanten Projekten und konkurrenzlosen Gehältern junge Talente. Sie kaufen Start-ups und mögliche Konkurrenten auf und werden dadurch auch führend in neu entstehenden digitalen Infrastrukturen. Sie steuern damit die technologische Entwicklung, bestimmen, was sich durchsetzt, und verhindern Entwicklungen, die nicht zu ihren Interessen passen.

Die Anbieter digitaler Infrastrukturen beherrschen auch die Entwicklung der neuesten Infrastruktur: Große Sprachmodelle als Kern generativer Systeme Künstlicher Intelligenz. Sie verfügen über die erforderlichen finanziellen Ressourcen und enormen Rechenkapazitäten sowie über die notwendigen Cloud-Infrastrukturen. Durch die von ihnen betriebenen Infrastrukturen können sie auf ungeheure Datenschätze zurückgreifen, über die sie allein verfügen, und sind damit hinsichtlich ihrer KI-Trainingsmöglichkeiten konkurrenzlos. Andere Entwickler sind gezwungen, auf ihren KI-Infrastrukturen aufzusetzen und sich darauf zu beschränken, diese auf

die spezifischen Bedürfnisse bestimmter Anwendungsbereiche wie etwa Medizin, Verwaltung oder Wissenschaft anzupassen. Die Entwicklung zu Künstlicher Intelligenz verstärkt daher ihre infrastrukturelle Macht zusätzlich.

2. Normativer Rahmen

Die Europäische Union hat neue Regelungen erlassen, um Gefahren durch die globalen digitalen Infrastrukturen einzuschränken und deren Macht zu begrenzen. Vor allem das Gesetz über digitale Dienste, das Gesetz über digitale Märkte, die Verordnung über künstliche Intelligenz (KI-VO) und die Datenschutz-Grundverordnung (DSGVO) enthalten Regelungen, um die Freiheit des Individuums zu schützen, die Voraussetzungen eines funktionierenden Marktes zu erhalten und demokratisch festgelegte Regeln des Zusammenlebens durchzusetzen. Sie sollen unter anderem informationelle Selbstbestimmung gewährleisten, vor Diskriminierung schützen und menschenzentrierte Gestaltung in der Entwicklung von Künstlicher Intelligenz erreichen. Aufsichtsbehörden sollen die Einhaltung dieser Ziele sicherstellen. Sie haben daher die Befugnis, bestimmte Verhaltensweisen anzuordnen und Sanktionen in spürbarer Höhe zu verhängen.

Den Anbietern digitaler Infrastrukturen helfen jedoch spezifische Schwachstellen der Unionsgesetze. So adressiert die DSGVO nur Verantwortliche und knüpft an den einzelnen Datenverarbeitungsvorgängen an, regelt aber nicht die freiheitsbeschränkenden Wirkungen großer digitaler Infrastrukturen. Ebenso enthält die KI-VO Gestaltungsanforderungen an KI-Systeme und nimmt damit primär Künstliche Intelligenz in Form von einzelnen Produkten in den Blick. Sie adressiert jedoch die infrastrukturelle Perspektive allenfalls indirekt, beispielsweise in Bezug auf Risikobewertungen und Folgenabschätzungen. Ob die Regelungen der Europäischen Union insgesamt genügen werden, um die verfolgten Ziele zu erreichen, muss sich erst noch erweisen. Sie sind jedenfalls sinnvolle erste Schritte zur Freiheitssicherung und Machtbegrenzung.

Die Anbieter digitaler Infrastrukturen agieren jedoch weltweit. Sie ignorieren daher vielfach die demokratisch getroffenen Entscheidungen zur regionalen Regulierung von Infrastrukturen – auch in Europa oder Deutschland. Sie legen ihrem Handeln eigene Regeln zugrunde, die den europäischen oder nationalen Regelungen oft widersprechen. Sie wollen ihre eigene globale Rechtsordnung – verkleidet als Vertragsbedingungen für die

Nutzung ihrer Infrastrukturen – weltweit durchsetzen. Ihre infrastrukturelle Macht erschwert die Durchsetzung des normativen, freiheitssichernden rechtlichen Rahmens in Europa erheblich.

Diese Hindernisse werden neuerdings noch dadurch verstärkt, dass die Anbieter digitaler Infrastrukturen (wenn auch fragile) Symbiosen mit der politischen Macht in den USA eingehen. Die amtierende US-Regierung betrachtet die Anwendung von geltendem Unionsrecht als gezielte Benachteiligung von US-Anbietern und droht mit wirtschaftlichen Vergeltungsmaßnahmen.

3. Folgen für Freiheit und Selbstbestimmung

Was kann Freiheit und Selbstbestimmung unter diesen neuen und sich verändernden Bedingungen bedeuten? Jede Infrastruktur ist mit bestimmten Technologien und Praktiken verbunden und durch ihre sozio-technische infrastrukturelle Form in besonderem Maße handlungsnormierend. Infrastrukturen eröffnen oder verschließen Handlungsmöglichkeiten und steuern Wissen, Werte und Ressourcen.

Eine wichtige Forschungsfrage für die Auswirkungen von digitalen Infrastrukturen ist, wie sich die komplexen Interaktionen zwischen sozialen Systemen und technischen Infrastrukturen entwickeln. Diese Interaktionen sind entscheidend für die Gestaltung und Nutzung von Technologien, die sowohl Chancen als auch Herausforderungen mit sich bringen. Wie aber beeinflussen technologisch geprägte Praktiken unterschiedliche Werte, die Vielfalt und Ambivalenz von Privatheitsansprüchen und die divergierende individuelle Vulnerabilität verschiedener Nutzergruppen?

Die Wirkung der Datenverarbeitung in digitalen Infrastrukturen hängt auch davon ab, wie die betroffenen Personen die auf sie bezogenen Datenverarbeitungen für sich deuten und erklären. Wann empfinden sie diese Einflüsse für ihre Freiheit als positiv oder negativ? Je nach Erwartung und Empfinden können die objektiven Wirkungen dateninvasiver Technologien einen relativen Freiheitsgewinn oder eine schmerzende Freiheitsverletzung bedeuten.

Um in digitalen Infrastrukturen Freiheit und Grundrechte ausüben zu können, sind je nach Situation unterschiedliche individuelle und unternehmerische Kompetenzen und Motive sowie familiäre, wirtschaftliche, aber auch politisch-institutionelle und technische Verwirklichungsbedingungen

erforderlich. Eine wichtige Forschungsfrage ist daher, wie Selbstbestimmung und Handlungsfähigkeit von Individuen sichergestellt werden kann.

Für die Auswirkungen auf Freiheit sind auch die Strategien bedeutsam, die betroffene Personen zum Schutz ihrer Selbstbestimmung in digitalen Infrastrukturen verfolgen können. Entscheidend dafür dürfte sein, wie Regulierung, Technologie, Nutzererwartungen und Interaktivität aufeinander abgestimmt sind. Nutzerzentrierte Datenschutzinitiativen können dabei hilfreich und wirksam sein, indem sie virtuelle Belästigungen verhindern sowie die Transparenz von Datenverarbeitungsprozessen erhöhen und dadurch Entscheidungsspielräume deutlich und nutzbar machen. Hierzu erscheint es unerlässlich, die Auswirkungen der algorithmischen Informationsverarbeitung und der damit verbundenen Datenschutzfragen zu verstehen.

4. Teilhabe an Infrastrukturen

Aufgrund der selbstverantworteten Abhängigkeit wird die Nutzung der digitalen Infrastrukturen zu den Bedingungen ihrer Anbieter von vielen als Zwang erlebt. In solchen Situationen könnte die Teilhabefunktion der Grundrechte an Bedeutung gewinnen. Grundrechte bieten nicht nur Abwehrrechte gegen staatliche Einschränkungen der Freiheit oder Schutz der Freiheit gegen Übergriffe mächtiger Privater, sondern fordern auch die Teilhabe an den Voraussetzungen modernen Miteinanderlebens. Gerade mit Blick auf die globalen digitalen Infrastrukturen ist zu diskutieren, ob die Rechtsprechung des Bundesverfassungsgerichts zur Geltung der Grundrechte für übliche Infrastrukturanbieter auch auf die Anbieter der globalen digitalen Infrastrukturen anzuwenden ist.

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

Dies gilt in verstärkter Weise, wenn die Infrastrukturbetreiber durch autoritative Setzung eine eigene Rechtsordnung in Form von „Gemeinschaftsregeln" erstellen, die staatlichen Rechtsregeln, die durch demokratische Prozesse zustande kommen, Konkurrenz machen. Im Zweifelsfall müssen das staatliche Recht und erst recht die Grundrechte der EU-Grundrechtecharta und des Grundgesetzes diesen „Gemeinschaftsregeln" vorgehen. Soweit Grundrechte betroffen sind, muss die Ausgestaltung und der Betrieb der Infrastrukturen stärker an diesen als an ökonomischen Konzernzielen ausgerichtet sein.

Daher sind mit der Rechtsprechung des Bundesverfassungsgerichts die öffentliche Verantwortung von Infrastrukturbetreibern und ihre verstärkte Grundrechtsbindung auch gegenüber privaten Infrastrukturbetreibern zu betonen. Auch wenn diese sich grundsätzlich auf Berufs- und Eigentumsfreiheit berufen können, muss gelten: Je abhängiger die Gesellschaft von ihren Infrastrukturleistungen ist und je tiefgreifender ihre Leistungserbringung die Verwirklichung von Grundrechten, insbesondere der informationellen Selbstbestimmung und der gesellschaftlichen Kommunikation, beeinflusst, desto eher unterliegen sie einer bis hin zu staatsgleichen Grundrechtsbindung.

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

5. Digitale Souveränität

Aufgrund der hohen Abhängigkeit von digitalen Infrastrukturen aus den USA wird zunehmend die Forderung nach digitaler Souveränität Europas erhoben. Eine häufig angewandte Definition versteht unter digitaler Souveränität „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können". Nicht nur eine konkurrenzfähige und selbstbestimmte wirtschaftliche Entwicklung setzt mehr digitale Souveränität voraus. Vielmehr werden durch sie auch die Bedingungen, individuelle und kollektive Freiheit auszuüben und europäische Werte in der digitalen Welt durchsetzen zu können, verbessert.

Forschungsthemen betreffen die Frage, mit Hilfe welcher nationalen und internationalen Mechanismen oder Rechtsinstrumente die Europäische Union oder ihre Mitgliedstaaten versuchen sollten, das Angebot von digitalen Infrastrukturen zu regulieren. Ansatzpunkte hierzu könnten das Wettbewerbsrecht, das Datenschutzrecht, das Produktrecht, das Vergaberecht oder der Grundrechtsschutz sein.

Für das Cloud Computing sind öffentliche Verwaltungen verpflichtet, strategisch souveräne Clouds zu fordern und zu nutzen. Angesichts der Übermacht der zumeist nicht-europäischen Hyperscaler und der Abhängigkeit von ihnen wird Souveränität im Cloud Computing schon angenommen, wenn eine ausreichende Wechselmöglichkeit, Gestaltungsfähigkeit und Einflussmöglichkeiten auf die Cloudanbieter bestehen. Open Source gilt als hilfreich, aber nicht als ausreichend.

Im Hinblick auf die Informationssuche könnte ein durch die Europäische Union geförderter offener Webindex als Basis für neue, unabhängige Suchmaschinen dienen und Innovationen im Bereich der Künstlichen Intelligenz fördern und so den monopolisierten Markt diversifizieren und Pluralität fördern. Ein solcher Index bringt nicht nur technische, sondern auch rechtliche und gesellschaftliche Herausforderungen mit sich, deren Berücksichtigung für eine erfolgreiche Umsetzung entscheidend ist.

Eng mit der digitalen Souveränität gegenüber Big Tech aus den USA ist die geopolitische Position Europas zu sehen, die zwischen den konkurrierenden US-amerikanischen und chinesischen Modellen digitaler Governance verortet werden kann. Während die USA einen Laissez-faire-Ansatz verfolgen und China auf staatliche Kontrolle und Überwachung setzt, strebt die Europäische Union einen eigenständigen „Dritten Weg" mit einem umfassenden regulatorischen Rahmen an, der Menschenrechte, Demokratie und Nachhaltigkeit betont. Durch die Umsetzung der DSGVO und weiterer Digitalrechtsakte, die digitale Infrastrukturen betreffen, will die Europäische Union globale Standards setzen und ihren Einfluss mittels des „Brüssel-Effekts" ausweiten. Die entscheidende Frage hierfür wird sein, ob das europäische Modell als Referenz für digitale Souveränität in den entscheidenden Schwellenländern angesehen wird.

6. Gestaltung von digitalen Infrastrukturen

Der beste Schutz von Freiheit und Demokratie kann erreicht werden, wenn es gelingt, digitale Infrastrukturen so zu entwickeln und zu gestalten,

dass durch sie Freiheit und Selbstbestimmung gestärkt und unerwünschte Entwicklungen vermieden werden. Hierfür ist es notwendig, sich interdisziplinär mit den Gestaltungsherausforderungen und -möglichkeiten digitaler Infrastrukturen auseinanderzusetzten. Diskutiert werden müssen technische, ökonomische, soziale, politische, rechtliche, kulturelle und pädagogische Ansätze, um den Schutz der Privatsphäre und der informationellen Selbstbestimmung unter den Bedingungen digitaler Infrastrukturen weiterzuentwickeln. Dabei sind normative, institutionelle und instrumentelle Konzepte eines freiheitsfördernden Datenumgangs im Kontext digitaler Infrastrukturen zu erörtern. Welche Gestaltungsmöglichkeiten bestehen oder entwickelt werden können, ist die zentrale Frage der meisten Beiträge dieses Bandes.

Zu untersuchen ist, welche relevanten technischen Funktionen adäquate Ergänzungen zur DSGVO darstellen. So ist zum Beispiel zu fragen, inwiefern *Privacy Enhancing Technologies* (PETs) zum Instrument einer globalen Regulierung werden können. Es wäre hilfreich, wenn Wege gefunden werden könnten, wie sie einsetzbar sind, um Selbstbestimmung gegenüber digitalen Infrastrukturen zu sichern. Hierfür wäre erforderlich, geeignet die Voraussetzungen und Rahmenbedingungen für ihre Umsetzung zu finden.

In der Realität werden digitale Infrastrukturen nicht nach grundrechtlichen Erwägungen gestaltet. Vielmehr werden sie nach technischen Anforderungen konstruiert oder entsprechend ökonomischen Zielsetzungen entwickelt. Sicherheits- oder Datenschutzaspekte werden erfahrungsgemäß nachträglich und nachrangig berücksichtigt. Ein späteres Aufsatteln oder Nachrüsten von Eigenschaften oder Funktionen, die Sicherheit und Datenschutz befördern, ist jedoch nicht immer einfach und jedenfalls schwieriger und teurer, als wenn sie von Anfang an berücksichtigt werden, manchmal ist es sogar unmöglich. Wichtig sind daher Untersuchungen, wie der Prozess der Entwicklung von digitalen Infrastrukturen so verändert werden kann, dass diese Aspekte von Anfang an in die Gestaltung einfließen.

7. Transformation der rechtlichen Infrastruktur

Auch der rechtliche Rahmen als Steuerungs- und Gestaltungsmittel für Infrastrukturen ist selbst Teil einer normativen Infrastruktur. Sie wird nicht nur durch Gesetzgebung, Rechtsprechung und Aufsichtsbehörden gezielt weiterentwickelt, sondern verändert sich auch durch die milliardenfachen alltäglichen gesellschaftlichen Praktiken, die sich in der Nutzung digitaler

Infrastrukturen ungezielt ausbilden. Abstrakte Rechtsregeln, die auf praktische Fälle angewendet werden müssen, nehmen in ihrer Konkretisierung auf den praktischen Fall dessen Eigenschaften und Umstände in den Entscheidungssatz mit auf. Dadurch ändert sich allmählich die Bedeutung eines Rechtssatzes über die Zeit mit der Veränderung der gesellschaftlichen Praxis.

Dies ist zum Beispiel deutlich nachzuvollziehen in der normativen Veränderung des Verhältnisses von Sicherheit und Freiheit. Die zunehmende Abhängigkeit von digitalen Infrastrukturen und die steigende Wahrscheinlichkeit von Ausfällen, Anschlägen und Manipulationen sowie das wachsende Schadenspotenzial lassen auch Vorsorge gegen und Bekämpfung von Risiken dringender erscheinen. Solche Entwicklungen verschieben allmählich die Balance zwischen der Nutzung von Technologie zur Förderung individueller Freiheiten und dem Schutz vor Missbrauch und Verletzungen der Privatsphäre.

Sollen solche – oft unbemerkten und ungezielten – Veränderungen des rechtlichen Rahmens vermieden werden, erfordert dies immer wieder eine gezielte und bewusste Transformation der rechtlichen Infrastruktur. Diese kann nicht darin bestehen, einen relevanten Wert zu ignorieren, sondern erfordert eine rechtliche Gestaltung des technischen Entwicklungsprozesses. Zu untersuchen ist, wie effektive Regulierung gestaltet werden kann, um sowohl die Sicherheit als auch die Selbstbestimmung der Nutzer zu stärken und die gesellschaftlichen und rechtlichen Rahmenbedingungen zu verbessern. Dies gelingt nur, wenn Recht auch die Umstände der riskanten gesellschaftlichen Entwicklung in den Blick nimmt. Erforderlich ist daher, die Design- und Entwicklungsprozesse der digitalen Infrastrukturen in den Blick zu nehmen und von Anfang an freiheitsverträgliche und demokratiefördernde Gestaltung einzufordern und durch Prozessgestaltung zu ermöglichen und sicherzustellen.

Der geopolitische Kampf um digitale Souveränität: Zur Digital-Governance der EU in der Rivalität zwischen den USA und China und der Wirkung des „Brüssel-Effekts“ im Globalen Süden

Ingrid Schneider

Zusammenfassung
Dieser Beitrag analysiert die europäische Digitalpolitik im Kontext geopolitischer Spannungen, wobei der Fokus auf der Position Europas zwischen den konkurrierenden US-amerikanischen und chinesischen Modellen digitaler Governance liegt. Während die USA einen Laissez-faire-Ansatz verfolgen und China auf staatliche Kontrolle und Überwachung setzt, strebt die Europäische Union einen eigenständigen „Dritten Weg“ mit einem umfassenden regulatorischen Rahmen an, der Menschenrechte, Demokratie und Nachhaltigkeit betont. Durch die Umsetzung der Datenschutz-Grundverordnung (DSGVO) und weiterer Gesetzgebungen will die EU zugleich globale Standards setzen und ihren Einfluss mittels des „Brüssel-Effekts“ ausweiten. Die empirische Studie basiert auf einer vergleichenden Analyse und Feldforschung in den Schwellenländern Mexiko, Brasilien, Indien und Südafrika, in denen die Wirksamkeit europäischer Digitalregulierung und des Brüssel-Effekts im Datenschutz untersucht werden. Die Ergebnisse zeigen, dass Europas regulatorischer Ansatz in Schwellenländern durchaus ein Leitbild bietet und positive Impulse setzen kann, gleichzeitig aber Herausforderungen bei der Durchsetzung der Gesetze bestehen. Die Arbeit beleuchtet, ob das europäische Modell als Referenz für digitale Souveränität in einer multipolaren Welt fungieren kann und zeigt andere Einflussfaktoren auf.

1. Einleitung

Digitalpolitik wird seit einigen Jahren zunehmend unter geopolitischen Vorzeichen betrachtet. Spätestens die zweite Amtszeit von Präsident Donald Trump in den Vereinigten Staaten hat Europa die große Abhängigkeit von digitalen US-Plattform-Unternehmen vor Augen geführt und den Ruf nach technologischer Souveränität weiter gestärkt. Das digitale Zeitalter hat konkurrierende Leitbilder digitaler Governance hervorgebracht, wobei die USA und China als zentrale Akteure jeweils grundlegend unterschiedliche Prinzipien und Praktiken vertreten. Während diese beiden digitalen Supermächte um technologische Dominanz und wirtschaftliche Einflusssphären ringen, positioniert sich die Europäische Union (EU) als Akteur mit einem eigenständigen normativen Ordnungsrahmen. Dieser Beitrag untersucht insbesondere am Beispiel des Datenschutzes den Anspruch der EU, als regulatorische Supermacht aufzutreten und für digitale Governance auf

der Basis von Menschenrechten, demokratischen Werten und ethischen Prinzipien ein globales Referenzmodell zu bilden.

Die Konfrontation zwischen dem US-amerikanischen und dem chinesischen Modell digitaler Governance stellt für die EU die Frage nach ihrem eigenen Weg. Die USA befürworten traditionell einen Laissez-faire-Ansatz, bei dem Innovation und Marktfreiheit im Vordergrund stehen, während China ein staatlich kontrolliertes System mit ausgeprägten Überwachungsmechanismen vertritt. Vor diesem Hintergrund bemüht sich die EU, einen „Dritten Weg" der digitalen Governance zu etablieren, der sich durch einen robusten Regulierungsrahmen wie die Datenschutz-Grundverordnung (DSGVO), den Digital Markets Act (DMA), den Digital Services Act (DSA), den Data Governance Act (DGA), den Data Act sowie den AI Act auszeichnet. Diese Regulierungsmaßnahmen zielen darauf ab, internationale Konkurrenzfähigkeit und Wirtschaftswachstum im EU-Binnenmarkt zu stärken, technologische Innovation zu gestalten, und gleichzeitig Menschenrechte, Rechtsstaatlichkeit und Demokratie zu gewährleisten sowie Nachhaltigkeit zu fördern. Sie wollen auch den Einfluss der EU über ihre Grenzen hinaus ausweiten und den sogenannten „Brüssel-Effekt" (siehe unten) zur Geltung bringen, mittels dessen die EU weltweit hohe regulative Standards prägen will.

Dieser Aufsatz verfolgt die Forschungsfrage, welche unterschiedlichen Governance-Modelle sich in den untersuchten Staaten entwickelt haben und ob das Streben Europas nach digitaler Souveränität und die EU-Digitalregulierung in Schwellenländern als Referenzmodell wahrgenommen wird. Zunächst wird untersucht, welche digitalen Governance-Modelle USA und China verfolgen und wie das europäische Modell sich davon unterscheidet, und sodann, welche globale Wirkung dieses entfaltet. Ausgehend von Anu Bradfords These des „Brüssel-Effekts" (Bradford 2019) wird der Einfluss der EU-Regulierung auf Drittstaaten analysiert. Die entsprechende Fallstudie zum Datenschutz untersucht die Gesetzgebung und Durchsetzung von Datenschutz in vier Schwellenländern und bewertet, ob und wie diese effektiv umgesetzt werden. Der Blick auf Schwellenländer erscheint besonders notwendig, da diese zu den Ländern mit den höchsten Internet-Nutzerzahlen gehören. Zudem spielen diese Länder in einer zunehmend multipolaren Welt eine wichtige Rolle bei der Gestaltung der internationalen Digital-Governance.

Methodisch stützt sich die Studie auf einen vergleichenden Ansatz und basiert auf insgesamt 12 Monaten empirischer Feldforschung, die zwischen 2020 und 2025 in Mexiko, Brasilien, Indien und Südafrika durchgeführt

wurde. Die Feldforschung wurde durch jeweils dreimonatige Entsendungen im Rahmen eines EU-Projekts mit dem Titel "Promoting Research on Digitalisation in Emerging Powers and Europe Towards Sustainable Development" (PRODIGEES) ermöglicht. Die Methodik umfasste in erster Linie leitfadengestützte qualitative Interviews mit 120 verschiedenen Akteuren. Dazu gehörten Experteninterviews mit staatlichen und akademischen Fachleuten, Vertreter:innen von Think Tanks, Branchenexperten und Digitalrechtsorganisationen sowie teilnehmende Beobachtung bei Veranstaltungen und eingehende Literatur- und Dokumentenrecherchen. Das Material wurde codiert und mit Methoden der qualitativen Inhaltsanalyse (Mayring 2022) ausgewertet.

2. Regimes digitaler Governance

Der Begriff der digitalen Governance-Regimes (vgl. Jia/Chen 2022; Staab 2024) umfasst die Gesamtheit der politischen Strategien, rechtlichen Regelungen und gestalterischen Rahmenbedingungen, die das Management und den Betrieb digitaler Technologien sowie des Internets bestimmen. Diese Governance-Regimes prägen eine Vielzahl von Themen, angefangen bei Datenschutz und Cybersicherheit bis hin zu Innovation, Wettbewerb und Marktzugang. Die geopolitische Bedeutung der digitalen Governance wird in den unterschiedlichen Ansätzen deutlich, die von den mächtigen globalen Akteuren wie den USA, China und der EU verfolgt werden. Dabei operieren diese Akteure unter jeweils eigenen regulatorischen Modellen, die von spezifischen Motivationen und Herausforderungen geprägt sind. In jüngerer Zeit werden diese Maßnahmen besonders stark hinsichtlich ihrer geopolitischen Implikationen diskutiert.

Die Vereinigten Staaten und China haben sich zu den wichtigsten Rivalen auf der globalen Bühne entwickelt, die beide nach einer technologischen Führungsrolle streben, welche letztlich die globalen Machtverhältnisse neu definieren wird. In Tabelle 1 sind die wesentlichen Unterschiede zwischen diesen beiden digitalen Governance-Regimes vergleichend dargestellt. Sie werden im Folgenden weiter ausgeführt.

Tabelle 1: Vergleich der Digital-Governance-Modelle zwischen den USA und China

	USA	**China**
Regulatorischer Ansatz	Minimale Regulierung: Zur Förderung des Wachstums der Technologiebranche verfolgt der Staat einen zurückhaltenden Ansatz mit geringer staatlicher Einmischung.	Staatlich kontrollierte Regulierung: Die Regierung übt eine umfassende Aufsicht aus, um die Ausrichtung auf nationale Prioritäten sicherzustellen.
Innovationsfokus	Starke Betonung des Aufrechterhaltens von Technologie-Führerschaft durch die Priorisierung von Innovation gegenüber Regulierung.	Technologie wird als Instrument des wirtschaftlichen Wachstums eingesetzt; die staatliche Aufsicht gewährleistet jedoch die Einhaltung geplanter politischer Vorgaben.
Marktdynamik	Setzt auf Marktkräfte zur Korrektur von Ungleichgewichten und verzichtet auf starke Regulierung, sofern nicht als unbedingt notwendig erachtet.	Die staatliche Intervention spielt eine zentrale Rolle in der Steuerung des Marktes und stellt sicher, dass Technologieunternehmen mit staatlichen Vorgaben konform gehen.
Wirtschaftliche Entwicklung	Marktorientierter Ansatz zur wirtschaftlichen Entwicklung; disruptive Technologieunternehmen sind führend bei Innovation und Expansion.	Ein durch die Regierung gelenkter Technologiesektor unterstützt nationale Wirtschaftsstrategien und Wachstumspläne.
Soziale Kontrolle	Begrenzte direkte staatliche Kontrolle über digitale Plattformen, allerdings teilweise Bedenken bezüglich Desinformation und Kinderschutz. Neuerdings Propagieren von „freedom of speech" für rechtspopulistische Sprechakte.	Technologie dient als Mittel zur sozialen und politischen Kontrolle und festigt digitalen Autoritarismus mittels Überwachung sowie staatlicher Zensur und Propaganda.
Daten-Governance	Dezentral organisierte Daten-Governance mit einer zentralen Rolle privater Unternehmen; Regularien wie die DSGVO fehlen weitgehend.	Umfangreiche Erfassung und staatliche Kontrolle der Daten von Bürger:innen zur Gewährleistung von Sicherheit und Stabilität.
Globaler Einfluss	Strebt globale Technologiedominanz primär durch privatwirtschaftliche Akteure wie Google, Apple, Meta, Amazon, Microsoft und Open AI an, staatlich unterstützt. Die Einflussnahme von großen Plattformen auf Handelspolitik und internationales Regierungshandeln ist gewachsen.	China propagiert sein Modell digitaler Steuerung weltweit, unter anderem durch Infrastruktur-Initiativen wie die „Digitale Seidenstraße", Setzung von Standards in internationalen Organisationen, eigene Internet-Foren und exportiert den Ansatz von Cyber-Souveränität und Datenlokalisierung in Partnerländer. Chinesische Unternehmen wie Tiktok, Huawei, Alibaba, Tencent, Baidu, Temu und Shein expandieren weltweit.

2.1 Das US-Modell digitaler Governance

Der Ansatz der USA zur digitalen Governance hat traditionell Marktfreiheit und Innovation in den Vordergrund gerückt. Der regulatorische Rahmen ist vergleichsweise gering, wodurch Technologieunternehmen erhebliche Freiräume zum Wachstum erhalten. Zu den zentralen Komponenten dieses Ökosystems zählen die staatliche Förderung entscheidender Innovationen (Mazzucato 2013), der Zugang zu hohen Risikokapital-Investitionen, das ingenieurwissenschaftliche Fachwissen und die Wissensressourcen der Universitäten sowie ein ausgeprägter Techno-Optimismus, der mit der Vorstellung einhergeht, dass ein „freies Internet" Freiheit und Demokratie fördert. All dies begünstigt rasches technologisches Fortschreiten und verschafft Start-ups eine schnelle Umsetzung in marktfähige Produkte und Dienstleistungen.

Die USA prägen die internationale Digitalpolitik in erster Linie durch ihre dominanten GAFAM-Plattformen – Google/Alphabet, Apple, Facebook/Meta, Amazon und Microsoft. Sie haben bisher einem libertären Modell den Vorzug gegeben, das marktwirtschaftliche Prinzipien priorisiert. Trotz wachsender öffentlicher Forderungen nach einer stärkeren Regulierung der Tech-Industrie angesichts von Datenschutzverstößen und schädlichen Online-Inhalten wurden regulatorische Interventionen durch intensives Lobbying der Unternehmen weitgehend ausgebremst. Es erscheint derzeit höchst unwahrscheinlich, dass ein bundesweites Datenschutzgesetz oder umfassende Reformen von Section 230 des Communications Decency Act von 1996 – der Online-Plattformen Haftungsimmunität für gepostete Inhalte gewährt – verabschiedet wird (Cohen 2019). Die Vereinigten Staaten setzen weiterhin auf die Maximierung ihres technologischen Potenzials, insbesondere um ihre Wettbewerbsfähigkeit gegenüber China zu wahren. Nationale Sicherheitsinteressen ermöglichen es der Regierung allerdings, auf Daten von Internetplattformen zuzugreifen (Bradford 2023).

Unter der Regierung von Präsident Biden zeigten sich jedoch spürbare Verschiebungen hin zu stärkerer staatlicher und gerichtlicher Aufsicht, wie die Durchsetzung von Kartellrecht durch die Federal Trade Commission und das Justizministerium sowie Bidens Executive Order zur Künstlichen Intelligenz demonstrierten (Biden 2023). Ein großer Teil dieser Maßnahmen wurde bereits in den ersten Wochen der zweiten Amtszeit von Präsident Trump per Dekret ausgesetzt und eine Abkehr von einer Regulierung der Tech-Konzerne vollzogen. Wie sich bereits bei Trumps Inaugurationsfeier zeigte, betonen die Eigentümer bzw. Geschäftsführer

der größten digitalen Plattform-Unternehmen eine große Nähe zur US-Regierung. Beispielsweise haben Meta und X Anfang Januar 2025 ihre Kooperation mit Fact-Checkern in den USA aufgekündigt und wollen diese durch sogenannte Community-Notes ersetzen. Inzwischen wird gegenüber Drittstaaten eine Verknüpfung von Digitalregulierung mit der Handelspolitik und Zöllen vollzogen, insofern als etwa der EU angedroht wird, eine scharfe Durchsetzung von DSA und DMA würde als „Erpressung" bewertet und hohe Bußgelder würden mit Zollerhöhungen „vergolten" (The White House 2025; Glenny/Muggah 2025; AP 2025). Die EU behält sich bisher vor, „alle Karten auszuspielen" und die Tech-Unternehmen weiterhin strikt zu regulieren (Reid 2025).

Unter Präsident Biden kam es zu verstärkten staatlichen Subventionen und industriepolitischen Maßnahmen, wie etwa durch den CHIPS Act zur Förderung der inländischen Halbleiterproduktion und Forschung sowie durch den Inflation Reduction Act. Mit solchen Initiativen hat die US-Technologiepolitik einen signifikanten Paradigmenwechsel vom traditionellen Laissez-faire-Herangehen hin zu einer stärkeren Förderung nationaler Wettbewerbsfähigkeit und Sicherheit vollzogen (Bradford 2023a). Unter Trump scheint sich das Zusammenspiel von staatlicher Politik und privatwirtschaftlichem Handeln noch zu verstärken, etwa bei der Ankündigung einer neuen KI-Infrastruktur namens „Stargate", wofür in den kommenden vier Jahren 500 Milliarden Dollar investiert werden sollen (Open.AI 2025) oder bei der Förderung von Elon Musks Satellitenprojekt Starlink in afrikanischen Ländern (Rudl 2025), was die zukünftige weltweite Gestaltung technologischer Entwicklungen prägen wird. Von libertären technologiepolitischen Vordenkern wie Peter Thiel und anderen werden Freiheit und Demokratie sogar zunehmend als Gegensatz konzipiert. Imaginiert werden dahingehend eine weitgehende Reduktion des Staates und sogar ein Verzicht auf demokratische Wahlen zugunsten einer Art von technologiegeführten Fürstentümern (vgl. Golumbia 2024).

2.2 Das chinesische Modell digitaler Governance

Im Gegensatz zu den USA ist das chinesische Modell der digitalen Governance staatlich und top-down geprägt, Technologie wird genutzt für wirtschaftliches Wachstum, soziale Kontrolle, Stabilität und Wahrung der Autorität der Kommunistischen Partei Chinas (KPCh). Die Regierung fördert die Wirtschaft durch Subventionen, Steuervergünstigungen und

Schutz vor ausländischer Konkurrenz. Ziel ist technologische Autarkie, etwa bei KI und Hochtechnologie, unterstützt durch Programme wie „Made in China 2025" (Holzmann/ Zenglein 2019). Das Internet ist durch die Große Firewall abgeschirmt, was dominante nationale Plattformen wie Baidu, Alibaba und Tencent begünstigt. Die Regierung schafft durch Gesetze wie Cybersecurity und Data Security Law ein strenges Regelwerk, das Kontrolle, Überwachung und Zensur ermöglicht. Diese Maßnahmen dienen dem Schutz der Industrie, der Stabilität und der Wahrung der Autorität der KPCh. Unter dem Motto „Gemeinsamer Wohlstand" verfolgt China eine inklusive Wachstumsstrategie, wobei der Nutzen für Bürger:innen mit strenger Internetkontrolle und Sanktionen bei Dissens einhergeht (Lilkov 2020).

Während technologische Entwicklungen mit ökonomischer Stoßrichtung staatlich gefördert werden, unterbindet der Staat gleichzeitig gezielt das Entstehen privatwirtschaftlicher Akteure, die seine Autorität gefährden könnten. Einige Eingriffe in jüngerer Zeit – wie das Vorgehen gegen Jack Ma's Ant Group (2020), die Milliardenstrafe gegen Alibaba (2021) und das Verhindern einer von Tencent unterstützten Fusion – spiegeln eine Neubewertung des staatlichen Umgangs mit dem Privatsektor wider (Bradford 2023a, S. 94ff.).

Das chinesische Modell baut flächendeckend digitale Technologien wie Gesichtserkennung, Big Data und KI zur Überwachung und sozialen Steuerung aus, um Loyalität und gesellschaftlichen Konformismus zu fördern (Lilkov 2020). Chinas Konzept der „Cyber-Souveränität" umfasst territoriale Datenlokalisierung, bei der alle Daten in China gespeichert und staatlicher Zugriff gesetzlich möglich sind. China propagiert dieses Modell international, insbesondere im Globalen Süden, um geopolitischen Einfluss zu gewinnen (Fischer 2022). Insgesamt steht das chinesische Modell für eine autoritäre Ausrichtung. Der chinesische Technologiesektor profitiert aber auch von marktgetriebener Innovation und Wagniskapital. Dies verdeutlicht, dass politische Freiheit kein notwendiges Erfordernis für technologischen Fortschritt und damit einhergehender wirtschaftlicher Prosperität ist – was verbreitete westliche Annahmen zunehmend herausfordert.

Extern stärkt China seinen Einfluss durch den Export digitaler Infrastruktur im Rahmen der „Digitalen Seidenstraße", etwa 5G-Technologien durch Huawei, Netzwerklösungen von ZTE sowie Smart-City-Projekte. Dieser Infrastruktur-Export gilt als kostengünstiger Weg zur Entwicklung, birgt aber hohe Schulden- und Abhängigkeitsrisiken, oft durch Kredite,

die mit Rohstoffen gesichert sind. China stärkt zudem seinen Einfluss in internationalen Standardorganisationen der digitalen Governance, wie der International Telecommunication Union (ITU) und der International Organization for Standardization (ISO) sowie bei Online-Zahlungssystemen zur Förderung des Yuan. Das zeigt sich in digitalpolitischen Gremien wie der UN-Open Ended Working Group, dem seit 2014 abgehaltenen Wuzhen Summit und der 2020 gestarteten „Global Data Security Initiative" (Erie/Streinz 2021; Recorded Future 2021). Zudem verzeichnet China eine wachsende Präsenz von Plattformen wie TikTok, Alibaba, Tencent, Temu und Shein auf globalen Märkten.

Zusammenfassend verbindet Chinas Ansatz zur digitalen Governance Elemente von digitalem Autoritarismus mit selektiver Adaption regulatorischer Praktiken, die durchaus an die EU angelehnt sind. Ziel ist technologische Überlegenheit, wirtschaftliche Entwicklung und politische Kontrolle. Es gibt Datenschutz- und Wettbewerbsregeln, die große chinesische Tech-Unternehmen einschränken, ähnlich wie in der EU (Bradford 2023a). Gleichzeitig nutzt China Technologie systematisch für Zensur und Überwachung, um Stabilität zu sichern. Ob dieses Modell langfristig nachhaltig ist, ist unklar, da wirtschaftliche Risiken wie Immobilienblasen und Jugendarbeitslosigkeit bestehen, und fraglich ist, ob die Bevölkerung mittels bequemer digitaler Dienste und Wachstum dauerhaft loyal bleibt.

2.3 Die sich zuspitzende Rivalität zwischen den USA und China

Das globale Feld digitaler Governance ist zunehmend geprägt von Spannungen, die Innovationspfade, Regulierungen und internationale Beziehungen beeinflussen. Die digitale Rivalität zwischen den USA und China hat insbesondere durch KI, Konkurrenz um strategische Rohstoffe wie seltene Erden, Hochleistungs-Chips und Datenzentren sowie handelspolitische Spannungen in den letzten Jahren stark zugenommen. Beide Staaten liegen bei der Wertschöpfung aus der Datenwirtschaft an der Weltspitze: Sie beherbergen den Großteil der globalen Hyperscale-Rechenzentren, verfügen über die schnellsten Internetverbindungen, generieren über 94 % der Investitionen in KI-Start-ups und vereinen etwa 90 % der Börsenkapitalisierung der zehn größten Digitalunternehmen auf sich (UNCTAD 2021). Zugleich entstehen dadurch neue Disparitäten und Innovationsgefälle, da physische Faktoren wie Wasser und Energieversorgung, lokales Fachpersonal und der Zugang zu spezialisierten Chips zu entscheidenden Voraussetzungen

der KI-Ökonomie werden (UNCTAD 2024). Drei Unternehmen - Amazon Web Services, Microsoft Azure und Google Cloud - bieten mehr als 65 Prozent der weltweiten Cloud-Dienste an, ein Markt, der 2024 auf über 750 Milliarden US-Dollar geschätzt wurde. 90 Prozent der europäischen Cloud-Infrastruktur wird von US-Unternehmen kontrolliert. Die USA dominieren auch die Dateninfrastruktur; ihre mehr als 5.400 Rechenzentren übertreffen die von Deutschland (529) und Großbritannien (523) ums Zehnfache. Schätzungsweise 70 Prozent des weltweiten Internetverkehrs fließen über Server in den USA (Glenny/ Muggah 2025).

In diesem sich verändernden globalen Kontext stellt sich die Frage, ob Europa und der Globale Süden zwischen diese geopolitischen Fronten geraten sind und sich für eines der beiden konkurrierenden Modelle im internationalen digitalen Wettbewerb entscheiden müssen – oder ob sie, wie etwa von der EU proklamiert, einen eigenen Ansatz zur Digital-Governance und digitalen Souveränität als „Dritten Weg" etablieren können.

Angesichts der enormen Marktmacht großer Plattformen ergibt sich zudem die Frage, wer tatsächlich die Regeln setzt und wer sich diesen zu unterwerfen hat: Sind große Digitalplattformen eigentlich „Rule-Taker" oder „Rule-Maker"? Haben sie mittlerweile gar mehr Einfluss auf digitale Geschäftsmodelle, Wertschöpfungsketten und das individuelle wie kollektive Verhalten als Nationalstaaten? In der Praxis fungieren diese Plattformen selbst als regulatorische Akteure – sie beeinflussen über ihre Geschäftsmodelle, technologischen Designs, Algorithmen und die Steuerung dessen, welche Inhalte in Suchmaschinen und sozialen Netzwerken prominent sichtbar sind, maßgeblich das digitale Nutzungsverhalten. In den USA wird dieser Sachverhalt beispielsweise mithilfe der Begriffe „Private Ordering" oder „Code is Law" (Lessig) diskutiert (vgl. Cohen 2019), während im Globalen Süden zuweilen von „digitalem Kolonialismus" gesprochen wird (Belli/Zingales 2017; Dachwitz/Hilbig 2025). Nichtsdestotrotz steht auch die Rückkehr staatlicher Steuerungsansprüche – insbesondere in der Forderung nach technologischer Souveränität und dem Streben nach strategischer Autonomie – zunehmend zur Debatte (CERRE 2024; FES 2024).

3. Das Regulierungsmodell der Europäischen Union für digitale Governance

3.1 Zentrale Regulierungsinitiativen der Europäischen Union

Die EU strebt danach, sich als ambitionierte regulatorische Supermacht zu positionieren und damit einen eigenständigen „Dritten Weg" zu etablie-

ren, der sie sowohl von den Modellen der Vereinigten Staaten als auch Chinas abgrenzt (Hobbs 2020). Innerhalb der EU mehren sich allerdings Stimmen, die unter dem Motto von „Vereinfachung", Entbürokratisierung und „Innovationsoffensive" eine Abkehr von dieser Strategie fordern (European Commission 2024; vgl. Csernatoni 2025; von Thun et al. 2025; Schneider 2025). In diesem Spannungsfeld versucht die EU, sich als internationales Referenzmodell für andere Staaten darzustellen. In den vergangenen Legislaturperioden hat die EU eine Reihe umfassender gesetzlicher Regelwerke verabschiedet (zum Überblick siehe Bruegel 2024). Die Datenschutz-Grundverordnung (DSGVO), die 2018 in Kraft trat, hat strenge Maßstäbe für den Datenschutz in der EU gesetzt und sieht bei Verstößen empfindliche Bußgelder vor. Der Digital Markets Act (DMA) zielt darauf ab, fairen Wettbewerb zu gewährleisten, indem er wettbewerbswidrige Praktiken großer Gatekeeper-Plattformen einschränkt. Der Digital Services Act (DSA) fokussiert auf sehr große Online-Plattformen und Suchmaschinen und fördert Transparenz und Sicherheit der Nutzer:innen. Der Data Governance Act (DGA) sowie der Data Act sollen durch mehr Datenzugang die europäische Datenökonomie für kleinere und mittlere Unternehmen erschließen. Die KI-Verordnung schließlich definiert Standards für Künstliche Intelligenz, kategorisiert vier Risikostufen und legt insbesondere für Hochrisikosysteme spezifische Auflagen fest.

Zusammengenommen bilden diese Regulierungen ein robustes Rahmenwerk der digitalen Governance, das die EU als Vorreiterin bei Datenschutz, fairem Marktzugang und nachhaltiger Innovation positioniert (CAIDP 2025; UNCTAD 2021 und 2024). Ziel ist ein *level playing field*, das Wachstum, Wettbewerb und Innovation sowohl im EU-Binnenmarkt als auch global fördert. Gleichzeitig stehen die Mitgliedstaaten vor der Herausforderung, technologische Entwicklung zu unterstützen und zugleich die Grundrechte der Bürger gegenüber staatlichen Sicherheitsinteressen und ausländischer Einflussnahme zu schützen.

Mit ihrer Strategie „Weg in die Digitale Dekade" hat die Europäische Union ehrgeizige Ziele für die digitale Transformation bis 2030 definiert (European Council 2022a und 2024). Der „Digital Compass" legt die Vision und Zielvorgaben für die Digitalisierung der EU fest (European Commission 2021), während das entsprechende internationale Politikprogramm das Rahmenwerk für ihre Umsetzung bereitstellt (European Council 2022b).

3.2. Der „Brüssel-Effekt": Konzept und Implikationen

Der Begriff „Brüssel-Effekt", wie ihn Anu Bradford (2019) geprägt hat, bezieht sich auf die weitreichenden extraterritorialen Wirkungen der regulatorischen Maßnahmen der Europäischen Union. Er umfasst zwei zentrale Prozesse: Erstens neigen globale digitale Plattformen und Unternehmen dazu, die hohen regulatorischen EU-Standards auch außerhalb Europas freiwillig zu übernehmen. Dies liegt daran, dass es für diese Akteure unpraktisch und zu aufwendig wäre, ihre digitalen Architekturen und Systemdesigns jeweils genau den unterschiedlichen nationalen Regularien anzupassen. Zweitens fungieren die EU-Regelungen zunehmend als Referenzmodelle für die Gesetzgebung in anderen Ländern, die ihre eigenen Rechtsrahmen an die EU-Standards angleichen, um Zugang zu wichtigen Märkten zu erhalten oder internationale Kooperationen zu erleichtern.

Der Brüssel-Effekt stellt daher Bradford zufolge eine Form der unilateralen, globalen Regulierung dar, bei der die Rechtsnormen der EU primär durch Marktmechanismen nach außen hin durchgesetzt werden. Dies sei auf mehrere Faktoren zurückzuführen: Die Größe des EU-Binnenmarktes mit seinen 450 Millionen Konsument:innen ermöglicht es, Einfluss auf ausländische Akteure auszuüben; die beträchtlichen regulatorischen Kapazitäten der EU erlauben eine wirksame Durchsetzung; EU-Vorschriften können den Zugang zu sämtlichen Märkten erleichtern; durch ihre Relevanz im globalen Verbrauchermarkt werden einheitliche Produktstandards bei multinationalen Unternehmen gefördert und regulatorische Kosten minimiert. Zusammengenommen führt dies zu dem, was Bradford als „de-facto-Brüssel-Effekt" bezeichnet, bei dem es primär die Unternehmen selbst sind, die die hohen EU-Standards nicht nur innerhalb der EU, sondern weltweit implementieren (Bradford 2019, S. 83-84.).

Daneben gibt es den „de jure-Brüssel-Effekt", bei dem Nicht-EU-Länder formell durch Gesetzgebung, Regulierung oder durch internationale Abkommen an EU-Standards angepasste Regeln in ihren eigenen Rechtssystemen verankern (dies., S. 67-68). Dadurch wird die Einflussnahme der EU auf globale Regulierungen institutionalisiert und verstärkt. Insgesamt zeigt der Brüssel-Effekt, wie die EU ihre regulatorische Macht über nationale Grenzen hinweg ausübt und globale Standards maßgeblich beeinflusst.

Insbesondere die Datenschutz-Grundverordnung (DSGVO) hat Wirkungen ausgelöst, die weit über das Territorium der EU hinausreichen. Erstens gilt unter dem Marktortprinzip, das in der DSGVO (Art. 3 Abs. 2) verankert ist, dass Anbieter digitaler Produkte und Dienste in der EU die

Datenschutzregeln der EU einhalten müssen, ungeachtet dessen, wo sie ihren Firmensitz haben. Zweitens sind europäische Datenschutzprinzipien in internationalen Handelsabkommen der EU mit Drittländern verankert, was die Etablierung globaler Standards fördert. Für globale Technologieriesen wäre es ökonomisch unklug, den lukrativen europäischen Markt aufzugeben; die Organisation ihrer Geschäftstätigkeit auf der Grundlage vieler verschiedener rechtlicher Rahmenbedingungen wäre mühsam, und die Mobilität der Daten erfordert faktisch eine transnationale Harmonisierung (Bendiek/Römer 2019). Zudem kann die EU für den Transfer persönlicher Daten in Drittländer einen Angemessenheitsbeschluss fassen, womit diese dem Datenschutz innerhalb der EU gleichgestellt werden und keine weitere Genehmigung bedürfen (laut Art. 45 Abs. 3 DSGVO).

Bradford (2019) argumentiert, dass es für die Unternehmen effizienter sei, strenge europäische Vorschriften weltweit umzusetzen, als Architektur und Design ihrer Dienste zu fragmentieren. Infolgedessen tendierten diese Anbieter digitaler Dienstleistungen dazu, Verbraucher:innen in anderen Rechtsordnungen das gleiche Schutzniveau zu bieten wie den Europäer:innen. Diese Situation führe dazu, dass die EU ihre Datenschutzgesetze effektiv über ihre Grenzen hinaus ausdehne und ausländische Marktteilnehmer veranlasse, sich an die EU-Vorschriften zu halten, unabhängig davon, ob sie Kund:innen in der EU, den USA oder in anderen Ländern beliefern.

3.3 Der EU-Ansatz für rechtsbasierte und menschenzentrierte digitale Governance

Das digitale Governance-Regime der Europäischen Union bietet einen strukturierten Rahmen, um der dominierenden Einflussnahme großer Tech-Unternehmen entgegenzuwirken. Es versteht sich als Korrektiv gegenüber den wahrgenommenen regulatorischen Schwächen in den USA und den Übergriffen des autoritativen Modells Chinas. Der EU-Rahmen zeichnet sich dadurch aus, dass er den Schwerpunkt auf die Förderung des öffentlichen Interesses, die Abwägung der Macht von Unternehmen und die Wahrung demokratischer Werte legt. Wie in Tabelle 3 dargestellt, basiert die digitale Governance der EU auf Prinzipien, die mit Menschenrechten und demokratischen Grundwerten in Einklang stehen. Dies fußt auf einem Gesellschaftsvertrag, der Grundrechte, Demokratie, Solidarität, und Rechenschaftspflichten verankert sowie auf dem Ziel, einen digitalen Binnenmarkt zu schaffen (Bradford 2023b; European Commission 2021).

Tabelle 2: Das digitale Governance-Modell der Europäischen Union

	Europäische Union
Regulatorischer Ansatz	Starkes regulatorisches Rahmenwerk mit Schwerpunkt auf Transparenz, Fairness und Rechenschaftspflicht in der digitalen Wirtschaft.
Innovationsfokus	Will ethische und menschenzentrierte Innovation priorisieren, um sicherzustellen, dass KI und digitale Technologien sicher, nachhaltig und vertrauenswürdig sind.
Marktdynamik	Sucht eine Balance zwischen Regulierung und Wettbewerb, um Monopole zu verhindern und gleichzeitig einen wettbewerbsfähigen Markt zu fördern.
Wirtschaftsentwicklung	Fördert eine digitale Wirtschaft, die mit europäischen Werten im Einklang steht, mit Schwerpunkt auf Nachhaltigkeit und sozialer Verantwortung.
Soziale Kontrolle	Betont digitale Rechte und will sicherstellen, dass Nutzer:innen die Kontrolle über ihre Daten und digitalen Interaktionen behalten.
Daten-Governance	Umfassendes Rahmenwerk für Daten-Governance, einschließlich DSGVO, um Datenschutz, Sicherheit und Nutzerermächtigung zu stärken.
Globaler Einfluss	Exportiert regulatorische Standards weltweit durch den „Brüssel-Effekt" und beeinflusst so Digitalpolitik über die eigenen Grenzen hinaus.

Die Vorteile des EU-Governance-Modells liegen in der Gemeinwohlorientierung und der Bewahrung demokratischer Strukturen. Doch es gibt Herausforderungen, vor allem bei der Innovationsfähigkeit: Kritiker warnen, dass strenge EU-Vorschriften die Innovation hemmen und verweisen auf die vergleichsweise geringe Zahl führender europäischer Tech-Unternehmen. Der Ende 2024 veröffentlichte Draghi-Bericht moniert viel zu geringe private und öffentliche Investitionen in digitale Technologien (European Commission 2024) und fordert regulative Vereinfachung. Bradford (2023b und 2024) weist jedoch darauf hin, dass Probleme wie ein fragmentierter digitaler Markt und unzureichende Risikokapitalressourcen sowie die Abhängigkeit von ausländischen Datenzentren eine größere Rolle bei der Innovationslücke spielen als die Regulierung selbst.

Für die EU ist es entscheidend, ihre Vorschriften kohärent in allen Mitgliedstaaten zu implementieren. Nur durch eine effektive Durchsetzung kann die EU ihre globale Glaubwürdigkeit sichern und die Wirksamkeit ihrer regulatorischen Maßnahmen unter Beweis stellen. Ein Beispiel für gewisse Vollzugsdefizite bildet die langwierige Durchsetzung der DSGVO. So hat die irische Datenschutzbehörde erst 2022/2023 begonnen, hohe Bußgelder gegen Digitalunternehmen zu verhängen, die ja überwiegend aus Steuergründen ihren europäischen Sitz in Irland haben. Das bislang höchste Bußgeld beträgt 1,2 Milliarden Euro gegenüber Meta Platforms

Ireland wegen unzureichender Rechtsbasis für deren Datenverarbeitung. Zudem verhängte die irische Aufsichtsbehörde eine Strafe in Höhe von 345 Millionen Euro gegen TikTok. Luxemburg sanktionierte Amazon Europe mit 746 Millionen Euro wegen unzureichender Rechtsbasis für die Datenverarbeitung (GDPR Enforcement Tracker 2025). Entscheidend für den Erfolg der europäischen Datenschutzaufsichtsbehörden wird sein, ob sie in der Lage sind, die Einhaltung der Vorschriften nicht nur durch hohe Bußgelder einzufordern, sondern andere, datenschutzkonforme Geschäftsmodelle durchzusetzen.

Der Erfolg neuer Regelwerke wie des Digital Services Act (DSA), des Digital Markets Act (DMA) und des AI-Acts hängt wesentlich davon ab, wie effektiv die EU diese Gesetze um- und durchsetzen kann. Dabei sind eine abgestimmte Policy-Koordination zwischen Europäischer Kommission und den nationalen Mitgliedstaaten sowie sektorübergreifende Strategien notwendig. Zudem muss die EU gegen Vorwürfe von Überregulierung antreten: Insbesondere aus den USA wird die Ansicht vertreten, die strengen Regeln der EU seien protektionistische Maßnahmen gegen US-Unternehmen (The White House 2025). Die EU betont jedoch, dass es um Verhaltensstandards gegen den Missbrauch marktbeherrschender Macht geht, unabhängig von der Nationalität der Unternehmen. Gleichwohl prägen die EU-Verordnungen weiterhin globale Standards und gelten vielfach als Vorbild für regulatorische Reformen, die von Gesetzgebern und zivilgesellschaftlichen Akteuren gleichermaßen begrüßt werden.

4. Die Wirkung des Brüssel-Effekts im Datenschutz

Der Datenschutz ist das prominenteste Beispiel für den Brüssel-Effekt. Die DSGVO hat zahlreiche Länder inspiriert, ihre eigenen Regelungen zu schaffen und gilt aufgrund des hohen Datenschutzniveaus weltweit als Goldstandard (UNCTAD 2021). Bislang haben 167 Staaten entsprechende – teilweise an die DSGVO angelehnte – Gesetze erlassen, über 94 Nationen Datenschutzbehörden eingerichtet, sodass etwa 83 % der Weltbevölkerung in Rechtsordnungen mit umfassendem Datenschutz leben (Banisar 2025). Dies klingt wie eine globale Erfolgsgeschichte der DSGVO. Es bleibt jedoch wichtig, nicht nur die formalen legislativen Errungenschaften zu betrachten, sondern auch die praktische Umsetzung des Datenschutzes in den jeweiligen Ländern zu untersuchen. In allen vier betrachteten Schwellenländern wird die Privatsphäre der Bürger:innen als ein fundamentales,

verfassungsrechtlich geschütztes Recht anerkannt. Die Umsetzung dieses Grundrechts mittels Datenschutzgesetzen und deren Implementierung ist jedoch mit erheblichen Herausforderungen verbunden, wie nun anhand der Datenschutzgesetze und ihrer Durchsetzung in Mexiko, Brasilien, Indien und Südafrika ausgeführt wird.

4.1 Datenschutz in Mexiko

Mexiko verfügt über zwei Datenschutzgesetze: eines für den privaten Sektor und ein zweites für den öffentlichen Sektor. Das 2010 verabschiedete Bundesgesetz zum Schutz persönlicher Daten in der Hand von Personen (*Ley Federal de Protección de Datos Personales en Posesión de Particulares*, kurz LFPDPPP) gilt für den Privatsektor. Für den öffentlichen Sektor wurde 2017 das Allgemeine Gesetz zum Schutz von Daten in der Hand von Verpflichteten (*Ley General de Protección de Datos en Posesión de Sujetos Obligados*) verabschiedet, das sich deutlich an der DSGVO orientiert. Diese Doppelstruktur schafft gewisse Inkonsistenzen, da der öffentliche Sektor nunmehr stärker reglementiert ist als der private. Zudem hat Mexiko 2018 die Konvention 108 des Europarats zum Datenschutz unterzeichnet, was einen bedeutenden Schritt in Richtung einer Harmonisierung des internationalen Datenverkehrs darstellt.

Das Nationale Institut für Transparenz, Zugang zu Informationen und Datenschutz (INAI – *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*) beschäftigte bis Ende 2024 etwa 100 Mitarbeitende, die sich dem Vollzug der Datenschutzvorschriften widmeten. Von 2014 bis Ende 2024 hat das INAI als unabhängige Behörde agiert.

Das INAI ist eine sehr aktive Aufsichtsbehörde, die im Jahr 2022 119 Verfahren eingeleitet und 78 davon abgeschlossen hat, was zu Bußgeldern in Höhe von umgerechnet insgesamt 2,8 Millionen Euro vor allem an Medienunternehmen, Finanzdienstleister und Versicherungen führte (Villanueva Plasencia 2023). Sanktionen durch das INAI werden jedoch häufig gerichtlich angefochten, was ihre Durchsetzung erschwert. Kritiker bemängeln, das INAI habe in der Vergangenheit zu wenig proaktiv agiert und Verstöße unzureichend verfolgt.

Herausforderungen in der Durchsetzung des Datenschutzes bestehen in einer schwachen Datenschutzkultur sowie in erheblichen Verstößen, die kaum geahndet werden. Das Freihandelsabkommen USMCA/T-MEC von

2020 enthält zwar eine Datenschutzklausel, verbietet jedoch Datenlokalisierung auf nationaler Ebene, was es Unternehmen erleichtert, ihre Server in die USA zu verlegen und damit die mexikanischen Vorgaben auszuhebeln. Dieses „Forum-Shopping" von großen Unternehmen um die niedrigsten Datenschutzstandards bildet zum Verdruss des INAI ein hohes Hindernis für das effektive Implementieren der mexikanischen Datenschutzgesetze. Weitere Schwierigkeiten ergeben sich aus mangelnder Sensibilisierung für Datenschutzfragen, geringer Bewusstheit über die rechtlichen Implikationen der Datenverarbeitung sowie mangelnder Kenntnis der Bürger:innen über ihre Rechte (Schneider 2022). Allerdings hat das INAI durchaus erfolgreich niedrigschwellige Aufklärung über Datenschutzrechte geleistet und dabei mit Comics, Spielen und anderen Informationseinheiten innovative Wege eingeschlagen.

Das INAI wurde, initiiert durch Präsident Andrés Manuel López Obrador und vollendet durch seine Nachfolgerin Präsidentin Claudia Sheinbaum, durch eine Verfassungsreform im Dezember 2024 ebenso wie sechs weitere autonome Behörden aufgelöst; begründet wurde dies mit Effizienz und Verwaltungsvereinfachung. Die Aufgaben der INAI wurden auf das neu geschaffene Sekretariat für Korruptionsbekämpfung und gute Regierungsführung übertragen und damit dem Ministerium unterstellt (Huitron 2025). Beobachter sehen darin eine bedeutsame Schwächung des Datenschutzes und fürchten, dass die Regierung den Datenschutz politischen Motiven gefügig macht. Mexiko war zudem im Begriff, von der EU einen Angemessenheitsbeschluss für den personenbezogenen Datentransfer zu erhalten, die es Mexiko ermöglicht hätte, digitale Dienstleistungen mit starken Datenschutzgarantien anzubieten. Dies ist nach dem Verlust der Unabhängigkeit als Behörde nunmehr wohl nicht mehr möglich. Im Zuge der Unsicherheit über die Zukunft des INAI haben eine Reihe langjähriger Mitarbeiter:innen das INAI verlassen, was auch mit dem Verlust von Erfahrungswissen einhergeht.

4.2 Datenschutz in Brasilien

Brasilien zählt zu den Pionieren im Bereich der digitalen Rechte. 2014 wurde der *Marco Civil da Internet* verabschiedet, ein grundlegendes Gesetz, das zentrale digitale Rechte, einschließlich der Netzneutralität, kodifiziert hat (Belli/Doneda 2022). Das 2018 in Kraft getretene Allgemeine Datenschutzgesetz (LGPD – *Lei Geral de Proteção de Dados*) stimmt in recht

hohem Maße mit der DSGVO überein. LGPD war gleichwohl das Produkt ausführlicher, mehrjähriger Debatten im Parlament, in Anwaltskreisen, Unternehmen und der Zivilgesellschaft (Brioni 2020).

Die brasilianische Datenschutzbehörde (ANPD – *Autoridade Nacional de Proteção de Dados*) wurde im November 2020 eingerichtet und erhielt im Oktober 2022 formale Autonomie. In den Anfangsjahren unter der Regierung von Präsident Jair Bolsonaro arbeitete die ANPD in einer schwierigen Konstellation, drei der fünf Direktoren stammen vom Militär. Obwohl ANPD von 50 im Jahr 2021 auf 141 Mitarbeitende im Jahr 2024 gewachsen ist, besteht weiterhin Ressourcenknappheit.

Die ANPD hat wichtige Regelungen zum Datenschutz in Brasilien erlassen, darunter Meldepflichten bei Datenpannen und Kooperationspflichten. Die Verhängung von Sanktionen erfolgt bedächtig, obwohl tausende von Beschwerden wegen Datenschutzverletzungen eingegangen sind. Bis Herbst 2024 wurden lediglich sieben Verwarnungs- und Sanktionsentscheidungen getroffen, zumeist im Bereich der öffentlichen Verwaltung und unzureichender Meldung von Sicherheitsvorfällen (ANPD 2024c).

Das Einhalten der Datenschutzvorschriften gestaltet sich sowohl im öffentlichen als auch im privaten Sektor herausfordernd. Datenschutz wird jedoch für Unternehmen bedeutender, da er sich auf ihre Reputation auswirkt. Die bisher wenigen, aber strengen Maßnahmen der ANPD veranschaulichen, dass ANPD bestrebt ist, Compliance-Praxen zu verbessern und interne Prozesse zu stärken. Unter der Regierung von Präsident Lula da Silva seit 2022 entwickelt sich die ANPD zu einer resilienteren und glaubwürdigeren Institution, insbesondere im Hinblick darauf, die Standards der OECD, zu der Brasilien beitreten will, zu erfüllen.

Seit 2024 erhielt ANPD weitere Aufgaben, sie fungiert nun auch als Koordinationsbehörde für die Regulierung Künstlicher Intelligenz. Im Zuge dieser Aufgabenerweiterung hat ANPD eine öffentliche Konsultation zu automatisierten Entscheidungen durch KI ausgeschrieben, deren Ergebnisse sie in einer Technischen Mitteilung zusammenfasst (ANPD 2024a). Das Personal soll nunmehr um weitere 200 Personen aufwachsen, um die Aufsicht bei der Regulierung von KI zu übernehmen. Ein brasilianisches KI-Gesetz wurde im Dezember 2024 vom Senat verabschiedet und an den Kongress zur Befassung überwiesen.

Im Juli 2024 erließ ANPD (2024b) eine Präventivmaßnahme, mit der die sofortige Aussetzung der neuen Datenschutzrichtlinie von Meta in Brasilien angeordnet wurde, welche die Verwendung der auf seinen Plattformen veröffentlichten personenbezogenen Daten für das Training von KI-Syste-

men erlaubten. Für die Nichteinhaltung wurde eine tägliche Geldstrafe von 50.000 R$ (rund 8000 Euro) festgesetzt. Im November 2024 begann die ANPD, TikTok hinsichtlich des Umgangs mit Daten von Kindern zu untersuchen. Die ANPD prüfte, ob die Plattform Daten von Minderjährigen unrechtmäßig sammelt und verarbeitet, und hat die Nutzung der App ohne Registrierung und Altersüberprüfung verboten. Im März 2025 versprach ByteDance, dieser Anordnung nachzukommen (Flach 2025).

Das 2025 in Brasilien gestartete Pilotprojekt „dWallet", initiiert von der der kalifornischen Firma DrumWave in Zusammenarbeit mit der staatlichen Firma Dataprev soll Bürger:innen ermöglichen, ihre persönlichen digitalen Daten zu verwalten, Eigentumsrechte daran geltend zu machen und durch deren Verkauf Geld zu verdienen. ANPD hat bereits 2022 ein Inspektionsverfahren gegen DrumWave eingeleitet, um seine Vereinbarkeit mit LGPD zu prüfen (ANPD 2022; Daros 2025).

TFH, einem Unternehmen, das von Sam Altman, CEO von OpenAI, und dem deutschen Informatiker Alex Blania gegründet wurde, gelang es, die Iris-Scan-Daten von 400.000 Brasilianer:innen zu registrieren, indem es ihnen einen Geldbetrag in Kryptowährung anbot. Im Januar 2025 ordnete ANPD jedoch an, dass Tools for Humanity (TFH) diese Praxis einstellen muss, unter Verweis auf eine Beeinträchtigung für die freie Zustimmung der Nutzer und Verstöße gegen das Datenschutzgesetz. TFH argumentiert, dass die Sammlung biometrischer Daten digitale Sicherheit erhöht und es Datenschutzstandards einhält, doch ANPD hält die Praxis aufgrund der Nicht-Rückholbarkeit der gesammelten Daten und der Vulnerabilität der Teilnehmenden für besonders bedenklich (ANPD 2025a, DW 2025).

Wie aus diesen Maßnahmen deutlich wird, hat ANPD inzwischen an Biss gewonnen und geht auch den Praktiken großer US-Unternehmen auf den Grund. Obwohl das LGPD eine wichtige Errungenschaft darstellt, ist seine Durchsetzung in Brasilien selbst bisher noch schwach. Dies liegt auch daran, dass eine Datenschutzkultur kaum ausgeprägt ist. In Brasilien ist es üblich geworden, die Steuernummer CPF (*Cadastro de Pessoas Físicas)* überall abzufragen; in Supermärkten erhält man damit einen Rabatt, auch Apotheken, Museen und Ämter erfragen sie. Sensible Daten können so leicht getrackt und unter der einheitlichen CPF zusammengeführt werden. Zudem trennen Brasilianer:innen in ihren sozialen Netzwerken und Messenger-Diensten nicht zwischen Beruf und Privatem, sondern teilen sogar recht intime Fotos bereitwillig mit Kollegen und Öffentlichkeit. Allfällige Datenlecks werden leichtfertig hingenommen.

Allerdings gibt es weitere Kräfte, die dazu führen, dass Privatsphäre ernster genommen wird. Dazu zählen das Verfassungsgericht, wo wichtige Verfahren anhängig sind und eine gut organisierte digitalrechtliche Zivilgesellschaft. Bundesrichter Alexandre de Moraes vom Obersten Bundesgericht Brasiliens ordnete beispielsweise am 30. August 2024 die Telekombetreiber an, die App X (ehemals Twitter) aufgrund unzureichender Bekämpfung von Hassrede und Verletzung der Regelungen zur Anwesenheit eines rechtlichen Vertreters im Land zu sperren. Diese Anordnung wurde am 2.September 2024 vom Obersten Gerichtshof bestätigt. Moraes hatte Elon Musk ein Ultimatum gesetzt, bestimmte rechtsradikale Nutzerkonten und die Verbreitung gewisser Falschinformationen, insbesondere zum Sturm auf die Regierungsgebäude in Brasilia im Januar 2023, zu löschen. Dem war Musk nicht nachgekommen, sondern zog stattdessen seinen rechtlichen Vertreter aus Brasilien ab. Nachdem X dann angeblich „versehentlich" eine Umgehungsmöglichkeit zur weiteren Nutzung von X in Brasilien eröffnet hatte, wurde zudem ein hohes Strafmaß verhängt. Aus diesem Kräftemessen mit X ging Moraes als Sieger hervor. Nach etlichen Verunglimpfungen fügte sich Musk, zahlte die Geldstrafe von rund 5 Mio. US-Dollar und benannte auch wieder einen Repräsentanten für das Land, woraufhin am 9. Oktober 2024 die Sperrung aufgehoben wurde (AP 2024). Zu Musks Einlenken hat sicherlich auch beigetragen, dass binnen weniger Tage Bluesky in Brasilien zwei Millionen neue Nutzer:innen (insgesamt 4 Millionen) verzeichnete (X hat 21 Millionen Nutzer in Brasilien).

Der Oberste Gerichtshof Brasiliens STF (*Supremo Tribunal Federal*) traf am 26. Juni 2025 eine weitreichende Entscheidung über die Haftung von Online-Plattformen für Nutzerinhalte. Die Richter entschieden mit einer Mehrheit von 8 zu 3 Stimmen, dass Social-Media-Plattformen in Zukunft direkt für illegale Inhalte ihrer Nutzer haftbar gemacht werden können. Eine vorherige gerichtliche Anordnung zur Löschung solcher Beiträge ist daher nicht mehr erforderlich (Krempl 2025).

Abschließend bleibt festzuhalten, dass das Datenschutzgesetz LGPD ein bedeutender Fortschritt ist, aber bisher auch aufgrund begrenzter personeller und finanzieller Ressourcen noch nicht stark durchgesetzt wird. US-Technologieplattformen wie Meta und Alphabet ziehen weiterhin große Mengen an personenbezogenen Daten ab. Dies wird durch geringe Datenkompetenz und Zero-Rating-Angebote begünstigt, bei denen Mobilfunkanbieter den Kund:innen Tarife anbieten, welche die Nutzung von Meta-Diensten wie Facebook, Instagram und WhatsApp ermöglichen, ohne dass dies ihr Datenvolumen einschränkt. Viele ärmere Internetnutzer nut-

zen somit fast nur diese Dienste und können entsprechende Postings nicht durch Suchmaschinen und andere Quellen überprüfen. ANPD hat jedoch seit 2022 durchaus an Gewicht gewonnen. Brasilien orientiert sich nicht nur an der DSGVO, sondern neuerdings auch am AI-Act und dem DMA der EU (Carvalho/Iglesias 2025). Insofern ist der Brüssel-Effekt durchaus wirksam.

4.3 Datenschutz in Indien

Indiens Weg hin zu einer Datenschutzgesetzgebung begann am 24. August 2017, als sein Oberster Gerichtshof im spektakulären *Puttaswamy v. Union of India-Urteil* das Recht auf Privatsphäre als verfassungsmäßiges Grundrecht anerkannte. Nach vier Durchgängen von Gesetzentwürfen, in denen deren Inhalt immer mehr verwässerte, verabschiedete das Parlament 2023 schließlich die *Digital Personal Data Protection Bill* (*PDPB*). Diese letztliche Gesetzesfassung ist jedoch bislang nicht in Kraft getreten; die hierfür notwendig zu erlassenden Ausführungsvorschriften (*Rules*) wurden erst im Januar 2025 als Entwurf veröffentlicht. Es sind zudem noch die Ernennung einer Datenschutzkommission sowie Mechanismen für Audits und grenzüberschreitende Datenübertragungen erforderlich.

Das PDPB-Gesetz integriert zentrale Prinzipien des Datenschutzes, tendiert jedoch eher zu einer prozeduralen Regulierung und stützt sich nicht explizit auf ein zu schützendes Grundrecht. Es enthält DSGVO-ähnliche Bestimmungen zum Zugang, zur Berichtigung und Löschung persönlicher Daten sowie Verpflichtungen bezüglich Datenminimierung, Zweckbindung und Eingrenzungen bei der Speicherung. Eine explizite Begrenzung der Datensammlung und eine spezifische Kategorie für sensible Daten fehlen jedoch, stattdessen wird ein schwammiges Konzept des „deemed consent" (vermutetes Einverständnis) eingeführt.

Das finale PDPB-Gesetz verzichtet auf die Forderung nach Datenlokalisierung, die Indien lange international vorangetrieben hatte. Stattdessen sieht es die amtliche Benachrichtigung über eine Liste „vertrauenswürdiger Geografien" für Datenübertragungen vor. Die aktuellen Entwürfe von Ausführungsbestimmungen enthalten Regelungen, die bedeutsame Datenverarbeiter verpflichten können, bestimmte Kategorien persönlicher Daten lokal in Indien zu speichern (Rajmohan 2025).

PDPB enthält Klauseln, die der Regierung recht umfassende Befugnisse zum Zugriff auf persönliche Daten gewähren, auf Grundlage weit ge-

fasster Interessen wie nationale Souveränität, Sicherheit, außenpolitische Beziehungen und öffentliche Ordnung (Chapter IV, 17, 2(a) PDPB). Kritiker bemängeln, dass das Gesetz eher die Machtbefugnisse der Regierung stärke als den Individuen größere informationelle Selbstbestimmung zu verschaffen (Jhalani 2022). Man vermutet, dass einige Bestimmungen des PDPB vor dem Verfassungsgericht landen werden und die Regierung Modi sich lediglich Zeit habe kaufen wollen (Interviews Indien). Angesichts der bislang verabschiedeten PDPB-Regelungen dürfte Indiens Datenschutzrahmen größte Schwierigkeiten haben, die Angemessenheits-Standards der EU hinsichtlich des grenzüberschreitenden Datenverkehrs zu erfüllen.

Die indische Regierung entwirft eine eigenständige, techno-nationalistische Digital-Agenda, unterstützt durch *NITI Aayog* (*National Institution for Transforming India*) und den privaten Thinktank *Observer Research Foundation* (*ORF*), gegründet von der schwerreichen Ambani Familie. Indien distanziert sich von China und hat beispielsweise den Betrieb der App Tiktok verboten. Neben dem Datenschutz verfolgt Indien eine strategische Neuausrichtung im Bereich der digitalen Governance und strebt die Etablierung eines „Vierten Weges" in der Digitalpolitik an, der auf die Förderung digitaler öffentlicher Infrastrukturen (*digital public infrastructures, DPIs*) setzt und zielt damit auf eine globale Transformationsrolle im Rahmen von G20 und UN (Sharma et al. 2023).

4.4 Datenschutz in Südafrika

Die Entwicklung des Datenschutzes in Südafrika reflektiert einen breiteren Trend in Afrika. Seit 2001 haben 35 afrikanische Staaten Datenschutzgesetze verabschiedet. Regionale Abkommen wie die Konvention für Cybersicherheit und Datenschutz der Afrikanischen Union (Malabo-Übereinkommen) betonen die Bedeutung eines umfassenden Datenschutzes, jedoch haben noch nicht alle Mitgliedsstaaten das Übereinkommen ratifiziert (Access Now 2024). In der neuen Verfassung Südafrikas nach dem Ende der Apartheit wurde 1996 das Recht auf Privatsphäre (Artikel 2, Abs. 14) konstitutionell verankert.

Das Schutzgesetz für persönliche Daten (*POPIA- Protection of Personal Information Act*), verabschiedet 2013, wurde erst 2020 vollständig umgesetzt und die Durchsetzungsmaßnahmen im Jahr 2021 eingeleitet. Das Gesetz enthält zahlreiche Elemente, die an die DSGVO erinnern. Es hat allerdings die Besonderheit, dass auch personenbezogene Daten juristischer Personen

geschützt sind. Die Umsetzung wird durch den unabhängigen *Information Regulator*, so der Name der Datenschutzbehörde, überwacht. Im Haushaltsjahr 2022/2023 wurden 895 Beschwerden eingereicht; 68,8 % dieser Fälle wurden gelöst (Malinga 2023). Diese hohe Aufklärungsrate unterstreicht das Engagement dieser Behörde, insbesondere bei Verletzungsfällen in Regierungsstellen. Im Jahr 2023 verhängte die Datenschutzbehörde erstmals Bußgelder, vor allem gegen staatliche Organisationen wie Justizministerium, Bildungsministerium und Polizeibehörden, was auf erhebliche Mängel im Umgang mit persönlichen Daten hinweist (Information Regulator 2023). 2024 folgten weitere Ordnungsmaßnahmen, etwa gegenüber der Wahlkommission und dem Bildungsministerium (Mzekandaba 2024a).

Der Information Regulator befasst sich zunehmend auch mit US-Unternehmen, was seinen Willen zur Durchsetzung der Vorschriften gegen große Akteure im Datenökosystem verdeutlicht. So wurde WhatsApp wegen Doppelstandards bei der Datenverarbeitung zwischen Europa und Südafrika gerügt, wobei vor allem Metas Praxis, WhatsApp-Daten mit Facebook ohne Widerspruchsmöglichkeit seitens der Nutzer zu teilen, kritisiert wurde. Bereits im März 2021 hatte der Information Regulator einen Brief an Facebook Südafrika gesendet, im September 2024 folgte eine Vollstreckungsverfügung (Information Regulator 2021; Mzekandaba 2024b).

Der Information Regulator ist auf einem guten Weg, Datenschutz solide zu implementieren. Trotz positiver Entwicklung bestehen jedoch Herausforderungen wie etwa knappe Personalressourcen, mit nur 90 Mitarbeitenden bei einem Jahresbudget von rund 100 Millionen ZAR (4,8 Mio. EUR). Die Bewältigung von Verletzungen bei der Datensicherheit und die Steigerung der Compliance bleiben weiterhin zentrale Anliegen. Die geringe Datenschutz- und Privatsphäre-Kultur in der Bevölkerung erschwert die Kontrolleinsätze zusätzlich. Die Überwachung von Social-Media-Plattformen befindet sich noch im Anfangsstadium; die Bußgeldschwelle von maximal 10 Millionen ZAR (rund 482.000 EUR) erscheint unzureichend, um größere Tech-Firmen abzuschrecken. Zudem mangelt es am Austausch mit zivilgesellschaftlichen Organisationen, was Potenziale stärkeren aufklärerischen Engagements ungenutzt lässt.

4.5 Fazit zum Datenschutz

Datenschutzbehörden müssen sich mit zunehmenden technologischen Komplexitäten befassen, insbesondere im Bereich sozialer Netzwerke, KI

und automatisierter Entscheidungsprozesse. Relevante öffentliche Akteure, Wissenschaftler:innen sowie zivilgesellschaftliche Organisationen in den untersuchten Ländern bekunden ihre Wertschätzung gegenüber den digitalen regulatorischen Bemühungen der EU. Mehrere Länder des Globalen Südens orientieren sich an der EU im Bestreben, die Macht der Big Tech-Unternehmen (GAFAM) einzuschränken, Marktdiversität zu fördern und die demokratische Integrität zu schützen. Allerdings sind die Durchsetzungsfähigkeiten der lokalen Institutionen finanziell und organisatorisch begrenzt, und die politischen Prioritäten der jeweiligen Staaten liegen häufig auf anderen Feldern.

Zusammenfassend lässt sich festhalten, dass die DSGVO die Datenschutzgesetzgebung in den genannten Ländern maßgeblich beeinflusst hat, und somit ein de-jure-Brüssel-Effekt durchaus erkennbar ist. In der praktischen Um- und Durchsetzung der nationalen Datenschutzgesetze gibt es jedoch eine große Spannbreite. Mexiko hat mit INAI eine aktive Datenschutzbehörde aufgebaut, die jedoch jüngst von der Regierung unter Kuratel gestellt und mit dem Verlust der behördlichen Unabhängigkeit deutlich geschwächt wurde. Brasilien und Südafrika haben durchaus ernsthafte Schritte in der Durchsetzung von Datenschutz unternommen. Brasiliens ANPD richtet sich derzeit stärker im Hinblick auf KI-Regulierung aus. Südafrikas Information Regulator hat bisher vor allem Datenschutzverletzungen im öffentlichen Sektor im Fokus und konzentriert sich auf das Durchsetzen bestehender Regularien zur Bekämpfung von Korruption und zur Stärkung der Rechenschaftspflichten der Regierung.

Im Hinblick auf eine stärkere Regulierung der großen Tech-Plattformen sind die untersuchten Länder bisher eher zaghaft. Dies liegt mit daran, dass die administrativen Kapazitäten als unzureichend angesehen werden, da Beamte teils nicht gut genug ausgebildet sind oder Personal häufig fluktuiert. Auch die Furcht, hohe Kosten bei Rechtsstreits aufzuwerfen und ggf. gerichtlich zu unterliegen, spielt eine Rolle. Nicht zuletzt ist die Lobbymacht und das Drohpotential der Plattformen nicht zu unterschätzen, da einige Plattformen bei Auseinandersetzungen durchaus gedroht haben, ihre Dienste aus dem Land abzuziehen. Dass sie dies in die Tat umsetzen, erscheint sehr unwahrscheinlich, sind doch die Länder des Globalen Südens nicht nur bevölkerungsreich, sondern es befinden sich dort bei gesättigten Märkten in den Industriestaaten auch die nächsten Milliarden Kund:innen. Gleichwohl zeitigen diese Drohungen eine gewisse Abschreckungswirkung. Das geschilderte Beispiel der temporären Suspendierung von X in Brasilien zeigt jedoch, dass demonstrative Stärke und Beharren auf dem Rechtsstaat

auch gegenüber einem Elon Musk obsiegen kann. Der eigenen Bevölkerung indes den kostenfreien Zugang zu Metas Diensten (im Sinne des Zero-Rating beim Handy-Datenvolumen) streitig zu machen, wird sich wohl weder Brasilien noch eine andere Regierung trauen, auch wenn man dieses Zero-Rating als Verstoß gegen die Netzneutralität werten könnte. Hier wäre der breite Ausbau öffentlicher WLAN-Netze eine Alternative, um auch ärmeren Bevölkerungsschichten den Zugang zum Internet zu gewähren.

Südafrika pocht gegenüber den großen US-Plattformen darauf, dass in Europa durchgesetzte Regelungen auch in Südafrika Geltung erlangen, etwa bei Metas Zusammenführung von Daten von WhatsApp mit Facebook, darüber hinaus auch bei kartellrechtlichen Untersuchungen (CCSA 2023). Insofern scheint Südafrika den Brüssel-Effekt sogar aktiv einzufordern, indem es sich darauf beruft, die Plattformen sollten nicht mit Doppelstandards agieren, sondern das hohe europäische Schutzniveau auch in Südafrika anwenden.

In Indien hingegen scheint Datenschutz - bisher jedenfalls - eher eine Fassade zu sein, denn ein ernsthaftes Unterfangen. Allerdings verfügt Indien über eine wache und agile Zivilgesellschaft, die Digitalrechte einfordert, jedoch zunehmend unter repressiven Druck seitens der Regierung von Präsident Narendra Modi gerät. Indiens „vierter Weg" in der Digitalpolitik, vorgestellt im Rahmen seiner G20-Präsidentschaft im Jahr 2023, zielt darauf ab, digitale Infrastrukturen als öffentliches Gut (DPIs) weltweit zu fördern. Mittels der Zusammenarbeit mit dem Entwicklungsprogramm der Vereinten Nationen (UNDP 2024) und dem „Global Digital Compact" durch die UN im Jahr 2024 strebt Indien eine führende Rolle in einer multipolaren globalen Ordnung an. Die Bedeutung der DPIs wächst international, wobei durchaus Synergien mit den EU-Initiativen im Bereich Daten Governance und Data Act entstehen können (Dang et al. 2024).

5. Schlussfolgerungen für die EU Digital-Governance

Während die Datenschutzbehörden die Relevanz der EU-Regulierungen anerkennen, bilden diese dennoch nur einen von mehreren Referenzpunkten. Indien, Brasilien und Südafrika sind auch Mitglied der BRICS-Staaten und sehen in der Ausweitung zu BRICSplus Optionen für ein stärkeres eigenständiges Gewicht des Globalen Südens. Insgesamt beharren alle vier Staaten darauf, Datenschutz an den eigenen sozio-politischen Kontext anzupassen, statt ein einheitliches Modell europäischer Vorschriften wie der

DSGVO zu implementieren. So wird etwa ein „Recht auf Vergessenwerden" von der Zivilgesellschaft in vielen Ländern abgelehnt, da sie befürchten, dass korrupte Politiker dadurch sie belastende Informationen unzugänglich machen könnten.

Insgesamt sind unterschiedliche Prioritäten erkennbar: Während Indien eine innovative, globale digitale Rahmenordnung anstrebt, die gleichen Zugang zu Technologie fördert, konzentriert sich Südafrika auf die Durchsetzung datenschutzrechtlicher Vorgaben in einem Kontext von historisch bedingtem Misstrauen (sowohl innerstaatlich wie international), wie auch angesichts enormer sozioökonomischer Herausforderungen. Indien navigiert derzeit durch innenpolitische Spannungen hinsichtlich Überwachung, nationaler Sicherheit und technikbasierter Kontrolle. Das biometrische Aadhaar-Authentifizierungs-System, bei dem über 1,2 Milliarden Inder:innen registriert sind, bildet die Grundlage für weitere „Schichten" des *India Stack*, das digitale Zahlungssysteme und weitere digitale Anwendungen großflächig ausrollen will. Indien verfolgt damit das Ziel, internationale Anerkennung und Wertschätzung für seinen Ansatz der digitalen öffentlichen Infrastrukturen (DPIs) zu gewinnen (Sieker 2024; Sharma 2023).

Der geopolitische Kontext, geprägt durch Russlands Invasion in der Ukraine und Konflikte im Nahen Osten, hat die Staaten des Globalen Südens vom Westen distanziert und sie im BRICSplus-Verbund enger an China und Russland herangeführt. Diese Verschiebung könnte sich auf den digitalen Raum auswirken. Zudem gibt es durchaus auch einen „Beijing-Effekt", mittels dessen China versucht, über technische Infrastrukturen, Standards und internationale Foren seine Einflusssphäre auszudehnen (Erie/Streinz 2021; Recorded Future 2021). Und man könnte möglicherweise von einem „Washington-Effekt" sprechen, bei dem die aktuelle US-Regierung durch Ausweitung der Exekutivbefugnisse und Vergeltungsdrohungen die Durchsetzung von Regulierungen in der EU und anderen Ländern zu behindern sucht (The White House 2025; Chen 2025). Das im April 2025 begonnene Verhängen unilateraler Zölle seitens der US-Regierung gegen ihre Handelspartner weltweit, legitimiert als (protektionistischer) Schutz der US-Industrie, dient demnach vor allem als Druckmittel, um Länder zu Zugeständnissen zu zwingen. Mitte des Jahres 2025 verhandeln die USA mit über 70 Ländern über Handelsbelange. Die US-Forderungen betreffen sowohl die Rücknahme von Digitalsteuern als auch die Abschwächung von Digital-Regulierungen wie DMA, DSA und AI-Act. Sie dienen zudem als Faustpfand für den US-Handelsbeauftragten (*USTR*), um den globalen digitalen Handel zu liberalisieren, privatisieren und deregulieren. Big-Tech-

Unternehmen stellen die US-Zölle als marktkorrigierende Mechanismen dar, die wettbewerbsverzerrende Praktiken bestrafen sollten. Digitale Regulierungen werden somit als „nichttarifäre Handelshemmnisse" reframed, und Handelspolitik als ein strategisches Instrument ergriffen, um strategische Prioritäten von großen US-Digitalunternehmen weltweit voranzutreiben. Beim Begünstigen der US-Digitalplattformen geht es darum, Services ohne Betriebsstätte im Land anzubieten, grenzüberschreitende Datentransfers unreguliert zu erlauben, Datenzentren aufzubauen sowie Daten zu extrahieren und zu speichern, ohne Steuern im jeweiligen Land zu errichten (Nayyar 2025; Kilic 2025; Hingle 2025; Banga et al. 2025).

Der Brüssel-Effekt wird häufig nur aus europäischer Perspektive betrachtet, was Reminiszenzen an koloniale Attitüden wecken kann. Die Länder verlangen kooperative Partnerschaften und Dialog auf Augenhöhe. Während die Staaten des Globalen Südens zunehmend eigene digitale Governance-Modelle entwickeln, stehen sie vor spezifischen Herausforderungen und suchen an ihre jeweiligen Kontexte angepasste Lösungen. Der Einfluss der EU ist spürbar, aber keineswegs ein Selbstläufer. Mexiko ist ökonomisch eng mit den USA verbunden und hat es schwer, eigene regulative Ansprüche durchzusetzen. Staaten mit stärkeren wirtschaftlichen Verflechtungen zur EU tendieren eher dazu, deren Regelwerke zu übernehmen, wobei gemeinsame Werte bezüglich Demokratie und Menschenrechten eine wichtige Rolle spielen – insbesondere bei jüngeren Demokratien wie Brasilien und Südafrika. Die Unterstützung der EU beim Kapazitätsaufbau und Wissenstransfer zur Regulierungspraxis könnte diesen Ländern helfen, wirksame digitale Governance-Strukturen zu etablieren (Schneider 2025).

Abschließend besteht Forschungsbedarf, um Anu Bradfords These zu prüfen, wonach Big Tech-Plattformen ihre Plattform-Designs global an den hohen EU-Standards ausrichten („de facto Brüssel-Effekt"). Zum einen gibt es – jedenfalls anekdotische – Hinweise dafür, dass die Digitalunternehmen ihre Dienste durchaus im Hinblick auf den Datenschutz differenzieren und die hohen EU-Vorschriften nicht gleichermaßen überall anwenden. Zum anderen könnten sich paradoxerweise gerade *durch* die zunehmenden *nationalen* gesetzlichen Regelungen des Datenschutzes graduelle oder gar stark divergierende Abweichungen vom DSGVO-Standard ergeben, so dass Unternehmen dies ausnutzen, etwa geringere Datenverarbeitungsstandards anwenden oder mehr Daten erheben und an Dritte weitergeben. Hier bedarf es weiterer empirischer Forschungen, um die tatsächlichen Effekte und Wechselwirkungen zu verstehen.

Auf einer übergeordneten Ebene stehen Europa und der Globalen Süden vor ähnlichen Herausforderungen, wie zunehmende geopolitische Spannungen und Abhängigkeiten von global agierenden Tech-Unternehmen. Diese Entwicklungen betonen die Notwendigkeit, die digitale Souveränität zu stärken und eigene technologische Kapazitäten aufzubauen. Beispielsweise kann die öffentliche Beschaffung als ein Instrument genutzt werden, um unterschiedliche Anbieter und technologische Lösungen zu fördern. Im Rahmen öffentlicher Aufträge trägt dies dazu bei, Abhängigkeiten zu verringern, Innovationen zu fördern und den Wettbewerb zu stärken (FES 2024). Europa sollte den Dialog mit den Ländern des Globalen Südens intensivieren, die meist technikoptimistischer sind und danach streben, digitale Entwicklungssprünge zu machen sowie als wichtige Akteure auf der Weltbühne anerkannt zu werden. Im Austausch zu europäischen historischen Erfahrungen, etwa gezogene Lehren aus staatlicher Überwachung, kann dies dazu beitragen, Sensibilisierung und gegenseitiges Verständnis zu fördern. Europa muss anerkennen, dass die Prioritäten des Globalen Südens neben Sicherheitsfragen etwa die Verbesserung der Konnektivität, die Überbrückung der digitalen Kluft und die Förderung digitaler Inklusion umfassen, stets im Einklang mit den UN-Zielen für nachhaltige Entwicklung (SDGs) (G20 South Africa 2025; UNCTAD 2024). Der stärkere Impetus auf kollektive Rechte, Entwicklung und globale öffentliche Güter in diesen Regionen erfordert es, unterschiedliche Narrative, kulturelle Kontexte und drängende Anliegen zu berücksichtigen, um einen gemeinsamen Verständigungsraum zu schaffen.

Insofern reicht es nicht, auf den Brüssel-Effekt zu vertrauen, sondern die EU muss sich stärker nach außen orientieren, um ihre Position in der globalen Digital-Governance zu behaupten. Die EU sollte strategische Allianzen mit gleichgesinnten Ländern wie Brasilien, Indien, Südafrika, Mexiko, Kanada, Großbritannien, Japan und Australien schmieden, um ihre digitale Resilienz, Souveränität und globale Stellung zu stärken. Solche Allianzen sind von entscheidender Bedeutung für die Förderung einer wettbewerbsfähigen und nachhaltigen digitalen Wirtschaft, in der die Grundwerte, die Menschenrechte und die Rechtsstaatlichkeit geachtet werden. Im „Digitalen Kompass", der EU-Strategie bis 2030, wird anerkannt, dass die EU einen umfassenden und koordinierten Ansatz für den Aufbau digitaler Koalitionen und diplomatische Initiativen benötigt, um geopolitische Rivalitäten zu bewältigen (European Commission 2021, Kap.6; European Council 2022 und 2024). Dabei ist es wichtig, Grundrechte, offene und menschenzentrierte Technologien in Partnerschaften zu integrieren und gemeinsam

geteilte technologische Souveränität anzustreben, um machtstarke Einflussnahmen, Cyberangriffe und technologische Dominanz zu verhindern. Die EU hat mit den digitalen Regulierungsakten bereits bedeutende Vorbilder geschaffen, doch um ihre Glaubwürdigkeit als globales Referenzmodell zu wahren, muss sie diese Verordnungen konsequent umsetzen und ihre Position gegen Tech-Monopole stärken (Csernatoni 2025; von Thun et al. 2025; Schneider 2018; 2020; 2025). In der internationalen Zusammenarbeit ist eine feste Allianz zur Einhegung von Tech-Giganten notwendig, um den Einfluss aus den USA, China und Russland einzudämmen. Die EU sollte sich zudem aktiv gegen das Ausnutzen der Marktmacht der Tech-Konzerne stellen, um ihre demokratischen Werte und wirtschaftlichen Interessen zu sichern, statt zögerlich auf Konfrontation zu verzichten. Nur durch mutige Regulierung und Kooperation kann die EU ihre technologische Souveränität und ihren globalen Einfluss langfristig sichern.

Danksagung

Diese Forschung wurde vom Rahmenprogramm für Forschung und Innovation „Horizont 2020“ der Europäischen Union im Rahmen der Marie-Sklodowska-Curie-Fördervereinbarung Nr. 873119, PRODIGEES (Promoting Research on Digitalisation in Emerging Powers and Europe towards Sustainable Development) mitfinanziert. Die Autorin dankt allen Interviewpartner:innen sehr herzlich für ihre wertvollen Einblicke und Perspektiven. Teile dieses Artikels basieren in überarbeiteter Fassung auf Auszügen aus meinem englischsprachigen Policy Report für die spanische IE University (Schneider 2025).

Co-funded by
the European Union

Literatur

Alle angegebenen Webseiten wurden zuletzt am 29. Juni 2025 besucht.

Access Now (2024): *Strengthening data protection in Africa. Key issues for implementation*. URL: https://www.accessnow.org/wp-content/uploads/2024/01/Strengthening-data-protection-in-Africa-key-issues-for-implementation-updated.pdf

ANPD (Autoridade Nacional de Proteção de Dados) (15. Juli 2022): Instauração de procedimento de fiscalização, https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos/arquivos-processos-de-fiscalizacao-concluidos/serpro-x-drumwave-00261-001457_2022_84_documentos_publicos.pdf

— (20. Juni 2024a): *ANPD é formalizada como coordenadora do Sistema Nacional de Inteligência Artificial*. URL: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-formalizada-como-coordenadora-do-sistema-nacional-de-inteligencia-artificial

— (2. Juli 2024b): *ANPD determina que Meta suspenda uso de dados pessoais para treinamento da IA*.URL: https://agenciagov.ebc.com.br/noticias/202407/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta

— (2024c): *Balanço de 4 Anos, 11/2024*. URL: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/anpd-balanco-4-anos.pdf

— (23. Mai 2025): *Inteligência Artificial: ANPD publica nota técnica sobre decisões automatizadas*. URL: https://lefosse.com/noticias/inteligencia-artificial-anpd-publica-nota-tecnica-sobre-decisoes-automatizadas/

— (24. Januar 2025b): ANPD determina suspensão de incentivos financeiros por coleta de íris, URL: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-de-incentivos-financeiros-por-coleta-de-iris

AP (Associated Press) (2024): *Musk's X to be reinstated in Brazil after complying with Supreme Court demands*. 09.10.2024. URL: https://apnews.com/article/brazil-x-elon-musk-supreme-court-de-moraes-e32c4b4171e78cbe8994f53713a922f7

— (2025): *JD Vance rails against 'excessive' AI regulation in a rebuke to Europe at the Paris AI summit*. 11.02.2025. URL: https://apnews.com/article/paris-ai-summit-vance-1d7826affdcdb76c580c0558af8d68d2

Banga, Karishma; Beyleveld, Alexander und Munu, Martin Luther (2025): Trading away tax sovereignty? How trade rules shape taxation of the digital economy in Africa, *Journal of International Economic Law*, 28(1), S. 43–62, https://doi.org/10.1093/jiel/jgaf004

Banisar, David (28. Januar 2025): National Comprehensive Data Protection/Privacy Laws and Bills 2025. URL: https://ssrn.com/abstract=1951416

Belli, Luca und Zingales, Nicolo (2017): *Platform regulations: how platforms are regulated and how they regulate us*. FGV Brasil, URL: https://repositorio.fgv.br/items/d35abb4b-ed3c-467c-97c8-5c59710cc9c7

Belli, Luca und Doneda, Danilo (2022): Data protection in the BRICS countries: legal interoperability through innovative practices and convergence, *International Data Privacy Law* 13(1): ipac019, https://doi.org/10.1093/idpl/ipac019

Bendiek, Annegret und Römer, Magnus (2019): Externalizing Europe: the global effects of European data protection. *Digital Policy, Regulation and Governance* 21(1), S. 32-43.

Biden, Joseph (2023): Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, 30.10.2023, URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

Bioni, Bruno (2020): Memory of the LGPD, URL: https://www.observatorioprivacidade.com.br/en/memory/

Bradford, Anu (2019): *The Brussels Effect: How the European Union Rules the World*. Oxford University Press.

— (2023a): *Digital Empires*. Oxford University Press.

— (2023b): Europe's Digital Constitution, 6.9.2023, Verfassungsblog, https://verfassungsblog.de/europes-digital-constitution/

— (2024): The False Choice Between Digital Regulation and Innovation, *Northwestern University Law Review*, 118(2).

Bruegel (2024): Digital factsheet #4: A dataset on EU legislation for the digital world, Q3, 20.07.2024, URL: https://www.bruegel.org/dataset/dataset-eu-legislation-digital-world

CAIDP (2025): Artificial Intelligence and Democratic Values Report, https://www.caidp.org/reports/aidv-2025/

Carvalho, Daniel und Iglesias, Simone (2025): Brazil Took on Musk and Won. Now Lula Is Sharing Notes With Europe, Bloomberg, 03.02.2025, URL: https://www.yahoo.com/news/brazil-took-musk-won-now-100000060.html

CCSA (Competition Commission South Africa) (2023): Online Intermediation Platforms Market Inquiry, Final Report and Decision, July 2023, URL: https://www.compcom.co.za/online-intermediation-platforms-market-inquiry/

CERRE (Centre on Regulation in Europe) (2024): Global Governance for the Digital Ecosystems Project, URL: https://cerre.eu/global-governance-for-the-digital-ecosystems/

Chen, Brian J. (2025): The 'Washington effect' could decide the AI race, 23.06.2025, URL: https://www.koreatimes.co.kr/opinion/20250623/the-washington-effect-could-decide-the-ai-race

Cohen, Julie E. (2019): *Between Truth and Power: The Legal Constructions of Informational Capitalism*. New York, NY: Oxford University Press.

Csernatoni, Raluca (2025): The EU's AI Power Play: Between Deregulation and Innovation, 20.05.2025, URL: https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation

Dachwitz, Ingo und Hilbig, Sven (2025): *Digitaler Kolonialismus. Wie Tech-Konzerne und Großmächte die Welt unter sich aufteilen*. München: C.H. Beck

Dang, Vy; Bootwalla, Aliasger; Lynders, Eva Maria; Reiners, Wulf (2024): Synergising digital public infrastructure and digital commons for sustainable development: the governance of digital resources in India and the EU, URL: https://www.gatewayhouse.in/synergising-dpi-digital-commons/

Daros, Gabriel (30. Mai 2025): In a world first, Brazilians will soon be able to sell their digital data, URL: https://restofworld.org/2025/brazil-dwallet-user-data-pilot/

DW (25.Januar 2025): ANPD proíbe pagamento por coleta de íris no Brasil, Deutsche Welle, https://www.dw.com/pt-br/anpd-pro%C3%ADbe-pagamento-de-criptomoedas-por-coleta-de-%C3%ADris-no-brasil/a-71404849

Erie, Matthew Steven und Streinz, Thomas (2021): The Beijing Effect: China's 'Digital Silk Road' as Transnational Data Governance. *N.Y.U. J. Int'l L. & Pol* 54 (1).

European Commission (2020): Digital Compass: The European way for the Digital Decade, COM/2021/118 final, URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52021DC0118

— (2024): The future of European competitiveness – A competitiveness strategy for Europe, Draghi Report, 09.09.2024, URL: https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en

— (2021): Digital Compass: the European way for the Digital Decade, COM/2021/118 final, URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0118

European Council (2022a): 'Path to the Digital Decade': the EU's plan to achieve a digital Europe by 2030, URL: https://www.consilium.europa.eu/en/infographics/digital-decade/

— (2022b): EU Digital Diplomacy: Council Conclusions, Foreign Affairs Council, 18 July 2022**,** 11406/22.

— (2024): A digital future for Europe, URL: https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/

FES (Friedrich Ebert Stiftung) (2024): Policy Study: Time to build a European digital ecosystem, 09.12.2024, https://library.fes.de/pdf-files/bueros/bruessel/21688.pdf

Fischer, David (2022): The digital sovereignty trick: why the sovereignty discourse fails to address the structural dependencies of digital capitalism in the global south. *Z Politikwiss* 32, S. 383–402 (2022).URL: https://doi.org/10.1007/s41358-022-00316-4

Flach, Natália (14.März 2025): TikTok complies with Brazilian data authority ruling on minors, O Globo, URL: https://valor.globo.com/empresas/noticia/2025/03/14/tiktok-cumpre-decisoes-da-anpd-sobre-acesso-de-jovens.ghtml

G20 South Africa (2025): Speech by Minister Solly Malatsi During the Opening Ceremony of the Second G20 Meeting of the Digital Economy Working Group, 07.04.2025, URL: https://g20.org/g20-media/minister-solly-malatsi-during-the-opening-ceremony-of-the-second-g20-meeting-of-the-digital-economy-working-group/

GDPR Enforcement Tracker (2025), URL: https://www.enforcementtracker.com/

Glenny, Misha und Muggah, Robert (2025), Big Tech Is Part of Trump's Threat to the Global Order, Foreign Policy, 03.06.2025, URL: https://foreignpolicy.com/2025/06/03/trump-big-tech-companies-silicon-valley-threat-geopolitics-digital-sovereignty/

Golumbia, David (2024): *Cyberlibertarianism: The Right-Wing Politics of Digital Technology*. University of Minnesota Press.

Hingle, Audrey (15. Mai 2025): The Winners of Tariff Diplomacy: U.S. Tech Companies, URL: https://internet.exchangepoint.tech/the-winners-of-tariff-diplomacy-u-s-tech-companies/

Hobbs, Carla (2020): The EU as a digital regulatory superpower: Implications for the United States, URL: https://ecfr.eu/article/commentary_the_eu_as_a_digital_regulatory_superpower_implications_for_the_u/

Holzmann, Anna und Zenglein, Max (2019): Made in China 2025 - Wie weit China auf dem Weg zu globaler Technologieführerschaft bereits gekommen ist. Merics. URL: https://merics.org/de/studie/made-china-2025

Huitron, Ale (9. Mai 2025): INAI desaparece; Secretaría Anticorrupción y Buen Gobierno asume funciones, URL: https://www.infobae.com/mexico/2025/05/10/inai-desaparece-secretaria-anticorrupcion-y-buen-gobierno-asume-funciones/

Information Regulator (2021): Information Regulator to take further action regarding the WhatsApp privacy policy, 13.05.2021, URL: https://inforegulator.org.za/wp-content/uploads/2020/07/ms-20210513-WhatsAppPrivacyPolicy.pdf

Information Regulator (2023): Annual Report 2022 – 2023, URL: https://inforegulator.org.za/wp-content/uploads/2020/07/Information-Regulator-Annual-Report-2023-Compressed.pdf

Jhalani, Radhika (2022): India's Data Protection Bill: the hits and misses, 07.12.2022, URL: https://www.context.news/surveillance/opinion/indias-data-protection-bill-the-hits-and-misses

Jia, K., Chen, S. (2022): Global digital governance: paradigm shift and an analytical framework. *GPPG* 2, 283–305). URL: https://doi.org/10.1007/s43508-022-00047-w

Kilic, Burcu (27 Juni 2025): Between Tariffs and Tech: What Will Europe Choose? Bot Populi, URL: https://botpopuli.net/between-tariffs-and-tech-what-will-europe-choose/

Krempl, Stefan (29. Juni 2025): Brazil's Supreme Court: Digital platforms are liable for user contributions, URL: https://www.heise.de/en/news/Brazil-s-Supreme-Court-Digital-platforms-are-liable-for-user-contributions-10463575.html

Lilkov, Dimitar (2020): Made in China. Tackling Digital Authoritarianism. Martens Center for European Studies, URL: https://www.martenscentre.eu/wp-content/uploads/2020/06/paper_made-in-china-webversion.pdf

Malinga, Sibahle (2023): InfoReg resolves 70% of POPIA complaints, Johannesburg, 05 April 2023, URL: https://www.itweb.co.za/article/inforeg-resolves-70-of-popia-complaints/LPp6VMrByz4MDKQz

Mayring, Philipp (2022): *Qualitative Inhaltsanalyse*. 13. Auflage. Weinheim; Basel: Beltz.

Mazzucato, Mariana (2013). *The Entrepreneurial State: Debunking Public vs. Private Myths in Risk and Innovation*. London: Anthem Press.

Mzekandaba, Simnikiwe (2024a): POPIA violation lands education dept in hot water, 14.11.2024, URL: https://www.itweb.co.za/article/popia-violation-lands-education-dept-in-hot-water/KzQenvjynNyqZd2r

Mzekandaba, Simnikiwe (2024b): WhatsApp privacy policy fails POPIA compliance, says watchdog, 11.09.2024, URL: https://www.itweb.co.za/article/whatsapp-privacy-policy-fails-popia-compliance-says-watchdog/Gb3BwMWaV1ov2k6V

Nayyar, Abhineet (26 Juni 2025): Trump's Tariffs and the Big Tech Takeover, Bot Populi, URL: https://botpopuli.net/trumps-tariffs-and-the-big-tech-takeover/

Open.AI (2025): Ankündigung: The Stargate Project, URL: https://openai.com/de-DE/index/announcing-the-stargate-project/

Rajmohan, Karthika (23. Januar 2025): Data Localization: India's Tryst with Data Sovereignty, URL: https://www.techpolicy.press/data-localization-indias-tryst-with-data-sovereignty/

Recorded Future (2021): China's Digital Colonialism: Espionage and Repression Along the Digital Silk Road, 27.07.2021, URL: https://go.recordedfuture.com/hubfs/reports/cta-2021-0727.pdf

Reid, Jenni (2025): The EU could hit Wall Street where it hurts with its tariff response – the tech giants, CNBC, 4.2.2025, URL: https:/www.cnbc.com/2025/04/04/how-the-eu-could-target-us-big-tech-with-its-tariff-response.html

Rudl, Thomas (21. Mai 2025): US-Regierung drängt Staaten zur Zulassung von Starlink, netzpolitik.org, URL: https://netzpolitik.org/2025/globaler-sueden-us-regierung-draengt-staaten-zur-zulassung-von-starlink/

Schneider, Ingrid (2018): Bringing the state back in: Big Data-based capitalism, disruption, and novel regulatory approaches in Europe, in: Schneider, Ingrid; Rudinow Saetnan, Ann; Green, Nicola (Hrsg.): *The Politics of Big Data: Big Data, Big Brother?* New York: Routledge, S. 129-175.

— (2020). Democratic Governance of Digital Platforms and Artificial Intelligence? Exploring Governance Models of China, the US, the EU and Mexico. *JeDEM - EJournal of EDemocracy and Open Government*, 12(1), 1-24. URL: https://doi.org/10.29379/jedem.v12i1.604

— (2022): Das ferne Echo Europas: Plattformregulierung, Datenschutz und Digitalkultur in Mexiko, in: Bogner, Alexander; Decker, Michael; Nentwich, Michael; Scherz, Constanze (Hrsg.): *Digitalisierung und die Zukunft der Demokratie. Beiträge aus der Technikfolgenabschätzung.* Baden-Baden: Nomos.

— (2025): Policy Report "Reclaiming Digital Sovereignty: The EU's Role in the Geopolitics of Digital Governance", IE University, Center for the Governance of Change, 02/2025, URL: https://static.ie.edu/CGC/CGC_ReclaimingDigitalSovereignty_PolicyPaper.pdf

Sharma, Sharad; Ramanathan, Madhumitha; Iyer, Arun; Abraham, Vivek (2023): Digital Public Infrastructures: Lessons from India for a Thriving Data Economy, IE CGC, 11/2023, URL: https://static.ie.edu/CGC/12.%20ISPIRT%20-%20Digital%20Public%20Infrastructures%20(November%202023).pdf

Sieker, Felix (2024): Aadhaar and the rise of Digital Public Infrastructure in India, 13.11.2024, URL: https://www.reframetech.de/en/2024/11/13/aadhaar-and-the-rise-of-digital-public-infrastructure-in-india/

Staab, Philipp (2024): *Markets and Power in Digital Capitalism*. Manchester: Manchester University Press.

The White House (21. Februar 2025): Memorandum: Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties, URL: https:/www.whitehouse.gov/presidential-actions/2025/02/defending-american-companies-and-innovators-from-overseas-extortion-and-unfair-fines-and-penalties/

UNCTAD (United Nations Conference on Trade and Development) (2021): *Digital Economy Report 2021*. New York.

— (2024): *Digital Economy Report 2024*, Shaping an environmentally sustainable and inclusive digital future, UNCTAD/DER/2024.

UNDP (2024): UN Releases Universal DPI Safeguards Framework to Promote Safe and Inclusive Digital Public Infrastructure, 24.09.2024, URL: https://www.undp.org/press-releases/un-releases-universal-dpi-safeguards-framework-promote-safe-and-inclusive-digital-public-infrastructure

Villanueva Plasencia, Daniel (11. Januar 2023): $60 Million in fines from the INAI, URL: https://www.linkedin.com/pulse/60-million-fines-from-inai-daniel-villanueva-plasencia/

von Thun, Max, Riekeles, Georg und Kuzev, Pencho 2025: Doubling Down, not Backing Down. Defending the EU's Digital Sovereignty in the Trump Era, 28.02.2025, KAS, URL: https://www.kas.de/documents/d/guest/doubling-down-not-backing-down

Freiheit by Design in digitalen Infrastrukturen

Marit Hansen, Andreas Baur und Felix Bieker

Zusammenfassung
Digitale Infrastrukturen sind die Basis für die Digitalisierung. Von ihrer Gestaltung hängt der Grad der Freiheit von Individuen und Gesellschaft angesichts der technischen Evolution ab. Je größer eine Abhängigkeit von den Infrastrukturen ist, je größer die Abhängigkeiten und Ungleichgewichte innerhalb dieser sind und je weniger sich die Nutzenden ihnen entziehen können oder wollen, desto wichtiger ist ein faires Design, das insbesondere vor einem Machtmissbrauch schützt. In diesem Beitrag beschreiben wir die grundlegende Relevanz heutiger digitaler Infrastrukturen und erläutern, welche unerwünschten Effekte damit einhergehen. Im Mittelpunkt stehen Ansatzpunkte für die freiheitliche und demokratische Gestaltung digitaler Infrastrukturen.

1. Einleitung

„Freiheit in digitalen Infrastrukturen" – dieses Thema wählte die Plattform Privatheit für ihre Jahreskonferenz 2024. „Freiheit" wird in diesem Zusammenhang als Abwehr von ungerechtfertigter Machtausübung und Schutz vor Machtmissbrauch verstanden – eine Voraussetzung für individuelle Selbstentfaltung und kollektive Selbstbestimmung. Freiheit ist also zentral für die Grundrechte jeder Person und für unsere Demokratie.

Digitale Infrastrukturen sind das technische Rückgrat unserer Gesellschaft. Ohne das Vorhandensein von Infrastrukturen funktionieren weder Kommunikation noch Vernetzung in der digitalen Welt. Das betrifft nicht nur den individuellen elektronischen Austausch zwischen Menschen oder die Nutzung von Informations- oder Unterhaltungsangeboten, sondern Finanzwesen, Energieversorgung, Güteraustausch, Mobilität und der Gesundheitsbereich sind heute zu großen Teilen ohne digitale Infrastrukturen nicht denkbar.

Wie viel individuelle und kollektive Freiheit gelebt werden kann, hängt stark von der Gestaltung der digitalen Infrastrukturen ab. In diesem Beitrag zeigen wir, wie heutige digitale Infrastrukturen diese Freiheit gefährden, statt ihre Ausübung zu unterstützen. Analog zu den Prinzipien von „Datenschutz by Design" aus der Datenschutz-Grundverordnung (DSGVO) und „Security by Design" aus der Cyberresilienz-Verordnung schlagen wir vor, bei der Gestaltung von digitalen Infrastrukturen auch das Prinzip von „Freiheit by Design" als Richtschnur anzulegen.

Im Folgenden stellen wir digitale Infrastrukturen und ihre Problemfelder dar (2.), führen bestehende Ansätze aus dem Bereich der Infrastrukturstudien ein, die eine umfassende Analyse ermöglichen (3.), und zeigen Ansatzpunkte für die freiheitliche und demokratische Gestaltung digitaler Infrastrukturen auf (4.), bevor wir mit einem Ausblick aufzeigen, wie wir zu solchen Lösungen gelangen können (5.).

2. Digitale Infrastrukturen

Unter digitalen Infrastrukturen versteht man „netzartige sozio-technische Systeme, die verlässlich einen einheitlichen Satz von Leistungen anbieten, die von Interessierten als Grundlagen des menschlichen Zusammenlebens, als Eröffnung von Handlungsmöglichkeiten und als Schutz gegenüber Lebensrisiken genutzt werden können – wie für Kommunikation, Energieversorgung, Güteraustausch, Mobilität oder Unterhaltung".[1]

Larkin (2013, S. 329, eig. Übersetzung) hebt hervor, dass Infrastrukturen nicht nur Objekte oder Technologien sind, sondern „Objekte, die die Grundlage für das Funktionieren anderer Objekte bilden". Technologische Konzepte wie Interoperabilität und Standardisierung sind daher für das Funktionieren einer Infrastruktur zentral.

Die systemische und grundlegende Bedeutung von Infrastrukturen lässt sich nicht nur daran zeigen, dass sie andere Technologien ermöglichen, sondern auch, darin, dass sie darauf aufbauende Technologien und soziale Praktiken prägen und normieren. Ein besonderes Augenmerk auf die normsetzende und handlungsbeeinflussende Eigenschaft von Infrastrukturen haben DeNardis und Musiani (2016) mit dem Konzept der „*Governance by Infrastructure*" gelegt. Infrastrukturen werden dabei auch als Rohrleitungen unterhalb des Sozialen, oder, wie Star (1999) es ausdrückt, als „unsichtbare Arbeit" verstanden. Infrastrukturen entfalten eine ermöglichende, aber auch handlungseinschränkende Wirkung entlang den in ihr angelegten Normen und Werten (Values-in-Design-Ansatz).

Infrastruktur wirkt sich auf Praktiken und Nutzungen aus und kann so die bewusste Regulierung oder Steuerung durch vom Menschen geschaffene Technologie und deren Wirkungen über die Wirkung des Rechts hinaus verlängern. Infrastrukturen können deshalb auch als *frozen governance*

1 Aus dem Text der Plattform Privatheit zur Jahreskonferenz 2024, https://plattform-privatheit.de/p-prv/jahreskonferenzen/jahreskonferenz-2024.php.

verstanden werden, die sich in den Materialien, Technologien, Institutionen und Praktiken von Infrastrukturen niederschlagen und dadurch langfristig auf das Soziale wirken. Gleichzeitig geht das Verständnis von *frozen governance* nicht weit genug, da es davon ausgeht, dass es nur das intentionale oder klassische politische Regieren durch Technologie übersetzt oder verlängert wird, was unbeabsichtigte Wirkungen versteckt.

Diese Formen der Governance und Handlungsbeeinflussung lassen sich auch unter dem Schlagwort der infrastrukturellen Macht verstehen und analysieren. Macht wird hierbei nicht nur in einer direkten Weise verstanden, also im Sinne von *power to* und *power over. Power to* bezeichnet die eigenen Handlungsmöglichkeiten und *power over* die Möglichkeit, andere zu Handlungen zu zwingen oder an diesen zu hindern. Einem strukturellen, auf Foucaults Arbeiten aufbauenden Verständnis nach wird Macht auch dann ausgeübt, wenn bestimmte Handlungen, Wissen und Identitäten ermöglicht oder erschwert werden – also die Grundlagen dafür beeinflusst werden (Haugaard 2022).

Digitale Infrastrukturen wie Clouds ermöglichen nicht nur KI-Anwendungen, sondern sie bedingen und prägen die auf der Infrastruktur aufbauenden Technologien und legen fest, was überhaupt möglich ist (Rieder 2020). Es sind die Infrastrukturen selbst, die infrastrukturelle Macht ausüben, nicht nur die Unternehmen und Betreiber:innen dieser Technologien. Für van Dijck u. a. (2019) ist es vor allem die Möglichkeit, Standards zu setzen, Plattform- und Netzwerkeffekte sowie Zugriff auf die anfallenden Nutzungsdaten, die infrastrukturelle Macht ausmachen. Luitse (2024, eig. Übersetzung) betont den polit-ökonomischen Anteil von infrastruktureller Macht, da diese Infrastrukturen nicht nur die darauf aufbauenden Technologien und Gesellschaften beeinflussen, sondern durch „die Fähigkeit eine Einheit aus Rechen-Infrastrukturen, KI-Entwicklungspraxis, Diskursen und Governance-Prozessen zu formen, mit dem Ziel und Effekt die Marktmacht der Infrastruktur zu stärken."

Die vertikale Integration von Big-Tech-Unternehmen und vor allem großen Cloud-Anbieter:innen, die von Hardware über Rechenzentren, Cloud-Systemen, APIs und Software bis hin zu KI-Trainingsmöglichkeiten, Trainingsdaten und -modellen reicht, ist ein zentraler Faktor der infrastrukturellen Macht (Luitse 2024, 33).

Infrastrukturen und die Kontrolle über sie üben auch direkte Macht aus: zum Beispiel durch die Entscheidung darüber, wer die darüber angebotenen Leistungen erhält und wer dagegen das Angebot nicht oder nur

eingeschränkt nutzen kann. Dies kann explizit, aber auch durch implizite Hindernisse oder erschwerte Bedingungen geschehen.

Besonders relevant wird dies, wenn eine (digitale) Infrastruktur notwendig für die Teilhabe am (digitalen) Leben oder in der Gesellschaft ist. Nicht nur die unmittelbare Leistungserbringung (oder -versagung) spielt hier eine Rolle, sondern auch die Möglichkeit der Überwachung der Nutzenden in ihrem Verhalten. Als Grundregel kristallisiert sich heraus: Je weniger sich Nutzende der Infrastruktur entziehen können, desto mehr Daten können gesammelt und desto mehr Einfluss kann auf die Nutzenden ausgeübt werden.

Weil Infrastrukturen so grundlegend und systematisch bedeutsam sind, ist ihre Gestaltung und Ausprägung für demokratische und freiheitliche Gesellschaften von großer Bedeutung. Gerade aber diese Gestaltung ist wegen des grundlegenden Charakters sehr komplex: Sie können gestaltet und verändert werden; ein Re-Design von im Einsatz befindlichen Infrastrukturen ist jedoch aufwendig. Die Gestaltung von Infrastrukturen folgt ebenso wie ein etwaiges Re-Design erfahrungsgemäß nicht grundrechtlichen Erwägungen, sondern wird als von technischen Anforderungen geprägt konstruiert oder vor allem ökonomisch getrieben.[2]

Sicherheits- oder Datenschutzaspekte sind somit regelmäßig nachrangig bei der Gestaltung. Das zeigt sich beispielsweise in der Rückschau auf die Entwicklung des World Wide Web (WWW) in Bezug auf zahlreiche Sicherheitsprobleme: Berners-Lee als einer der wichtigsten Begründer des WWW verteidigte die Entscheidung, nicht gleich von Beginn mehr Sicherheit eingebaut zu haben, weil dies dem Ziel, eine für Entwickler:innen leicht bedienbare Plattform zu schaffen („eine Plattform zu schaffen, die Entwickler:innen vertraut ist und einfach zu nutzen"), entgegengestanden hätte (Leyden 2014, eig. Übersetzung). Demnach wurde in Kauf genommen, dass wichtige Eigenschaften und Funktionen wie Sicherheitsfeatures fehlten und so später ergänzt werden mussten, beispielsweise die Transportverschlüsselung in der Kommunikation zwischen Webbrowser und Webserver. Ein späteres Aufsatteln oder Nachrüsten von Eigenschaften oder Funktionen ist jedoch nicht immer einfach und in einigen Fällen schwierig, teuer oder sogar unmöglich.

2 So wurden Vorschläge zur vertrauenswürdigen Mobilkommunikation zwar in der wissenschaftlichen Diskussion aufgenommen, aber hatten keinen wirklichen Einfluss auf die Gestaltung der Mobilnetze (Federrath 1998).

Aktuell werden im KI-Bereich Infrastrukturen ausgebaut. KI basiert auf Cloud-Diensten, wird aber zunehmend selbst eine Infrastruktur für die Anwendungen unterschiedlicher Betreiber:innen. Diese Perspektive ist noch nicht ausreichend untersucht; dabei wäre es gerade zum jetzigen Zeitpunkt noch möglich und nach unserer Überzeugung auch erforderlich, bei KI-Infrastrukturen gestaltend einzugreifen.[3]

In der KI-Debatte wird häufig auf die Effizienz von KI oder durch diese zu erreichende Effizienzsteigerungen verwiesen. Dabei bleibt außer Acht, dass Effizienz kein Ziel an sich ist, und offen, was genau effizienter gestaltet wird und zu welchem Zweck. In den USA lässt sich aktuell verfolgen, wie unter dem Deckmantel von Effizienzsteigerungen demokratische und rechtsstaatliche Strukturen abgebaut werden. Demokratie und Rechtsstaatlichkeit sind jedoch nicht effizient. Sie sollen es auch nicht sein, sondern sie verteilen und kontrollieren Macht bewusst. Aushandlungen, Widerspruchsmöglichkeiten, Kontrolle und transparente demokratische Verfahren sind gerade nicht auf Effizienz ausgelegt, sondern wollen erreichen, dass nicht eine Gewalt oder eine Stelle unwidersprochen und ungeprüft ihre Ziele ohne Rücksicht auf andere Interessen und Normen durchsetzen kann.

Die Trump-Regierung setzt dabei auf den Abbau von Gewaltenteilung, Bürokratie, Verantwortlichkeit und Maßnahmen gegen strukturelle Diskriminierung (vgl. Teirstein 2025, Vought 2023). KI funktioniert als magische Effizienzmaschine, die zu besseren Ergebnissen gelangen und gleichzeitig Personal und Finanzmittel einsparen soll, wobei die gravierenden Umweltauswirkungen und durch sie verursachten wirtschaftlichen und sozialen Kosten ignoriert werden. Tatsächlich steht zu befürchten, dass Einsparungen und der Ersatz von öffentlichen Beschäftigten eher dazu führen, dass öffentliche Dienstleistungen aufgrund fehlenden Fachpersonals nicht mehr für darauf angewiesene Personen verfügbar sind (Hadgu/Gebru 2025).

Vor diesem Hintergrund stellt sich die Frage, wie (rechtliche und digitale) Infrastrukturen so gestaltet werden können, dass sie demokratische und freiheitliche Gesellschaften unterstützen und solchen Angriffen möglichst widerstehen können.

---

3 Die KI-Verordnung (KI-VO) enthält zahlreiche Regelungen für und Gestaltungsanforderungen an KI-Systeme. Damit greift die europäische Gesetzgebung gestaltend in den KI-Markt ein. Die KI-VO nimmt jedoch primär KI in Form von einzelnen Produkten in den Blick und adressiert die infrastrukturelle Perspektive allenfalls indirekt, beispielsweise in Bezug auf Risikobewertungen und Folgenabschätzungen.

Digitale Infrastrukturen formen die Bedingungen für das Leben in der digitalen Welt aus. Sie sind nicht naturgegeben, sondern werden von Akteur:innen aus Staat und Wirtschaft[4] entwickelt, aufgebaut und betrieben. Die Gestaltung ist daher auch keineswegs zufällig: Sie folgt überwiegend vorgegebenen, bewussten und unbewussten Design-Entscheidungen. Selbst wenn im Entwicklungsprozess nicht jede Design-Anforderung absichtsvoll unter Einbeziehen sämtlicher vorhersehbarer Folgen formuliert wird, werden von Entwicklungsteams ständig Entscheidungen zur Gestaltung getroffen. In diesem Sinne wird beispielsweise auch entschieden, ob und welche Voreinstellungen implementiert werden, ob etwas (und wenn ja, in welchem Rahmen) durch die Anwendenden oder die Endnutzenden konfigurierbar ist usw. Der Verzicht auf eine Implementierung einer Funktion oder einer Eigenschaft ist ebenfalls eine Gestaltungsentscheidung. Im Ergebnis bedeutet dies: Es gibt kein Nicht-Design.

Gleichzeitig sind Infrastrukturen im Alltag unsichtbar (s. auch Star 1999); erst durch eine Fehlfunktion, einen Glitch, werden sie sichtbar. Heutige digitale Infrastrukturen sind in den meisten Fällen funktionsfähig, jedoch, wie oben aufgezeigt, dysfunktional (s. auch Berlant 2016): Sie ermöglichen nämlich nicht eine gleichberechtigte Teilhabe aller Menschen, sondern sind verbunden mit Machterhalt und -erweiterung von Akteur:innen in Wirtschaft und Politik. Um die Infrastrukturen und ihre bereits in diesem Abschnitt benannten Dysfunktionalitäten sichtbar zu machen und sie zu analysieren, zeigen wir im folgenden Abschnitt bestehende Ansätze auf, die genau daran ansetzen.

3. Erste Analyseansätze

Für eine Untersuchung digitaler Infrastrukturen kann auf bestehende Ansätze der Infrastrukturstudien zurückgegriffen werden. Diese sind in Deutschland bisher noch nicht breit rezipiert worden, bieten aber zahlreiche Ansatzpunkte.

In den Infrastrukturstudien (z. B. Star 1999; Edwards u. a. 2009; Easterling 2014; Berlant 2016) wird mit den Perspektiven verschiedener Disziplinen die strukturelle Bedeutung von technischen Infrastrukturen untersucht.

4 Es können sich auch Projekte von einzelnen Personen, die keine kommerziellen Interessen haben, zu Infrastrukturen entwickeln. Üblicherweise lässt sich der zuverlässige Betrieb von Infrastrukturen jedoch nicht von Einzelpersonen gewährleisten.

Nach Berlant formt Infrastruktur die Gesellschaft; Easterling argumentiert, dass „einige der radikalsten Veränderungen in der globalisierten Welt nicht in der Sprache des Rechts oder Diplomatie geschrieben werden, sondern in […] infrastrukturellen Technologien" (2014, 15). Infrastrukturen sind in besonderem Maße handlungsnormierend, da sie durch Technologien und Praktiken, also ihre sozio-technische infrastrukturelle Form, soziale Handlungen, aber auch Wissen und Ressourcen steuern.

Oft werden wir uns Infrastrukturen erst dann bewusst, wenn sie nicht funktionieren (Star 1999). Aber wenn sie funktionieren, enthalten sie eine „systemische Logik und Logistik […]. Sie prägen die Art und Weise, wie wir leben und wie Gesellschaft organisiert wird" (van Dijck u. a. 2018, 9, eig. Übersetzung).

Science and Technology Studies erforschen das ko-konstitutive Verhältnis von Technik, im Speziellen auch Infrastrukturen, und Mensch/Gesellschaft: wie sie miteinander existieren und sich gegenseitig bedingen (z. B. Jasanoff 2004). Sie bauen auf Disziplinen wie der Techniksoziologie auf und ergänzen, z. B. durch Konzepte wie Latours *Akteur-Netzwerk-Theorie*, dass Technologien selbst als soziale Phänomene verstanden werden können (vgl. z. B. Bijker u. a. 1987; Felt u. a. 2017). Ansätze wie *Responsible Research and Innovation,* anwendungsbezogene Technikethik und *Constructive Technology Assessment* erforschen nicht nur, wie diese Zusammenwirkungen zu verstehen sind, sondern wie eine bessere und werteorientierte Gestaltung und Entwicklung von neuen Technologien aussehen kann (vgl. z. B. Rip u. a. 1995).

Die Fragen einer bewussten Gestaltung umfassender und ubiquitärer Infrastrukturen und vor allem KI-Infrastrukturen auf Systemebene sind bislang noch nicht beantwortet. Erste Ansätze finden sich zum Beispiel bei Musiani (2022), die die Prozesse der Einbettung von digitaler Souveränität in Infrastrukturen – *infrastructuring sovereignty* – untersucht. Infrastrukturen werden hierbei als prozessual und relational verstanden und nicht als fixe Artefakte, die außerhalb des Sozialen Handelns liegen. Dieses Verständnis von Infrastrukturen als Praktiken und Prozesse ermöglicht nicht nur, das Entstehen und Wirken von Infrastrukturen zu analysieren, zu verstehen und zu bewerten, sondern auch einzelne Ansatzpunkte für Einwirkungen und aktive Einbettung von Werten in die Prozesse, Praktiken und Technologien zu identifizieren und anzugehen.

Auch das Recht selbst kann auf verschiedene Arten als Infrastruktur betrachtet werden: Nach Byrne u. a. (2024, 1237f.) ko-konstituieren Rechtsnormen, -praxis und Institutionen *Legal Infrastructures* (rechtliche Infra-

strukturen). Diese *Legal Infrastructures* unterscheiden sich von anderen Arten von Infrastrukturen durch ihre normativen Eigenschaften: Recht konstruiert gesellschaftliche Infrastrukturen und hat dadurch eine inhärente Infrastrukturdynamik. Dabei kommt Recht auch eine soziale Ordnungsfunktion zu. Die *Legal Infrastructures* wirken konkret auf die Verteilung von *Affordances*, wie Macht, ein, da sie in anderen, materiellen, technischen oder sozialen Infrastrukturen eingebettet sind (Byrne u. a. 2024, 1241 u. 1243 f.).

In den bestehenden *Legal Infrastructures* wird also festgelegt, wie Macht innerhalb von Gesellschaften verteilt wird, welche Gruppen sie in welchem Maße ausüben und welche Gruppen ausgeschlossen werden. Dies ergänzt die vorwiegend individualistische Betrachtungsweise von Diskriminierungsdynamiken innerhalb des Rechts. Bei dieser von Individuen oder Gruppen ausgehenden Betrachtung wird oft von konkreten Fällen ausgegangen, in denen eine Diskriminierung bereits erfolgt ist. Aus den daraus ableitbaren strukturellen Gesellschaftsdynamiken, die bereits ausführlich untersucht wurden (vgl. Bieker/Hansen 2023b m. w. N.), lassen sich Schlussfolgerungen und Ansatzpunkte für die infrastrukturelle Ebene gewinnen.

Weiterhin können *Legal Infrastructures* als Praktiken betrachtet werden. Sie existieren nicht ohne soziale Auseinandersetzung mit ihnen. Recht konstituiert sich fortlaufend, Rechtsnormen müssen durch eine beständige Praxis aufrechterhalten werden, die ihr Legalität (Brunné/Tohope 2010) verleiht. Ein Ansatzpunkt hierzu ist auch die Frage, wie sich in Praktiken normative Strukturen und Anordnungen über Grenzen und Gemeinschaften hinweg (re-)produzieren. Aus infrastruktureller Sicht kommt dabei der Untersuchung, wie *Legal Infrastructures* das Teilen, Hinterfragen und Ausführen von Rechtsnormen ermöglichen, besondere Bedeutung zu, die sich nicht auf soziale Interaktionen beschränkt, sondern auch die verbundenen Ebenen rechtlich-technischer Integration betrachtet (Byrne u. a. 2024, 1242).

Für digitale Infrastrukturen bietet sich eine Betrachtung der Integration von Recht in Technik an. Problematisch ist hier in Hinblick auf By-Design-Ansätze, dass sie in der Praxis nicht (ausreichend) umgesetzt werden – trotz bestehender Rechtspflichten. Obwohl etwa Art. 25 DSGVO technikneutral formuliert ist, zusätzlich konkrete Hinweise auf Maßnahmen bietet und auf die unterschiedlichen Risiken individueller Datenverarbeitungen skaliert, ist die Vorschrift innerhalb der Wissenschaft und Praxis umstritten (vgl. Dewitte 2024). Ein Problem der Umsetzung liegt darin, dass Hersteller

von der DSGVO nicht adressiert werden und daher kein gesteigertes Eigeninteresse am Anbieten datenschutzfreundlicher Produkte haben. Während die datenschutzrechtlich Verantwortlichen im Prinzip die Möglichkeit haben, bei der Beschaffung von speziellen Produkten auf die Berücksichtigung des Art. 25 DSGVO zu drängen, unterbleibt zumeist ein Einfordern der Umsetzung des Datenschutzrechts, weil dies gar nicht innerhalb des eigenen Verantwortungsbereichs empfunden wird oder ohnehin unrealistisch erscheint.

Ein weiterer Ansatzpunkt für die rechtliche Analyse ist die Verknüpfung der Bereitstellung von physischer Infrastruktur mit Jurisdiktion. Dabei wird von verschiedenen Akteuren etwa der Bau von Straßen als Anlass zur Normsetzung genommen. Dies wurde in Hinblick auf (neo-)koloniale Kontexte untersucht (Cowan 2023, Rodiles 2022, Kwet 2022). Im Verhältnis zwischen den USA und der EU und anderen Regionen im Bereich von Cloud-Infrastrukturen, erfolgt ebenfalls eine Verknüpfung von Infrastrukturbereitstellung mit Jurisdiktion: Die USA haben mit dem US CLOUD Act umfassende Regelungen erlassen, die ihnen Zugriff auf die bei US-amerikanischen Unternehmen gespeicherte Daten einräumen, auch wenn dies durch den Zugriff auf die physische Infrastruktur regionaler Niederlassungen außerhalb der USA erfolgt.

4. Ansatzpunkte für demokratische und freiheitliche Infrastrukturen

Die europäische Gesetzgebung der letzten Jahre für den Digitalbereich ist durch einen risikobasierten Ansatz gekennzeichnet: Risiken sollen identifiziert, bewertet und ausreichend eingedämmt werden. Zum Eindämmen der Risiken wird der By-Design-Ansatz verfolgt. Dies zeigt sich beispielsweise in der DSGVO, die mit Art. 25 auf Datenschutz by Design und by Default setzt, aber auch in den jüngeren gesetzgeberischen Entwicklungen im Bereich der Cybersicherheit wie der NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) und dem Cyber Resilience Act (CRA, Cyberresilienz-Verordnung, Verordnung (EU) 2024/2847), der das Paradigma „Security by Design" verfolgt. Doch wie geht „Freiheit by Design"? Oder – sinnvoll weitergedacht – „Grundrechte by Design"?

Um eine grundrechtskonforme Gestaltung von Infrastrukturen zu erreichen, bietet sich eine Kombination verschiedener Ansatzpunkte an, die sich an unterschiedliche Akteur:innen und die Ausgestaltung der Technologien selbst richten. Einige der Ansatzpunkte gehen von Anwender:innen

aus, die Alternativen zu Big-Tech-Infrastrukturen suchen oder ergänzende Maßnahmen treffen müssen, um das von den diesen Infrastrukturen ausgehende Risiko ausreichend zu beherrschen. Entscheidend ist, inwieweit technische Standards so gestaltet werden, dass sie (grund-)rechtliche Anforderungen umsetzen oder unterstützen.

Zu diskutieren sind zudem (weitere) Regulierungen des grundlegenden Infrastrukturbereichs auf gesetzlicher Ebene. Derartige Regulierungen müssen jedoch auch durchgesetzt werden; hier muss besser gewährleistet sein, dass sich Infrastrukturanbieter:innen an die rechtlichen Vorgaben halten. Einige interessante Ansatzpunkte werden im Folgenden erläutert.

4.1 Selbstbestimmung und Reduzierung von Abhängigkeiten

Der Freiheitsbegriff ist unmittelbar verbunden mit Selbstbestimmung; eine Fremdbestimmung soll vermieden oder zumindest eingeschränkt sein. Dieses Konzept ist verwandt mit der digitalen Souveränität. Unter diesem Schlagwort sowie überlappenden Konzepten wie der technologischen, operationalen und Daten-Souveränität werden aktuell vor allem in Europa Maßnahmen zur Reduktion der Abhängigkeit von Big Tech diskutiert (z. B. Glasze u. a. 2022, Baur 2024, Baur 2025). Eine häufig angewandte Definition versteht unter digitaler Souveränität „die Summe aller Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rollen in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“ (Kompetenzzentrum Öffentliche IT 2017). Da der Begriff der digitalen Souveränität ein sehr schillernder ist, mit unterschiedlichen Definitionen und Anwendungen und in dem sich auch sehr widerstreitende Interessen wiederfinden, sind einige konzeptionelle Ergänzungen sinnvoll.

Der Begriff der Souveränität, an dem sich die digitale Souveränität bedient, stammt aus der politischen Theorie und kennt vor allem zwei Dimensionen: eine interne und eine externe. Die externe bezeichnet die Ordnung von Autoritäten und damit Abwehr ungerechtfertigter Einflussnahme meist mithilfe von staatlichen Territorien, während die interne die legitime Autorität innerhalb eines Staates definiert. Souveränität wurde erst durch Philosophen wie Rousseau auf demokratische Systeme und damit demokratisch legitimierte Machtausübung und Rechtstaatlichkeit erweitert.

Mit dem Argument der digitalen Souveränität können deswegen auch einer Abschottung und einer autoritären Organisation und Überwachung von Gesellschaften Vorschub geleistet werden, wie es zum Beispiel in

Russland unter dem Begriff des „souveränen Internets“ geschieht. Es ist deswegen wichtig, bei Initiativen zur Steigerung der digitalen Souveränität darauf zu achten, dass nicht nur staatliche Institutionen als Referenzpunkt genannt werden, sondern eben vor allem Gesellschaften und Individuen. Diese gilt es in ihrer Selbstbestimmung zu fördern und dabei nicht ihre Überwachung bzw. autoritäre Kontrollmechanismen und Abschottung voranzutreiben.

Digitale Souveränität im Sinne der Gesellschaft und der Individuen bedeutet, die Risiken ausreichend einzudämmen, die mit der Verarbeitung der Daten oder anderen Digitalisierungskomponenten verbunden sind. Dies betrifft insbesondere die Abhängigkeiten von der korrekten (und gewünschten) Funktionsweise von Hard- und Software und damit auch von Hersteller:innen, Zulieferer:innen oder Betreiber:innen. Es gilt, Klumpenrisiken zu vermeiden, beispielsweise Risikokonzentration aufgrund von zentralen singulären und nicht oder kaum auswechselbaren Komponenten. Zu den strategischen Zielen, die die öffentliche Verwaltung in Bezug auf digitale Souveränität verfolgt, gehören eine Wechselmöglichkeit, eine Gestaltungsfähigkeit und Einflussmöglichkeiten auf Anbieter:innen (IT-Planungsrat 2021).

4.2 Offene Standards und Transparenz

Offene Schnittstellen, Formate und Protokolle[5] unterstützen die Möglichkeit des Auswechselns von Komponenten auf der technischen Ebene. Dagegen erschweren proprietäre und nicht offengelegte Gestaltungen der Technik die für digitale Souveränität wünschenswerte oder gar erforderliche Interoperabilität und Interkonnektivität. Insoweit kommt auch den Open-Source-Entwicklungen eine große Bedeutung für digitale Souveränität zu. Dass Open Source das Potenzial für mehr Kontrolle, Einflussnahme und Beherrschbarkeit hat, ist keine neue Erkenntnis (Köhntopp u. a. 2000).

Da die Hauptverantwortung für Infrastrukturen im Allgemeinen und für digitale Infrastrukturen im Besonderen beim Staat liegt (vgl. Roßnagel 1997[6], Berlit 2011), kommt den Initiativen des Staats für digitale Souveräni-

5 Technische Schnittstellen, Formate und Protokolle sind mindestens ebenso relevant wie der eigentliche Code (Lessig 2001).

6 Roßnagel ging bereits 1997 davon aus, dass der Staat und das Recht nicht mehr in der Lage seien, im „immateriellen Sozialraum der Netze Gemeinwohlbelange durchzu-

tät der Verwaltung eine besondere Bedeutung zu. So hat beispielsweise das Land Schleswig-Holstein (2024) eine Open-Source-Strategie ausgearbeitet – das Land stellt allmählich seine Verarbeitung auf Open-Source-Komponenten um. Auf Bundesebene wirkt das Zentrum für Digitale Souveränität darauf hin, dass für die Verwaltung in Bund und Ländern Open-Source-Lösungen bereitgestellt werden (ZenDiS 2025). Dies geschieht unter anderem über die Plattform openCode.[7] Auch der IT-Planungsrat (2025) erkennt die Notwendigkeit von offenen Dokumentenstandards und offenen Kollaborationslösungen in der öffentlichen Verwaltung und fordert die Umsetzung in Deutschland bis 2027.

Das Konzept „Open Source" garantiert aus sich heraus noch nicht, dass es sich auch tatsächlich um einen korrekten Code ohne Schwachstellen handelt (Köhntopp u. a. 2000) – und schon gar nicht, dass der Code Werte-basiert ist. So hat die Konferenz der unabhängigen Datenschutzaufsichtsbehörden (2023) in ihrem Positionspapier zu Souveränen Clouds Open Source als Soll- und nicht als Muss-Kriterium aufgeführt; aus Sicht der Datenschutzkonferenz ist Open Source hilfreich für digitale Souveränität, aber keine notwendige Voraussetzung. Hinzu kommt, dass einerseits im Einsatz von Open-Source-Tools, andererseits im Entwicklungsprozess von Open Source heutzutage ebenfalls Abhängigkeiten bestehen, die Risiken mit sich bringen (instruktiv Seeger 2024). Besonders wichtig ist daher, in Anspruch genommene Produkte, Komponenten und Dienste durch (rechtskonforme) Alternativen ohne unverhältnismäßigen Aufwand auswechseln zu können.[8]

Generell spielt für die Produkt- und Systementwicklung und auch für die Wechselfähigkeit die technische Standardisierung eine wesentliche Rolle. Das Befolgen von technischen Standards ist in einigen Sektoren eine Pflicht, in anderen Bereichen zumindest angeraten. Für einen rechtssicheren Einsatz von Produkten und Systemen ist es hilfreich, wenn grund-

setzen und die Bürger zu schützen". Aufgrund der Schutzmöglichkeiten auf der Basis von Informationstechnik wandele sich die Erfüllungsverantwortung des Staates zu einer Strukturverantwortung. Der Staat werde seiner Schutzpflicht gerecht, wenn er Strukturen schaffe, „die seine Bürger befähigen, ihre Interessen in der Welt der Netze selbstbestimmt zu schützen". Es geht dabei weniger um einen Selbstdatenschutz, der die Last weitgehend auf die Schultern der Bürger:innen legt, sondern um die staatliche Rolle zur Befähigung der Betroffenen in Ergänzung zu einem Systemdatenschutz – auch und gerade im Sinne der digitalen Souveränität.

7 https://opencode.de/de.

8 Europäische Alternativen für digitale Produkte werden beispielsweise unter diesem Link gesammelt: https://european-alternatives.eu/ (Graf 2025).

rechtsrelevante Kriterien in technischen Standards berücksichtigt werden. Der Prozess der Erarbeitung technischer Standards ist üblicherweise von unternehmensübergreifenden ökonomischen Interessen getrieben. Jedoch müssen beispielsweise die von der Europäischen Kommission bei den Standardisierungsgremien CEN und CENELEC in Auftrag gegebenen Standards zur KI-VO auch die dort enthaltenen Anforderungen, die sich auf Grundrechte oder Energieverbrauch beziehen, berücksichtigen (Europäische Kommission 2023b).

Die Teilnehmenden in den Standardisierungsgremien stammen großenteils aus der Industrie. Auch wenn eine Teilnahme von Vertreter:innen aus der Zivilgesellschaft nicht ausgeschlossen ist, geschieht dies nur in geringem Umfang, schon weil der – üblicherweise unbezahlte – Zeitaufwand groß ist und internationale Reisen finanziert werden müssen. Aus denselben Gründen ist zurzeit auch die Beteiligung von Datenschutzaufsichtsbehörden an Standardisierungsinitiativen auf Einzelfälle begrenzt.

Weil technische Standards so einflussreich sein können, müssen sie und der Prozess der Erarbeitung gegen eine Manipulation geschützt werden. Die US-amerikanische Standardisierungsorganisation NIST (National Institute of Standards and Technology) hatte sich aufgrund einer zunächst unerkannten Einflussnahme des Geheimdiensts NSA (National Security Agency) im Bereich der Verschlüsselung gezwungen gesehen, eine bereits veröffentlichte Empfehlung für einen Krypto-Algorithmus zurückzuziehen (NIST 2014). Es ist generell wahrscheinlich, dass Geheimdienste versuchen, in vielen Standardisierungsgremien Einfluss zu nehmen (Rogers/Eden 2017). Abgesehen von möglichen Unterwanderungen der Standardisierungsprozesse sei betont, dass trotz des potenziell hohen Wirkungsgrads auf unsere Gesellschaft technische Normung nicht auf einer unmittelbaren demokratischen Legitimierung basiert – anders als bei parlamentarischen Entscheidungen über rechtliche Normen. Als Ansatzpunkte zur Verbesserung sollte diskutiert werden, wie gesellschaftliche Interessen, rechtliche Anforderungen und generell Risiken für die Grundrechte und Grundfreiheiten zuverlässig in den Standardisierungsprozessen behandelt und entsprechende Design-Entscheidungen dokumentiert werden können. Dass mehr Transparenz notwendig ist, zeigt sich auch daran, dass selbst die Ergebnisse der Standardisierung – also die technischen Standards, die umgesetzt werden sollen oder müssen – nicht generell frei und kostenlos zur Verfügung gestellt werden. Der EuGH hat mittlerweile in der Malamud-Entscheidung festgestellt, dass überwiegendes öffentliches Interesse

an der Verbreitung von harmonisierten europäischen Normen bestehen kann (EuGH-Urteil vom 05.03.2024 – C-588/21 P).[9]

Technische Standards für einzelne Komponenten in der Verarbeitung können in der Regel keinen rechtssicheren Einsatz garantieren; häufig kommt es auf den Einsatzkontext und die Einsatzumgebung an. Im Endeffekt muss der Verantwortliche sich selbst davon überzeugen, dass die rechtlichen Anforderungen eingehalten werden. Ein Faktor könnte dabei die Zertifizierung nach Art. 42f. DSGVO darstellen, auch wenn sie in der Praxis noch fast gar nicht vorkommt. Von den Datenschutzaufsichtsbehörden wird häufig eine Sofort-Bewertung der Datenschutzkonformität eines Produkts erwartet – am besten für alle möglichen Versionen und Konfigurationen. Dies ist unrealistisch, und Produktprüfungen gehören auch nicht zu den unmittelbaren Aufgaben der Datenschutzaufsicht, wofür sie zurzeit auch nicht ausgestattet sind. Diese Behörden unterstützen durchaus, in dem sie aufzeigen, welche Prüfpunkte Verantwortliche anlegen müssen, oder abstrakte Lösungen als Positivbeispiele skizzieren. Es ist aber so noch nicht gewährleistet, dass diejenigen Verantwortlichen, die sich an Recht und Gesetz halten wollen, ausreichende Hilfen erhalten. Nach Möglichkeit sollten die Verantwortlichen eine Situation vorfinden, in der es leicht ist, die rechtlichen Anforderungen zu erfüllen. Das gilt besonders für die Infrastrukturen, derer sie sich bedienen.

4.3 Moving Targets und Verantwortungsdiffusion angehen

Bisher schaffen es Big-Tech-Unternehmen, sich der Verantwortlichkeit durch Zeitverzögerung zu entziehen. Es werden Dienste angeboten, bevor Risiken identifiziert oder gar adressiert wurden, oft mit dem Hinweis bestehende Regelungen seien auf diese neuartige Technologie nicht anwendbar. Wenn sich Risiken in Schäden für betroffene Personen niederschlagen, werden diese zunächst abgestritten, bei wachsendem Druck kleine Änderungen umgesetzt, die die meist systemischen Ursachen nicht angehen. In etwaigen behördlichen oder gerichtlichen Verfahren werden Informationen nur langsam herausgegeben und im Anschluss auf ein ungünstiges Urteil nur minimale Änderungen vorgenommen oder argumentiert, dass diese be-

9 Die Standardisierungsorganisationen IEC und ISO wehren sich gegen den Informationszugang und haben beim EuGH Klage gegen die Europäische Kommission eingereicht (anhängige Rechtssache T-631/24, veröffentlicht am 17.02.2025, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:C_202500919).

reits erfolgt seien und das Urteil damit nicht mehr auf die aktuelle Situation anwendbar sei (Bieker/Hansen 2023a).

Unter den aktuellen wirtschaftlichen Bedingungen wird diese Verzögerungstaktik belohnt. Auch hier funktioniert das Vorgehen nach der Maxime „Move fast and break things": In der gewonnenen Zeit können die Anbieter:innen bereits Gewinne erwirtschaften und sich eine starke Position auf dem Markt verschaffen. Sie haben damit einen großen ökonomischen Vorteil, insbesondere gegenüber gründlicheren und – was leider keine Selbstverständlichkeit ist – rechtstreu orientierten Anbieter:innen, die sich an bestehende Regelungen anpassen.

Dies zeigt sich auch im Bereich der KI, in dem es insbesondere Microsoft und Amazon als großen Cloud-Dienstleistern gelungen ist, mit dieser für große KI-Modelle notwendigen Infrastruktur infrastrukturelle Macht aufzubauen und maßgebliche Anbieter zu werden, die zum einen die technische Recheninfrastruktur bereitstellen, aber auch von der Datenerhebung, der Modellerstellung und dem Training sowie dem Endkund:innenkontakt wichtige Aspekte der KI-Dienste in sich vereinen (Luitse 2024). Selbst große Betreiber von eigenen KI-Anwendungen sind auf ihre Recheninfrastruktur angewiesen.

Aus informationstechnischer Perspektive benennen Balayn und Gürses (2024) agile Entwicklungsumgebungen als Teil dieses Problems: Aktuelle KI-Angebote beruhten auf einer Vielzahl von Diensten unterschiedlicher Anbieter:innen, die Betreiber:innen zusammenklicken, sodass kurzfristig Änderungen vorgenommen werden können, aber eben auch ein hochkomplexes Gefüge unterschiedlicher Akteur:innen entsteht. Dabei hätten die Betreiber:innen meist keine große Machtposition gegenüber ihren Diensteanbieter:innen, sodass sie auch nur begrenzten Einfluss auf die Gestaltung der Prozesse und ihnen zugrundeliegenden Infrastrukturen hätten. Sie fordern, dass diese Entwicklungsumgebungen reguliert werden müssen, anstatt sich auf einzelne Technologien zu beschränken, wie bei der KI-VO.

Zwar gibt es mit der DSGVO bereits eine technikneutrale Regulierung, die sich allgemein auf Datenverarbeitungen bezieht. Baylan und Gürses stellen jedoch fest, dass diese bisher nicht erfolgreich darin war, den genannten Verzögerungstaktiken und dieser Verantwortungsdiffusion effektiv entgegenzutreten.

Auf der zeitlichen Ebene wäre es denkbar, den gerichtlichen Rechtsweg, wie es bereits im Wettbewerbsrecht nach § 73 GWG geregelt ist, in bestimmten Fällen auf den BGH zu begrenzen, damit europarechtliche Fragen nicht erst, wie üblich, nach mehreren Instanzenzügen durch den EuGH

vorab entschieden werden können und so schneller Rechtssicherheit für alle Beteiligten hergestellt wird. Für die Klärung wichtiger Grundsatzfragen mit weitreichenden und teilweise faktisch irreversiblen Auswirkungen auf die Realität, wie dies bei der Gestaltung von digitalen Infrastrukturen nicht selten ist, wäre ein Fast Track beim EuGH denkbar.

Bezüglich der Verantwortungsdiffusion ist ein großes Problem der DSGVO, dass diese nur Verantwortliche und Auftragsverarbeiter:innen kennt. Hersteller:innen oder Anbieter:innen, die keine eigenen Zwecke mit der Datenverarbeitung verfolgen, sondern nur Dienste oder Infrastrukturen bereitstellen, fallen nicht in den Anwendungsbereich der DSGVO. Dies hat der EU-Gesetzgeber in der KI-VO explizit anders geregelt. Insofern können Verantwortliche etwa durch die Verpflichtung von Anbieter:innen nach Art. 9 KI-VO ein Risikomanagementsystem zu betreiben, voraussichtlich leichter Informationen für ihre eigenen Risikobeurteilungen (etwa nach Art. 27 KI-VO, Art. 35 und 24 DSGVO) erhalten. Allerdings ersetzt dies eigenständige Verpflichtungen der Anbieter:innen nach der DSGVO nicht ausreichend und birgt ebenfalls Gefahren der regulierten Selbstregulierung (Bieker 2025).

4.4 Inzentivierung korrigieren und Infrastrukturen regulieren

Das Digitale-Dienste-Verordnung (Verordnung (EU) 2022/2065) bezieht die infrastrukturelle Perspektive insoweit ein, dass sehr große Online-Plattformen und Suchmaschinen (Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs)) besonderen Pflichten unterworfen werden. Ziel der Digitale-Dienste-Verordnung ist es, illegale oder schädliche Online-Aktivitäten sowie die Verbreitung von Desinformation über die Plattformen und Suchmaschinen zu verhindern. VLOPs und VLSEs sind dadurch charakterisiert, dass sie mehr als 10% der 450 Mio. Verbraucher:innen in Europa erreichen. Nach der Definition betrifft dies eine kleine Anzahl (2023: 19 (Europäische Kommission 2023a), bis zum 1. Quartal 2025 wurde die Liste der VLOPS und VLOSEs auf 25 Angebote erweitert[10]); Anbieter:innen von LLMs gehören bisher nicht dazu.

Es ist noch unklar, ob die Regelungen zur Plattformkontrolle ausreichen und sie sich effektiv durchsetzen lassen. Schließlich basieren bisherige

10 Aktuelle Liste der VLOPs und VLOSEs: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (Abruf am 09.05.2025).

Geschäftsmodelle zahlreicher Anbieter:innen darauf, die Aufmerksamkeit der Internet-Nutzenden und vor allem deren Klicks auf sich zu lenken. Belohnt werden gerade nicht die sorgfältige Recherche und die korrekte Darstellung, sondern unseriöses Gebaren mit extremen Darstellungen, die verfälscht oder auch vollständig erfunden sein können. Hier müsste in die Geschäftsmodelle des Ausspielens von Werbung im Internet eingegriffen werden, wenn man wirklich eine Änderung erreichen möchte – z. B. indem nicht schnelle Klicks monetarisiert werden können, sondern etwa Klicks auf korrekte, ausgewogen dargestellte und vor allem qualitätsgesicherte Inhalte, die länger Bestand haben,

Zusätzlich wären Möglichkeiten zur Gewinnabschöpfung denkbar, wenn ein:e Akteur:in nicht nachweisen kann, dass diese Gewinne auf rechtmäßige Art und Weise entstanden sind. Es könnten Fonds eingerichtet werden, die abgeschöpfte Gewinne an Geschädigte weitergäben. Hierzu sind noch keine detaillierten Ausarbeitungen bekannt; wir finden es aber lohnend, dies weiterzuverfolgen.

Monopole und umfassende Marktmachtkonzentrationen sollten kartellrechtlich angegangen und entflochten werden. Hierbei ist es wichtig, nicht nur einzelne Dienstleistungen und Sektoren getrennt zu betrachten, sondern die Netzwerk- und Abhängigkeitseffekte integrierter Infrastrukturen zu berücksichtigen. Problematisch hierbei sind, dass trotz der interessanten und richtigen Ansatzpunkte in der EuroStack-Initiative auch hier Forderungen nach einem Abbau ‚lähmender Regulierung' und nach mehr Konsolidierung in Europa laut werden (Caffarra u.a. 2025, S. 6 f.). Eine sinnvolle Antwort auf die Nachteile fehlender Regulierung und großer Machtkonzentration in anderen Märkten kann jedoch nicht in der Kopie dieses Ansatzes liegen.

Während die Datenschutz-Grundverordnung den Fokus auf die Verarbeitung personenbezogener Daten legt und die Digitale-Dienste-Verordnung primär die Plattformen und Diensteanbieter:innen in den Blick nimmt, können bei Freiheit by Design weitere wesentliche Aspekte eine Rolle spielen. So wird der Klimawandel massive Auswirkungen auf die Freiheit haben, wo auf der Erde noch Lebensbedingungen herrschen, die sich für Menschen eignen. Für die Entwicklung des Klimas sind wiederum der Energieverbrauch und die Energieproduktion von großer Bedeutung. Besonders der Hype um KI führt aktuell und künftig zu einem erheblich gesteigerten Bedarf an Energie (IEA 2025). Dies führt dazu, dass Big-Tech-Unternehmen für ihre KI-Angebote eigene Kraftwerke bauen und betreiben.

Die Entscheidung darüber, welche Risiken und Nebenwirkungen von der Gesellschaft in Kauf genommen werden, was die Energieversorgung angeht, treffen diese Unternehmen großenteils in Eigenregie. Bisher ist jedenfalls nicht absehbar, dass der Betrieb von Atomkraftwerken damit verbunden ist, sowohl die Betriebsrisiken ausreichend abzusichern als auch die Langzeitlagerung und -versorgung für die Brennstäbe zu garantieren.

4.5 Öffentliche Infrastrukturen fördern und vor Vereinnahmung schützen

Forderungen nach öffentlichen Infrastrukturen treffen häufig auf die Erwiderung, dass diese durch Diskriminierung, Zensur und Überwachung leichter politisiert und auch missbraucht werden können. Gerade die Entwicklungen in den USA seit Beginn der zweiten Amtszeit von Präsident Donald Trump (Teirstein 2025[11]) zeigen jedoch, dass auch private Anbieter nicht per se Schutz vor Politisierung und Vereinnahmung garantieren.

Wir beobachten außerdem eine falsche Dichotomie zwischen komplett privaten Infrastrukturen auf der einen Seite und solchen, die direkt der Regierung und Exekutive eines Landes oder politischen Ordnung unterstellt sind. Gerade Beispiele des öffentlichen Rundfunks und anderer öffentlicher Institutionen zeigen, dass Ordnungsprinzipien denkbar sind, die sich dieser Dichotomie entziehen. Deswegen muss der Zivilgesellschaft eine stärkere Rolle zukommen.

Darüber hinaus sind die oben genannten Prinzipien der Werte-orientierten Infrastrukturgestaltung und der By-Design-Ansätze wichtige Anker innerhalb der vernetzten Technologien, die einen Missbrauch und Umwidmung erschweren und damit besonders marginalisierte Gruppen schützt.

5. Ausblick

Angesichts der aktuellen geopolitischen Entwicklungen und des rasanten technischen Fortschritts verdienen die Forschung zu digitalen Infrastrukturen und die Ausarbeitung von Lösungsstrategien gegen Machtkonzentration in und durch Infrastrukturen sowie Machtmissbrauch durch Staaten oder Wirtschaftsunternehmen deutlich mehr Aufmerksamkeit. Für den

11 Mit Verweisen auf zwei Websites, die als „Project 2025 Tracker" die Schritte der Verfassungskrise der USA und ihre Transformation dokumentieren.

Bereich der Cybersicherheit ist das Problembewusstsein zwar in jüngerer Zeit gestiegen, und der europäische Gesetzgeber hat in Rechtsnormen wie der NIS-2-Richtlinie und der Cyberresilienz-Verordnung Anforderungen für mehr Sicherheit und Risikobeherrschung über die gesamte Lieferkette für Hardware und Software formuliert. Weitere Digitalrechtsakte der EU, von der DSGVO aus dem Jahr 2016 bis zur KI-VO aus dem Jahr 2024 nehmen das Risiko für die Betroffenen und ihre Rechte und Freiheiten in den Blick. Während die DSGVO diesen Risikobegriff vor allem in Bezug auf die Pflichten der Verantwortlichen (und der Auftragsverarbeiter:innen) anwendet, hat das Konzept seitdem eine Ausweitung in DDVO und KI-VO erfahren. Ob diese Skalierung entlang von weitgefassten Risikobegriffen eine Verbesserung für den Grundrechteschutz darstellt, bleibt abzuwarten (vgl. Bieker 2025).

Die Durchschlagskraft der DSGVO im Sinne der europäischen Grundrechte war bisher jedoch, gelinde gesagt, beschränkt. Insbesondere gegenüber Anbieter:innen von Produkten und Dienstleistungen im Bereich der digitalen Infrastrukturen fehlt es an der nötigen Umgestaltung. Der Aufbau von (europäischen) Alternativen zu etablierten Infrastrukturen verläuft bisher zögerlich. Angebote, die von Anfang an konform zu den rechtlichen Anforderungen – im Sinne von „Grundrechte by Design" – gestaltet wurden, hatten in der Vergangenheit nicht unbedingt einen Marktvorteil.

Der aktuelle Prozess einer geopolitischen Disruption rechtfertigt einen Paradigmenwechsel: Es ist jetzt nötiger als je zuvor, dass die bisherigen digitalen Infrastrukturen samt den damit verbundenen Abhängigkeiten auf den Prüfstand kommen, und bei der Entwicklung neuer Infrastrukturen die grundrechtlichen Kriterien berücksichtigt werden. Europa muss sich faire Infrastrukturen leisten wollen. Im Fall von KI kann dies bedeuten, dass dezentralisierte, spezialisierte, aufwendiger trainierte Systeme ausgewählt werden, statt auf große allgemeine Modelle zu setzen, die mit fragwürdigen Methoden entwickelt wurden.

So wie Technologien nie die alleinige Lösung für soziale Probleme sein können, so sind auch Infrastrukturen nie ausreichend zum Schutz vor einer anti-demokratischen Übernahme geeignet. Technische Infrastrukturen werden Demokratien nicht schützen. Werte-orientierte öffentliche Infrastrukturen sind eine notwendige Bedingung für eine stabile, inklusive und freiheitliche Demokratie, aber keine hinreichende für ihre Existenzsicherung. Anti-demokratischen politischen Kräften muss in Gesellschaft und Politik begegnet und entgegengetreten werden, Demokratie dort gelebt und stabilisiert werden.

Infrastruktur-Design darf nicht zufällig passieren. Es bedarf eines systematischen, partizipativen und inklusiven Ansatzes unter Beteiligung aller gesellschaftlich relevanter Gruppen, um Risiken zu erkennen, Lösungen mit ihren Vor- und Nachteilen zu diskutieren und sich auf ein Vorgehen zu verständigen – kurzum: Es bedarf einer verlässlichen Infrastruktur zur fairen Gestaltung von Infrastrukturen.

Danksagung

Dieser Beitrag wurde teilweise gefördert durch das Ministerium für Wirtschaft, Arbeit und Tourismus Baden-Württemberg im Rahmen des Projekts Datenplattform der KI-Allianz BW und vom Bundesministerium für Forschung, Technologie und Raumfahrt im Rahmen des Projekts Neue Datenschutz-Governance – Technik, Regulierung und Transformation (DatenTRAFO)

Literatur

Balayn, Agathe und Gürses, Seda (2024): Misguided: AI regulation needs a shift in focus. *Internet Policy Review*, https://policyreview.info/articles/news/misguided-ai-regulation-needs-shift/1796.

Baur, Andreas (2024): European Dreams of the Cloud: Imagining Innovation and Political Control. *Geopolitics*, 29(3), S. 796–820. https://doi.org/10.1080/14650045.2022.2151902.

Baur, Andreas (2025): European ambitions captured by American clouds: digital sovereignty through Gaia-X?. *Information, Communication & Society*, S. 1–18. https://doi.org/10.1080/1369118X.2025.2516545.

Berlant, Lauren (2016): The commons: Infrastructures for troubling times. *Environment and Planning D: Society and Space,* 34(3), S. 393–419.

Berlit, Uwe (2011): Staatliche Infrastrukturverantwortung für rechtssichere Kommunikation im Netz – rechtliche Rahmenbedingungen und Probleme, *JurPC Web-Dok.* 39/2011, Abs. 1–45.

Bieker, Felix (2025): Risikobewertung im EU-Datenrecht: Effektiver Grundrechteschutz oder Feigenblatt?, *EuDIR (4)*, S. 190–197.

Bieker, Felix und Hansen, Marit (2023a): Daten-Fairness als Daten-Gerechtigkeit by Design. In: Friedewald, Michael u. a. (Hrsg.): *Daten-Fairness in einer globalisierten Welt.* Nomos, S. 29–56.

Bieker, Felix und Hansen, Marit (2023b): Data Protection in 2033: Playing Whac-A-Mole with Injustices? *European Data Protection Law Review (EDPL),* 9(4), S. 399–408. https://doi.org/10.21552/edpl/2023/4/6.

Bijker, Wiebe E.; Hughes, Thomas P. und Pinch, Trevor J. (Hrsg.) (1987): *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA.: MIT Press.

Brunnée, Jutta und Toope, Stephen J. (2010): Legitimacy and Liability in International: An Interactional Account. Cambridge University Press, https://doi.org/10.1017/CBO9780511781261.

Byrne, William Hamilton; Gammeltoft-Hansen, Thomas und Stappert, Nora (2024): Legal Infrastructures: Towards a Conceptual Framework. *German Law Journal,* 24, S. 1229–1246.

Caffarra, Cristina; Fermigier, Stefane; Hidalgo, Agata; Lechelle, Yann; Parsons, Clark; Styma, Felix und Yen, Andy (2025): 'Deploying the EuroStack: What's Needed Now', 19. Mai 2025. https://eurostack.eu/wp-content/uploads/2025/06/eurostack-white-paper-final-19-05-25-3.pdf.

Cowan, Deborah (2023): Law as Infrastructure of Colonial Space: Sketches from Turtle Island. *AJIL Unbound,* 117, S. 5–10.

DeNardis, Laura und Musiani, Francesca (2016): Governance by Infrastructure In: Musiani, Francesca; Cogburn, Derrick L.; DeNardis; Laura und Levinson, Nanette S. (Hrsg.): *The Turn to Infrastructure in Internet Governance.* Basingstoke: Palgrave Macmillan, S. 3–21.

Dewitte, Pierre (2024): The Many Shades of Impact Assessments. *Technology and Regulation,* S. 209–253. https://doi.org/10.26116/techreg.2024.018. https://doi.org/10.26116/techreg.2024.018.

Easterling, Keller (2014): *Extrastatecraft: The Power of Infrastructure Space*. London, New York: Verso.

Edwards, Paul N.; Bowker, Geoffrey C.; Jackson, Stefen J. und Williams, Robin (2009): Introduction: An Agenda for Infrastructure Studies. *Journal of the Association for Information Systems,* 10(5), S. 365–374.

Europäische Kommission (2023a): *More responsibility, less opacity: what it means to be a "Very Large Online Platform" – Statement by Commissioner Breton.* STATEMENT/23/2452, Brüssel, 25.04.2023. https://ec.europa.eu/commission/presscorner/detail/sk/STATEMENT_23_2452.

Europäische Kommission (2023b): *Durchführungsbeschluss der Kommission vom 22.5.2023 über einen Normungsauftrag an das Europäische Komitee für Normung und das Europäische Komitee für elektrotechnische Normung zur Unterstützung der Unionspolitik im Bereich der künstlichen Intelligenz*, C(2023) 3215 final, sowie Anhänge I und II, https://ec.europa.eu/growth/tools-databases/enorm/mandate/593_de.

Federrath, Hannes (1998): *Vertrauenswürdiges Mobilitätsmanagement in Telekommunikationsnetzen.* Dissertation, TU Dresden, Fakultät Informatik, Februar 1998.

Felt, Ulrike; Fouché, Rayvon; Miller, Clark A. und Smith-Doerr, Laurel (Hrsg.) (2017): *The Handbook of Science and Technology Studies*. 4. Aufl. Cambridge: MIT Press.Glasze, Georg u. a. (2022): Contested Spatialities of Digital Sovereignty. *Geopolitics*, 28(2), S. 919–958. https://doi.org/10.1080/14650045.2022.2050070.

Graf, Constantin (2025): *Europäische Alternativen für digitale Produkte.* https://european-alternatives.eu/de.

Hagdu, Asmelash Teka und Gebru, Timnit (2025): Replacing Federal Workers with Chatbots Would Be a Dystopian Nightmare. *Scientific American*. https://www.scientificamerican.com/article/replacing-federal-workers-with-chatbots-would-be-a-dystopian-nightmare/.

Haugaard, Mark (2022): Foucault and Power: A Critique and Retheorization. *Critical Review*, 34(3–4), S. 341–371. https://doi.org/10.1080/08913811.2022.2133803.

International Energy Agency (IEA) (2025): *Energy and AI*, IEA, Paris. https://www.iea.org/reports/energy-and-ai.

IT-Planungsrat (2021): *Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung – Strategische Ziele, Lösungsansätze und Maßnahmen zur Umsetzung*, Version 1.0 Januar 2021. https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf.

IT-Planungsrat (2025): *Offene Austauschformate*. Beschluss 2025/06 vom 26.03.2025. https://www.it-planungsrat.de/beschluss/beschluss-2025-06.

Jasanoff, Sheila (Hrsg.) (2004): *States of Knowledge: The Co-Production of Science and the Social Order*. London: Routledge.

Köhntopp, Kristian; Köhntopp, Marit und Pfitzmann, Andreas (2000): Sicherheit durch Open Source? – Chancen und Grenzen. *Datenschutz und Datensicherheit (DuD)* 24(9), S. 508–513.

Kompetenzzentrum Öffentliche IT (ÖFIT) (2017): *Digitale Souveränität,* November 2017. https://www.oeffentliche-it.de/publikationen?doc=71579&title=Digitale+Souveränität.

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2023): *Kriterien für Souveräne Clouds.* Positionspapier vom 11. Mai 2023. https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kriterien-Souv-Clouds.pdf.

Kwet, Michael (2022): Digital Colonialism and Infrastructure-as-Debt. *University of Bayreuth African Studies Online,* S. 65–77. https://ssrn.com/abstract=4004594.

Land Schleswig-Holstein (2024): *Die Open Innovation und Open Source Strategie des Landes Schleswig-Holstein.* https://www.schleswig-holstein.de/DE/landesregierung/themen/digitalisierung/linux-plus1/Downloads/_dateien/open-source-strategie.pdf.

Larkin, Brian (2013): The Politics and Poetics of Infrastructure. *Annual Review of Anthropology,* 42(1), S. 327–343. https://doi.org/10.1146/annurev-anthro-092412-155522.

Lessig, Lawrence (2001): *Code Version 2.0.* Basic Books, New York. https://commons.wikimedia.org/wiki/File:Code_v2.pdf.

Leyden, John (2014): *Sir Tim Berners-Lee defends decision not to bake security into www.* The Register, https://www.theregister.com/2014/10/08/sir_tim_bernerslee_defends_decision_not_to_bake_security_into_www/.

Luitse, Dieuwertje (2024): Platform Power in AI: The Evolution of Cloud Infrastructures in the Political Economy of Artificial Intelligence. *Internet Policy Review,* 13(2). https://doi.org/10.14763/2024.2.1768.

Musiani, Francesca (2022): Infrastructuring Digital Sovereignty: A Research Agenda for an Infrastructure-Based Sociology of Digital Self-Determination Practices. *Information, Communication & Society,* 25(6). S. 785–800. https://doi.org/10.1080/1369118X.2022.2049850.

National Institute of Standards and Technology (NIST) (2014): *NIST Removes Cryptography Algorithm from Random Number Generator Recommendations.* 21.04.2014, https://www.nist.gov/news-events/news/2014/04/nist-removes-cryptography-algorithm-random-number-generator-recommendations.

Rieder, Bernhard (2020): *Engines of Order: A Mechanology of Algorithmic Techniques.* Amsterdam University Press. https://doi.org/10.2307/j.ctv12sdvfl.

Rip, Arie; Misa, Thomas J. und Schot, Johan (Hrsg.) (1995*): Managing Technology in Society: The Approach of Constructive Technology Assessment*. London: Pinter Publishers.

Rodiles, Alejandro (2022): Infrastructural Developmentalism and Its Many Types of Global Law: A Comparative Look at the UN Sustainable Development Goals and China's Belt and Road Initiative. *London Review of International Law,* 10, S. 367–390.

Rogers, Michael und Grace Eden (2017): The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures. *International Journal of Communication* 11, 802-823.

Roßnagel, Alexander (1997): Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger, *Zeitschrift für Rechtspolitik*, 26 ff.

Seeger, Martin (2024): Aktenzeichen XZ ungelöst – Haarscharf an einer Katastrophe vorbei? *Datenschutz und Datensicherheit (DuD),* 48(9), S. 589–594.

Star, Susan Leigh (1999): The Ethnography of Infrastructure. *American Behavioral Scientist,* 43(3), S. 377–391. https://doi.org/10.1177/00027649921955326.

Teirstein, Zoya (2025): Project 2025 was extreme. Trump's first 100 days have been even more radical. *Grist,* 30.04.2025. https://grist.org/accountability/project-2025-tracker-trump-environmental-policy-legal-constitutional-crisis/.

van Dijck, José; Poell, Thomas und Waal, Martijn (2018): *The Platform Society: Public Values in a Connective World*. New York: Oxford University Press.

van Dijck, José; Nieborg, David und Poell, Thomas (2019): Reframing Platform Power. *Internet Policy Review,* 8(2). https://doi.org/10.14763/2019.2.1414.

Vought, Ross (2023): Executive Office of the President of the United States of America, in: Dans, Paul und Groves, Steven (Hrsg.): A Mandate for Leadership – Project 2025, S. 43–67.

Zentrum Digitale Souveränität (ZenDiS) (2025): *Digitale Souveränität als Staatsaufgabe – Bausteine einer souveränen Digitalstrategie,* 02/2025. https://admin.zendis.de/wp-content/uploads/2025-02-Bausteine-souveraene-Digitalstrategie-LP21-Kurzfassung.pdf.

Ein offener Webindex: Anwendungen, rechtlicher Rahmen, Akzeptanz

Leopold Beer, Paul C. Johannes, Huda Koulani, Christian L. Geminn, Matthias Söllner und Stefan Voigt

Zusammenfassung
Ein frei zugänglicher europäischer offener Webindex (OWI) könnte als Grundlage für eine Vielzahl von Suchmaschinen dienen und das Entstehen neuer webdatenbasierter Anwendungen, einschließlich Systemen der künstlichen Intelligenz (KI), fördern. Damit würde ein solcher offener Index wesentlich zur Vielfalt in digitalen Märkten beitragen und Nutzern die Möglichkeit geben, zwischen verschiedenen Diensten zu wählen. Auf diese Weise würde der Index zum Pluralismus auf dem aktuell monopolisierten Suchmaschinenmarkt beitragen. Der OWI könnte auch für Innovationen im Bereich der KI von entscheidender Bedeutung sein, da er die notwendige Datenbasis für das Training und die Weiterentwicklung von Retrieval Augmented Generation (RAG) und anderen KI-Systemen schaffen würde. Der vorliegende Beitrag befasst sich mit dem rechtlichen Rahmen für einen solchen offenen Webindex und erörtert Herausforderungen. Nach einer Einleitung (1) wird zunächst das Potenzial eines offenen Webindex (2) und seiner Anwendungen dargestellt. Sodann werden die verschiedenen Akteure (3) erörtert und Anwendungsfälle (4) beleuchtet, darunter vertikale Suchmaschinen (4.1), das Training von Large Language Models (LLMs) (4.2), die Verbesserung lokaler Suchdienste (4.3), Business Intelligence und Analytics (4.4) sowie die Aufdeckung von Desinformation und Bot-Netzwerken (4.5). Chancen und Risiken für die Grundrechte und -freiheiten (5) werden besprochen, gefolgt von einem Überblick über die rechtlichen Anforderungen an einen OWI (6) in Bezug auf Datenschutz (6.1), digitale Dienste (6.2), Rechte des geistigen Eigentums (6.3) und künstliche Intelligenz (6.4). Erste Überlegungen zur Untersuchung von Akzeptanz und Vertrauen der Nutzer werden angestellt (7). Abschließend werden die Erkenntnisse zusammengefasst und ein Ausblick in die Zukunft gegeben (8).

1. Einleitung

In der digitalen Welt zu navigieren, ist ohne Suchmaschinen kaum möglich. Ihre Nutzung wird als vermeintlich kostenlose Dienstleistung angeboten, die sich durch die Auswertung von Nutzerdaten nicht nur finanziert, sondern auch eine immense Gewinnschöpfung ermöglicht.[1] Zunehmend werden Suchmaschinen jedoch durch LLM-basierte Systeme (Large Lan-

1 Alphabet erwirtschaftete laut eigenen Angaben (https://abc.xyz/investor/) im ersten Quartal 2025 einen Gesamtumsatz von 90,23 Milliarden US-Dollar, wovon 50,7 Milliarden US-Dollar auf den Bereich Google Search entfielen. Der Nettogewinn des Konzerns betrug in dem Zeitraum 34,54 Milliarden US-Dollar. Der Nettogewinn für das Segment Google-Suche ist nicht separat ausgewiesen.

guage Models), die auf künstlicher Intelligenz basieren, ergänzt oder ersetzt. Diese Systeme, die in verschiedene Dienste integriert werden, bieten eine intuitivere Schnittstelle für die Recherche zu verschiedenen Themen. Dennoch greifen auch diese LLM-basierten Systeme letztlich auf die Daten und Strukturen von Suchmaschinen zurück, um ihre Antworten zu generieren und zu optimieren.

Mit dem Ziel, die Funktionalität und die Dienstleistungsqualität sicherzustellen, erfassen und verarbeiten Anbieter vieler Suchmaschinen und LLMs große Mengen personenbezogener Daten, aus denen vielfältige Rückschlüsse auf Interessen und Lebensumstände der Nutzenden möglich sind. Gerade die individualisierte Werbung wird in der Folge zu einer zentralen Einnahmequelle. Hinzu tritt die Möglichkeit zur Monetarisierung der Anzeigereihenfolge von Suchergebnissen (z. B. durch an erster Stelle präsentierte Anzeigen oder eine bezahlte Besserstellung in der Anzeigereihenfolge). Die daraus resultierenden Probleme haben die Google-Gründer Brin und Page bereits Ende der 90er Jahre selbst benannt und vorausgesagt: „[W]e expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers."[2] In anderen Worten: „[T]he search engines we have are not neutral or benevolent. They determine what data to collect from us and how to use it in algorithms. They are not open and transparent. So, it is hard to spot any bias or manipulation. They profile us. They divide us. This is not the search we want. We need search algorithms tuned for humanity, not individual greed."[3]

Alle Suchmaschinen basieren auf einem sogenannten Webindex, den man sich wie die Kartei einer Bibliothek vorstellen kann, nur eben um ein Vielfaches größer und viel dynamischer. Das Internet muss ständig nach neuen oder geänderten Inhalten durchsucht werden, damit diese über eine Suchmaschine abgerufen werden können. Dies erfordert eine hohe Rechenleistung und große Speicherkapazitäten, was die Erstellung und den Betrieb eines Webindex komplex und kostspielig macht. Neue Suchmaschinen haben es daher schwer, sich zu etablieren. Zwar gibt es alternative Suchanbieter wie Ecosia oder DuckDuckGo, diese benötigen aber in der Regel Zugriff auf einen oder sogar mehrere bestehende Webindizes und

2 *Brin/Page*, Anatomy of Large-Scale Hypertextual Web Search Engine, Computernetzwerke und ISDN-Systeme 1998, S. 107.

3 *Smith*, 2023.

entsprechenden Rankings. Dabei müssen sie sich den Bedingungen des Betreibers unterwerfen.[4]

Bislang gibt es weltweit nur vier umfassende Indizes des Internets: Google, Microsoft (beide USA), Baidu (China) und Yandex (Russland). Diese Anbieter diktieren die Bedingungen für den Zugang zu ihren Indizes und nehmen damit die Rolle von Torwächtern (Gatekeeper) auf dem Suchmaschinenmarkt ein. Das schränkt die Wahlmöglichkeiten der Verbraucher ein. So können Nutzende beispielsweise keine besonders datenschutzfreundlichere Suchmaschine wählen. Datenschutz und andere Belange der Privatsphäre, denen in der Europäischen Union (EU) besondere Bedeutung beigemessen wird, dürften bei den Gestaltungsentscheidungen für bestehende Indizes aufgrund des Sitzes der jeweiligen Unternehmen eine untergeordnete Rolle spielen. Durch die jetzige Ausgestaltung der vorherrschenden Suchindizes und das Fehlen von datenschutzfreundlichen Wettbewerbern kann das Grundrecht auf Privatsphäre und Datenschutz von den Nutzenden der Suchmaschinen kaum effektiv wahrgenommen werden. Das umfangreiche Sammeln und Auswerten von Nutzerdaten durch Suchmaschinen[5] erfüllt das Bedürfnis nach Privatsphäre[6] der Bevölkerung keinesfalls.

Der Marktanteil von Googles Suchmaschine in Deutschland liegt derzeit bei rund 90 %;[7] der weltweite Marktanteil auf allen Geräten (Desktop und mobil) beträgt 89,6 %.[8] Einer der Hauptgründe für diese Dominanz ist der über Jahrzehnte aufgebaute Webindex von Google. Ein Blick auf den Marktanteil von Microsofts Suchmaschine Bing (weltweit: 4,0 %[9]) zeigt jedoch, dass ein hochwertiger Webindex nicht der einzige Faktor für die Dominanz von Google in diesem Bereich sein kann. Vielmehr spielen auch Gewöhnungseffekte, Vertrauen,[10] Benutzerfreundlichkeit, andere angebundene Dienste, Voreinstellungen, Hindernisse beim Wechsel auf ande-

4 Z.B. basiert die deutsche Suchmaschine Ecosia auf dem Index von Bing.
5 Ein Blick in Google's Datenschutzerklärung (abrufbar unter https://policies.google.com/privacy?hl=de#infocollect) zeigt die umfangreiche Erhebung personenbezogener Daten durch das Unternehmen, etwa von Sprach- und Audiodaten oder Standortdaten.
6 *Braun/Trepte*, Privatheit und informationelle Selbstbestimmung, 2017, S. 6.
7 *StatCounter*, Marktanteile der führenden Suchmaschinen in Deutschland, 2024.
8 *StatCounter*, Marktanteil der führenden Suchmaschinen weltweit, 2025.
9 *StatCounter*, Marktanteil der führenden Suchmaschinen weltweit, 2025.
10 *Schultheiß/Lewandowski*, Misplaced trust?, Journal of Information Science 2021.

re Suchdienste und die subjektiv empfundene Qualität der Dienste eine wichtige Rolle.[11]

Ein offener, frei zugänglicher und großmaßstäbiger Webindex könnte dazu beitragen diese Probleme lösen, indem er anderen Suchmaschinenbetreibern als Grundlage für die Bereitstellung ihrer Dienste dient und so das Entstehen neuer, nutzer- und datenschutzfreundlicherer Suchmaschinen fördert.[12] So könnte ein offener Index einen wichtigen Beitrag zur Vielfalt und Wahlfreiheit im Bereich der Internetsuche leisten. Crawling und Indexierung würden vom eigentlichen Betrieb der Suchmaschine getrennt werden. Kleine und aufstrebende Anbieter können sich den Aufbau und Betrieb eines eigenen Indexes meist nicht leisten; ein offener Webindex würde ihnen langfristig eine Perspektive bieten. Der offener Webindex könnte auch für Wissenschaft und Forschung zugänglich gemacht werden. Darüber hinaus wäre ein solcher Index in hohem Maße innovationsfördernd für den Bereich der Künstlichen Intelligenz, da er die notwendige Datenbasis für das Lernen, Trainieren und Weiterentwickeln von Retrieval Augmented Generation (RAG) und anderen KI-Systemen schaffen würde. Insbesondere die aktuelle Entwicklung großer KI-basierter Sprachmodelle (z.B. ChatGPT von OpenAI/Microsoft oder Gemini von Google) unterstreicht die hohe Relevanz umfassender und qualitativ hochwertiger vorgefilterter Web-Datenbanken, wie sie ein offener Webindex bieten würde. Solche Datenbanken sind sowohl für die digitale Wirtschaft als Ganzes als auch für den Suchmaschinenmarkt der Zukunft im Besonderen von größter Bedeutung.[13]

Möglich wäre das alles nur durch eine kollaborative Anstrengung, bei der viele Institutionen bei Crawling und Indexing sowie bei der Bereitstellung und Pflege des Index zusammenwirken. Sogar *Brin* und *Page* betonten anfangs die Vorteile eines kollektiven Zusammenwirkens, bevor sie mit Google Search eine zentralisierte und profit- und werbegetriebene Lösung etablierten. Ein offener Web-Index könnte die Websuche revolutionieren: „[…] presenting the results from querying that index could be done completely unfiltered – simply clustered by source such as researched and

11 *Liaw/Huang*, An investigation of user attitudes toward search engines, Computers in Human Behavior 2003, 751.

12 *Lewandowski*, in: König/Rasch (Hrsg.), Reflections on Web Search, 2014, S. 49; *Lewandowski*, The Web is missing an essential part of infrastructure, Communications of the ACM 2019, 24.

13 *Wilson*, Microsoft Bing vs. Google Bard, 2023.

reviewed, mainstream media, social media trends, independent content. And you could have the controls to dive in and explore and filter by any criteria you chose – rather than being blinkered to a subset prepared to match you. And the rating from various fact checker organizations could be used to red-flag content. The validated would no longer get submerged under the popular. Fact would be distinct from fiction. That would be revolutionary."[14] Ein wirkmächtiges Instrument der informationellen und kommunikativen Selbstbestimmung könnte entstehen, das zugleich dem strategischen Ziel der Stärkung von Demokratie und Gesellschaft dient. Eine offene Suchinfrastruktur ermöglicht es, den gerade in Suchmaschinen präsenten Möglichkeiten der Kontrolle und Überwachung zu begegnen.

Die Etablierung eines offenen, europäischen Web-Index würde zudem einen wesentlichen Beitrag leisten, Standortnachteile für Deutschland und Europa abzubauen und wäre ein wichtiger Schritt hin zur Realisierung von digitaler Souveränität. Zugleich würde die dadurch ermöglichte Pluralisierung des Marktes für Suchmaschinen Privatheit und Datenschutz stärken, sofern sichergestellt würde, dass die Gestaltung der entstehenden Suchinfrastruktur an der bestmöglichen Verwirklichung von Grundrechten und -prinzipien sowie des geltenden Datenschutzrechts ausgerichtet würde. Diese Pluralisierung würde zudem die individuelle Handlungsfreiheit der BürgerInnen fördern und die Qualität der Internetsuche insgesamt verbessern: „When geographic map data was opened, competition ensured we got the better road navigation systems we all love in our cars. So similarly now, we need to open the web map data, the search indexes, so that competition can get us better web navigation systems."[15] Diese erwünschten positiven Auswirkungen auf Privatheit und Selbstbestimmung können sich aber nur entfalten, wenn sie eine Unterstützung erfahren, die sowohl eine Ausrichtung an Grundrechten und am einfachen Datenschutzrecht als auch Fragen der Nutzerakzeptanz neuer Technologien betrifft. Insgesamt wäre ein offener Web-Index ein wichtiger Schritt, um im zentralen Bereich der Internetsuche Informationelle Selbstbestimmung als langfristigen Wettbewerbsvorteil und Katalysator für Innovationen zu stärken.

Die Aussagekraft von im Kontext der Internetsuche anfallenden Daten und die daraus resultierenden Bedrohungen von Privatheit und Selbstbestimmung soll ein Beispiel illustrieren:[16] Im Jahr 2006 veröffentlichte die

14 *Smith*, 2023.
15 *Smith*, 2023.
16 Beispiel entnommen aus *Geminn*, Deus ex machina?, 2023, 25.

Forschungsabteilung des Internetanbieters AOL eine Textdatei, die Suchanfragen der unternehmenseigenen Suchmaschine über die AOL Client Software enthielt. Enthalten waren die Anfragen von 657.000 U.S.-Amerikanern über einen Zeitraum von drei Monaten (März bis Mai 2006), wobei deren Identität durch zufällig generierte Zahlen ersetzt wurde. Die Suchanfragen betrafen die Interessen und Sorgen der Nutzer, und dabei auch dunkle Facetten der Persönlichkeit; so fanden sich auch zahlreiche Anfragen zu Suizidmethoden oder etwa auch solche wie „how to kill your wife". Die New York Times deckte in der Folge anhand der Suchanfragen die Identität von Nutzerin Nr. 4417749 auf; es handelte sich um die damals 62-jährige Thelma Arnold aus Gilburn, Georgia. Die Identifizierung war in diesem Fall besonders einfach, denn die Nutzerin hatte zahlreiche Suchanfragen gestellt, die den Nachnamen Arnold oder ihren Wohnort enthielten. In einem Interview mit der Zeitung fand Frau Arnold deutliche Worte: „We all have a right to privacy. Nobody should have found this all out."[17] Das Bedürfnis nach Privatheit und Selbstbestimmung wird von den aktuell dominierenden Suchmaschinen indes nicht erfüllt, sondern ganz im Gegenteil erheblich bedroht. Eine offene Suchinfrastruktur ermöglicht es indes, den gerade in Suchmaschinen präsenten Möglichkeiten der Kontrolle und Überwachung zu begegnen.

Einen ersten praktischen Schritt hin zu einem offenen Webindex geht das Horizon Europe-Projekt OpenWebSearch.EU (2022-2026). In diesem Projekt wird von einem technisch-wissenschaftlich orientieren Konsortium aus 14 europäischen Großrechenzentren, Wissenschaftszentren, Universitäten sowie der Open Search Foundation eine offene und verteilte Suchinfrastruktur für das Internet konzipiert und prototypisch implementiert. Dabei werden sowohl signifikante Webdatencrawls als auch die weiterführende Webdatenanalyse und Webindexerstellung für eine Nutzung in Suchdiensten für Europa durchgeführt. Das vom Bundesministerium für Bildung und Forschung (BMBF) geförderte Projekt „Privatsphäre fördernde Digitale Infrastrukturen – PriDI" unterstützt die Erstellung eines offenen Webindex durch rechtswissenschaftliche und wirtschaftsinformatorische Expertise.[18]

17 *Barbaro/Zeller Jr.*, A Face Is Exposed for AOL Searcher No. 4417749, The New York Times v. 9. August 2006.

18 Beitrag basiert auf und erweitert Whitepaper Geminn u.a., Anwendungsfälle eines offenen Webindex, 2025; abrufbar unter https://pridi-projekt.de.

2 Der offene Webindex

Ähnlich wie die Indizes von Google oder Bing wird der OWI durch systematisches Crawlen des Webs, die Analyse der gecrawlten Inhalte und deren Speicherung mit Metadaten in einer Datenbank erstellt.[19] Der OWI soll die digitale Souveränität der EU stärken, indem er die Abhängigkeit von außereuropäischen Monopolisten im Suchmaschinenmarkt durch einen nachhaltigen, frei zugänglichen Webindex verringert.

Entwickelt wurde eine verteilte Crawling-, Indexierungs- und Hosting-Architektur für den OWI. Diese besteht in der Kombination eines Frontier-Crawlers, der im Wesentlichen das Web entlang eingebetteter Links kartiert und URLs sammelt, mit verteilten Worker-Crawlern, die später die Websites abrufen und deren Inhalte in sogenannten Web-Archivdateien (WARC) speichern. Später werden die "rohen" Webdaten weiterverarbeitet, bereinigt, gefiltert, mit Metadaten angereichert, nach Sprache und Genre klassifiziert und als Webindex-Charts im Common Index File Format (CIFF) gespeichert.

Das System ist so konzipiert, dass es Speicher- und Rechenkapazitäten in mehreren Hochleistungsrechenzentren in ganz Europa bündelt und dynamisch erweitert werden kann, indem weitere Rechenzentren in den Verbund aufgenommen werden. Um auf den Index zuzugreifen, können sich Suchmaschinenanbieter oder andere wissenschaftliche Nutzer des OWI über ein öffentliches System authentifizieren und über die Befehlszeile auf Teile des Index zugreifen und diese abrufen. Derzeit werden die Webdaten unter einer Forschungslizenz zur Verfügung gestellt. Das Forschungsteam wird den Zugang zum System jedoch auch für kommerzielle Akteure ermöglichen.

Die öffentliche Zugänglichkeit des Index soll die Freiheit der Internetsuche stärken und eine Grundlage für Innovationen in Wissenschaft und Wirtschaft bilden. Die Forscher haben inzwischen rund 2,23 Milliarden URLs in 185 verschiedenen Sprachen gecrawlt. Der offene Webindex hat derzeit ein Volumen von rund 14 TB und steht interessierten Entwicklern für Tests zur Verfügung. Der Index von Google ist mit einem Volumen von rund 100 000 TB allerdings deutlich größer.[20]

19 Weitere Einzelheiten über die Erstellung und den Betrieb des OWI in Hendriksen *u.a.*, Open Web Index, Advances in Information Retrieval 2024.

20 *Google*, How Google Search organizes information, 2025.

3 Akteure

Bei der Bewertung des OWI aus rechtlicher Sicht und mit Blick auf die Nutzerakzeptanz wird im Folgenden zwischen den verschiedenen Interessengruppen unterschieden. Zum einen sind das die *Betroffenen*. Diese Rolle beschreibt Personen oder Unternehmen, deren persönliche Daten (betroffene Personen) oder geistiges Eigentum (Rechteinhaber) im OWI gespeichert sind und von Tools oder Suchmaschinen, die auf dem OWI basieren, genutzt oder gefunden werden können. Der Index selbst wird vom *OWI-Entwickler* entwickelt und gepflegt. Der OWI-Entwickler hat sich zu einer unabhängigen juristischen Person, dem Betreiberkonsortium, zusammengeschlossen. Die Abrufer oder Konsumenten der im OWI enthaltenen Daten und Informationen werden als *Anwendungsentwickler* bezeichnet. Es handelt sich um Personen oder Systeme, die Webdaten aus dem Index abrufen, um auf Grundlage der abgerufenen Daten verschiedene Anwendungen und Modelle zu erstellen und zu entwickeln.[21] Dabei kann es sich um Einzelpersonen, Unternehmen, öffentliche Einrichtungen oder Wissenschaftler:innen handeln, die die offenen Daten des OWI nutzen, um ihre eigenen Anwendungen und Dienste zu entwickeln. Schließlich kommen auch die *Endnutzer* mit dem Index in Berührung. Sie sind die natürlichen oder juristischen Personen, die von den Anwendungsentwicklern entwickelte Werkzeuge und Systeme nutzen.

4 Anwendungsfälle

Der offene Web-Index lässt sich in einer Vielzahl von Anwendungsbereichen[22] nutzen, die im nachfolgenden überblicksartig dargestellt werden.[23]

21 Z.B. im Rahmen von Trainingsprozessen für KI-Anwendungen, siehe 4.2 und 4.4.
22 Siehe auch Studie *Nowakowski u.a.*, Market potential assessment, 2024.
23 Aufstellung basiert auf *Geminn u.a.*, Anwendungsfälle eines offenen Webindex, 2025, welche hier in Teilen wiedergeben wird.

4.1 Entwicklung vertikaler Suchmaschinen

Der OWI kann als Grundlage für die Entwicklung neuer (vertikaler) Suchmaschinen[24] dienen. Es könnten etwa Suchmaschinen für bestimmte Nutzergruppen, Lokalitäten oder Themen entstehen. Der OWI schafft die Grundlage dafür, indem er eine umfangreiche Datenbasis zur Verfügung stellt. Auf diese können Anwendungsentwickler von spezialisierten Suchmaschinen zugreifen und genau die Daten herausfiltern, die für den jeweiligen Zweck relevant sind. So können auch kleinere Organisationen und Unternehmen Suchmaschinen entwickeln und die Vielfalt im Suchmaschinenmarkt erhöhen.[25] Denn sie müssen keine enormen Ressourcen für das Crawlen und Indexieren des gesamten oder eines Teils des Internets aufbringen, sondern können auf Grundlage des OWI präzise und relevante Ergebnisse für spezifische Themengebiete liefern. Da der Quellcode des OWI öffentlich einsehbar ist, können die Anwendungsentwickler zudem die zugrundeliegenden Algorithmen verstehen und auf ihre spezifischen Bedürfnisse anpassen. Mithilfe des offenen Webindex können neue Suchmaschinen für Nachrichten entstehen, die Privatpersonen Nachrichten über sowohl aktuelle als auch vergangene Ereignisse zur Verfügung stellen. Darüber hinaus können Pressespiegel zu verschiedenen Themen, Ereignissen oder auch Unternehmen zusammengestellt werden.

4.2 Training von Large Language Models (LLMs)

Für das Training von Large Language Models (LLMs)[26] sind umfassende und qualitativ sehr gut vorgefilterte Webdatenbestände von hoher Relevanz. Ein Beispiel für ein LLM ist GPT-4 von OpenAI, worauf das Sprachmodell ChatGPT basiert. Solche Modelle werden mit großen Mengen an Textdaten trainiert, die überwiegend aus online verfügbaren Quellen stammen. Mithilfe von maschinellem Lernen unter Nutzung von neuronalen Netzwerken und Deep Learning-Methoden lernen LLMs, statistische Zusammenhänge zwischen Wörtern und Sätzen zu erkennen, um auf der Grundlage statistischer Häufigkeiten Sprach-Artefakte zu vervollständigen oder zu ge-

24 *Curran/McGlinchey*, Vertical search engines, The ITB Journal 2003, S. 22.
25 Vgl. *Geminn u.a.*, Anwendungsfälle eines offenen Webindex, 2025, S. 11f.
26 *Dakhel u.a.*, in: Nguyen-Duc u.a. (Hrsg.), Generative AI for Effective Software Development, 2024, S. 3f.

nerieren. Der OWI trägt dazu bei, neue LLMs zu entwickeln, indem er auch kleineren Unternehmen kostengünstig eine hinreichende Menge an Trainingsdaten zur Verfügung stellt. Dadurch weisen die Produkte solcher Start-Ups im Vergleich zu den derzeit auf dem Markt angebotenen Sprachmodellen eine konkurrenzfähige Qualität auf.[27]

RAG, oder *Retrieval Augmented Generation*, ist ein Ansatz in der KI, bei dem Textgenerierungsmodelle um eine Komponente zur Informationsbeschaffung erweitert werden.[28] Dabei kombiniert RAG die Fähigkeit eines Sprachmodells, Antworten zu generieren, mit einer Retrieval-Komponente, die relevante Informationen aus externen Wissensquellen wie Datenbanken oder Dokumenten abruft. Die erste Komponente von RAG, das Sprachmodell, wird auf großen Textmengen trainiert, um Sprache zu verstehen und Texte zu generieren. Es bildet das Grundgerüst für die Generierung von Antworten. Die zweite Komponente, das Retrieval, greift auf eine Wissensbasis oder eine Dokumentensammlung zu, um bei jeder Anfrage relevante Informationen abzurufen. Diese Kombination ermöglicht präzisere und aktuellere Antworten, da das Modell nicht nur auf statisches Wissen beschränkt ist, sondern gezielt aktuelle Informationen in die Generierung integrieren kann. Anwendungsfelder für RAG sind unter anderem Kundensupport, medizinische Beratung und Wissensmanagement, bei denen es auf spezifische und aktuelle Antworten ankommt.

Mithilfe der Daten im OWI könnten auch andere webdatenbasierte KI-Anwendungen trainiert werden, etwa Systeme des *Knowledge Representation and Reasoning* (KRR).[29] Hier geht es im Gegensatz zu LLMs, die mit Statistik Texte produzieren, darum, Informationen so darzustellen, dass sie ein Computer verarbeiten und gleich einem Menschen komplexe Probleme lösen kann. Ziel sind „intelligente" Maschinen, die vom menschlichen Wissen lernen und gleich diesem handeln. KRR-Systeme werden beispielsweise im Qualitätsmanagement zur Überwachung der Produktqualität eingesetzt oder zur Betrugsprävention im Versicherungswesen.

27 Vgl. *Geminn u.a.*, Anwendungsfälle eines offenen Webindex, 2025, S. 13f.
28 *Arslan u.a.*, A survey on RAG with LLMs, Procedia Computer Science 2024, S. 3781.
29 *Sharma/Garg*, Artificial Intelligence, 2021.

4.3 Verbesserung lokaler Suchdienste

Google verknüpft via Google Maps Nutzer mit Unternehmen. Im Sinne dieses Dienstes könnte der OWI dazu genutzt werden neue Kartendienste zu verbessern. Denn die Webdaten aus dem Index enthalten katalogisiert Informationen zu Städtenamen, Hotels, Restaurants, Geschäften und Sehenswürdigkeiten. Diese Daten können mit den jeweiligen Orten auf einer Karte verknüpft werden. Zudem ist es möglich, weitere Hintergrunddaten aus dem OWI automatisiert zu den jeweiligen Orten hinzuzufügen, wie etwa die Historie von Städten oder Preise von Hotels, Restaurants und Geschäften. Auf diese Weise sind Anbieter von Kartendiensten nicht mehr auf eine umfangreiche Mitarbeit von Nutzern angewiesen, sondern können ihre Inhalte auf Grundlage der Webdaten initial aufstellen und laufend aktualisieren. Dies ist ein Kostenvorteil, der dazu führen könnte, dass neue Anbieter von Kartendiensten auf den Markt eintreten.[30]

Zudem ist es mithilfe des OWI möglich, das lokale Web für Bewohner oder Touristen in einer bestimmten Region in eine separate Suchmaschine zu überführen und so eine lokale Suche zu ermöglichen. In den Suchergebnissen werden dann automatisch nur die Inhalte lokaler Anbieter angezeigt. Der Nutzer findet so zielgerichtet die Informationen, die aufgrund seiner Lokalität für ihn relevant sind. Es ergäbe sich der Effekt einer Art Gemeindeplattform, in der sich die Bürger untereinander austauschen können und lokale Ökosysteme gestärkt werden. Das würde auch dazu führen, dass lokale Unternehmen gestärkt und ihre Angebote vor Ort sichtbarer gemacht werden. Auf diese Weise würden durch Suchmaschinen die günstigsten und besten lokalen Angebote angezeigt und nicht diejenigen, die mit dem Suchmaschinenanbieter verbunden sind.[31]

4.4 Business Intelligence und Analytics

Business Intelligence (BI) und Analytics spielen eine zentrale Rolle in modernen Unternehmen, da sie datenbasierte Entscheidungsprozesse ermöglichen.[32] BI umfasst die Sammlung, Verarbeitung und Darstellung von

30 Vgl. *Geminn u.a.*, Anwendungsfälle eines offenen Webindex, 2025, S. 17.
31 Siehe auch das Urteil gegen Google wegen unlauterer Selbstreferenzierung in Google Shopping: EuGH, Urteil vom 10. September 2024 – Ref. C-48/22 P.
32 *Baars/Kemper*, Business Intelligence & Analytics, 2021.

Geschäftsdaten, um historische Trends und aktuelle Leistungskennzahlen zu visualisieren. Analytics geht einen Schritt weiter und nutzt fortschrittliche statistische Methoden sowie maschinelles Lernen, um tiefergehende Einblicke zu gewinnen und Vorhersagen zu treffen. Unternehmen können dadurch nicht nur Entwicklungen aus der Vergangenheit analysieren, sondern auch zukünftige Geschäftsstrategien optimieren. Diese datengetriebenen Ansätze führen zu verbesserten Geschäftsentscheidungen, effizienteren Prozessen und folglich zu Wettbewerbsvorteilen in einem zunehmend datenintensiven Markt. Die Ansätze von Business Intelligence und Analytics erfordern operative Daten, Kundendaten, Finanzdaten, Web- und Social-Media-Daten, logistische Daten, Marktdaten, externe Daten sowie Maschinendaten, um fundierte Analysen durchzuführen und datengetriebene Entscheidungen zu unterstützen.[33] Es lassen sich Produkte entwickeln, die die Ansätze aus Business Intelligence und Analytics implementieren und geeignete Webdaten aus den OWI-Subindizes für diese Berechnungen heranziehen. Nicht alle genannten Datenarten wären im OWI verfügbar, da zum Beispiel Finanz- und Kundendaten von Unternehmen nicht im Internet zur Verfügung stehen. Daher können Anwendungsentwickler relevante Daten aus den verschiedenen Subindizes und dem OWI ziehen, um den individuell geeigneten Datensatz für die Berechnungen zusammenstellen.

4.5 Aufdeckung von Desinformation und Bot-Netzwerken

Der offene Webindex kann dabei helfen, Desinformation[34] und Bot-Netzwerke aufzudecken. Auf Grundlage des umfangreichen Datenpools können plattformübergreifende Lösungen entwickelt werden, um Social Media Accounts zu erkennen und zu verfolgen, die allein oder in Netzwerken Desinformation in der digitalen Welt verbreiten. Das gilt ebenso für Accounts, die künstlich ein bestimmtes (politisches) Narrativ verbreiten wollen, was sich zuletzt im Zusammenhang mit dem Angriff Russlands auf die Ukraine als Herausforderung dargestellt hat. Systematische Verzerrungen der öffentlichen Meinungsbildung können dann entsprechend geflaggt oder aus dem jeweiligen Netzwerk herausgenommen werden. Der OWI wäre für die Entwicklung eines Tools zur Aufdeckung von Desinformation und Bot-Netzwerken hilfreich, da mithilfe des OWI-Inhalte über verschiedenen

33 Vgl. *Geminn u.a.*, Anwendungsfälle eines offenen Webindex, 2025, S. 20.
34 *Shams u.a.,* Web search engine misinformation notifier extension, Healthcare 2021.

Plattformen und Webseiten verfolgt werden können, um auf diese Weise den Ursprung der Nachrichten verifizieren zu können.[35]

5 Chancen und Risiken für Grundrechte und -freiheiten

Gerade in Rechtsgebieten, die einem schnellen Wandel unterliegen, birgt die Betrachtung grundrechtlicher Anforderungen gewisse Vorteile im Vergleich zu einer Analyse einfachgesetzlicher Anforderungen. Grundrechte und -freiheiten dienen als beständige, allgemein gültige Leitplanken. Durch Erstellung und Kuratierung eines offenen Web-Index sind potenziell eine Vielzahl von Grundrechten und Grundfreiheiten aus dem Grundgesetz (GG) und der EU-Grundrechte-Charta (GRCh) betroffen:

Art. 2 Abs. 1 iVm. Art. 1 GG beinhaltet das Recht auf informationelle Selbstbestimmung, welches durch das Crawling und Indexieren persönlicher Daten betroffen sein kann. So besteht durch den Index insbesondere das Risiko einer zweckunbestimmten Datenvorratshaltung.

Eine solche Datenvorratshaltung stünde zunächst im Konflikt mit dem Recht auf Achtung der Kommunikation aus Art. 7 GRCh und dem Recht auf Schutz personenbezogener Daten aus Art. 8 GRCh. Gleichzeitig kann durch den offenen Webindex allerdings auch Transparenz über die Verarbeitung personenbezogener Daten im Netz geschaffen und den betroffenen Personen eine Kontrollmöglichkeit über die Verbreitung solcher Informationen gewährt werden.

Art. 15 GRCh und Art. 11 GG schützen die Berufsfreiheit. Das Crawling und die Indexierung von Daten kann dazu führen, dass Daten gegen den Willen oder in Widerspruch mit den Interessen des Urhebers oder Rechteinhabers genutzt werden und so Geschäftsmodelle gestört werden. Auch die in Art. 16 GRCh geschützte unternehmerischen Freiheit kann dadurch betroffen sein. Es ergeben sich für die berufsbezogenen Grundrechte und -freiheiten jedoch auch erhebliche Chancen durch das Aufbrechen bestehender Quasi-Monopole.

Das Eigentum wird in Art. 17 GRCh und Art. 14 GG geschützt. Insbesondere das sogenannte geistige Eigentum ist von einem Kontrollverlust durch den offenen Webindex bedroht, etwa wenn Werke gegen den Willen des Rechteinhabers in den Index aufgenommen und verbreitet werden. Andererseits kann der Index auch dazu beitragen, urheberrechtlich geschützte

35 Vgl. *Geminn u.a.*, Anwendungsfälle eines offenen Webindex, 2025, S. 22f.

Werke weiter zu verbreiten und besser auffindbar zu machen, sodass kreative Urheber mehr Kunden erreichen können und die Verwertungsrechte an wirtschaftlichem Wert gewinnen. Der Index könnte den Rechteinhabern auch helfen, überhaupt unrechtmäßige Verwendungen ihres geistigen Eigentums online aufzudecken.

Durch die Zugänglichmachung von Webinhalten durch den Index können auch das Recht auf freie Meinungsäußerung, die Informationsfreiheit (Art. 11 GrCH und Art. 5 Abs. 1 GG) sowie die Freiheit von Kunst und Wissenschaft (Art. 13 GRCh und Art. 5 Abs. 3 GG) betroffen sein. Denn der Index birgt grundsätzlich die Gefahr, unwahre Informationen zu verbreiten oder Meinungen zu manipulieren. Zugleich kann ein offener Webindex den Zugang zu Informationen im Netz erleichtern sowie vielfältige Meinungsäußerungen und wissenschaftliche Publikationen einem breiten Publikum zugänglich machen.

Art. 36 und Art. 22 GRCh beinhalten das Recht auf Zugang zu Dienstleistungen von allgemeinem wirtschaftlichem Interesse sowie den Schutz der Vielfalt der Sprachen. Abhängig davon, welche Inhalte in den Index aufgenommen werden und für wen der offene Webindex zugänglich ist, können auch diese Grundfreiheiten betroffen sein.

Zuletzt wird der Webindex offen ausgestaltet sein und derzeit durch europäische Akteure finanziert und umgesetzt. Vor diesem Hintergrund sind Risiken von zu großer oder missbräuchlicher politischer Einflussnahme mit den Art. 20 und 23 GG in Einklang zu bringen.

6 Einfachgesetzlicher Rechtsrahmen

Die Komplexität des OWI wirft viele rechtliche Fragen auf, so dass der Rechtsrahmen nicht einfach zu bestimmen ist. Das europäische Recht für Daten und Online-Dienste hat sich in den letzten Jahren stark verändert. Während zunächst vor allem die Datenschutz-Grundverordnung (DSGVO, Verordnung (EU) 2016/679) den Umgang mit personenbezogenen Daten detailliert regelte, ist inzwischen ein Netz von mehr oder weniger spezialisierten, unmittelbar geltenden Rechtsakten entstanden. Der Digital Services Act (DSA, Verordnung (EU) 2022/2065), der Data Governance Act (DGA, Verordnung (EU) 2022/868), der Data Act (DA, Verordnung (EU) 2022/868), der Digital Markets Act (DMA, Verordnung (EU) 2022/1925) und die KI-Verordnung (KI-VO, Verordnung (EU) 2024/1689) bilden

einen weiten rechtlichen Rahmen für digitale Dienstleistungen und Geschäftsmodelle, die auch einen OWI und Anwendungsentwickler betreffen können.[36] Diese Verordnungen gelten unmittelbar und einheitlich in allen Mitgliedsstaaten.

Gleichzeitig gibt es in der Europäischen Union einen harmonisierten Rahmen für das Urheberrecht. Er wird in erster Linie durch eine Kombination aus EU-Richtlinien, internationalen Verträgen und nationalen Gesetzen der Mitgliedstaaten geregelt. Obwohl die Union bestrebt ist, die Urheberrechtsgesetze in ihren Mitgliedstaaten zu harmonisieren, gibt es immer noch Unterschiede auf nationaler Ebene.

Im Folgenden werden das Datenschutzrecht (6.1), der Digital Services Act (6.2), das Urheberrecht (6.3) und die KI-Verordnung (6.4) beleuchtet.

6.1 Datenschutzrecht

Der OWI wird, absichtlich oder unabsichtlich, personenbezogene Daten von natürlichen Personen (betroffene Personen) im Sinne von Art. 4 Nr. 1 DSGVO in den gecrawlten Daten enthalten.[37] Es kann sich dabei sogar um Daten besonderer Kategorien im Sinne von Art. 9 Abs. 1 DSGVO handeln. Personenbezogene Daten können auch Teil der im OWI gesammelten und angereicherten Metadaten sein (z. B. Eigentümer von Webseiten, Kontaktangaben). Die Tätigkeit von Dritten ins Internet gestellte oder dort veröffentlichte Informationen zu finden, automatisch zu indexieren und (ggf. auch nur vorübergehend) zu speichern und schließlich Anderen zur Verfügung zu stellen ist insofern eine Verarbeitung personenbezogener Daten iSv Art. 4 Nr. 1 und 2 der DSGVO.[38]

Die Institution, welche den OWI betreibt, ist in Bezug auf diese personenbezogenen Daten verantwortlich im Sinne des Art. 4 Nr. 7 DSGVO.[39] Wird der OWI von einem Joint-Venture verschiedener Organisationen oder

36 Dazu *Geminn/Johannes*, Handbuch europäisches Datenrecht, 2025.

37 *Geminn u.a.*, Legal Challenges of an Open Web Index, International Cybersecurity Law Review 2021, 183; *Geminn*, Rechtsfragen eines offenen Web Index, Multimedia und Recht 2021, 18.

38 EuGH, Urteil vom 8.12.2022 – Az. C-460/20 (TU, RE/Google LLC), Rn. 49 -ECLI:EU:C:2022:962.

39 EuGH, Urteil vom 13.5.2014 – Az. C-131/12 (Google Spain), Rn. 41 - ECLI:EU:C:2014:317; EuGH, Urteil vom 27.9.2019 – Az. C-136/17 (Google vs. CNIL), Rn. 35 - ECLI:EU:C:2019:773.

öffentlicher Einrichtungen angeboten, sind die beteiligten Stellen gemeinsam für die Verarbeitung verantwortlich.

Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn sie auf eine entsprechende Rechtsgrundlage im Sinne von Art. 6 DSGVO gestützt werden kann. Die Erstellung und der Betrieb eines unabhängigen, frei zugänglichen Webindex durch öffentlich-rechtliche Einrichtungen (oder in deren Auftrag) liegt im öffentlichen Interesse, z. B. um die Abhängigkeit von Unionsbürgern von ausländischen Suchmaschinen zu verringern. Für die Rechtmäßigkeit der Verarbeitung im öffentlichen Interesse gemäß Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO bedarf es einer Rechtsgrundlage im Unionsrecht oder im Recht der Mitgliedstaaten gemäß Abs. 3. Eine solche Grundlage ist bislang nicht ersichtlich, sodass die öffentliche(n) Stelle(n), die den OWI entwickeln, auf eine allgemeine Ermächtigung im mitgliedstaatlichen Recht zurückgreifen müssten. Beispielsweise dürfte ein Rechenzentrum, welches als öffentliche Stelle in Bayern organisiert ist, personenbezogene Daten für einen OWI, z. B. das Crawlen, Kopieren und Sortieren von Webseiten und deren Indexierung, aufgrund seiner eigenen Zweckbestimmung (d. h. Satzung und/oder Errichtungsgesetz) in Verbindung mit Art. 4 Bayerisches Datenschutzgesetz (BayDSG) auf der Grundlage von und in Verbindung mit Art. 6 Abs. 1 Nr. 1. lit. e und Abs. 2 und 3 DSGVO verarbeiten.

Bei privatwirtschaftlichen Einrichtungen können die Erstellung und der Betrieb des Open Web Index (OWI) nur auf die Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten gemäß Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO gestützt werden. Dies erfordert eine sorgfältige Abwägung der Interessen des OWI-Betreibers mit den Grundrechten der betroffenen Personen.

Das berechtigte Interesse des OWI-Entwicklers als verantwortliche Stelle besteht darin, ein OWI zu erstellen und zu betreiben, um das Internet zu indexieren und Informationen im Internet auffindbar zu machen. Dies dient nicht nur den wirtschaftlichen Interessen des Betreibers, sondern auch einem berechtigten Interesse der Allgemeinheit, Zugang Informationen zu erhalten. Zur Erstellung des Index muss der OWI-Entwickler möglichst viele Internetseiten crawlen und indexieren. Dabei verarbeitet er zwangsläufig personenbezogene Daten einer Vielzahl von betroffenen Personen. Diese Verarbeitung ist aus Sicht des OWI-Entwicklers erforderlich, um das berechtigte Interesse zu verwirklichen, da es keine gleichwertigen Mittel gibt, die weniger stark in die Grundrechte und Grundfreiheiten der betroffenen Personen eingreifen.

Fraglich bleibt, ob das Interesse betroffener Personen, nicht in einen Webindex aufgenommen zu werden und damit ihre informationelle Selbstbestimmung und ihr Recht auf Datenschutz zu schützen, das berechtigte Interesse des OWI-Entwicklers überwiegen kann. Dies erscheint unwahrscheinlich, insbesondere wenn man bedenkt, dass die gleichen Daten bereits mehrfach von anderen Indexbetreibern wie Google, Bing, Yandex oder Baidu gecrawlt wurden. Da ein Indexdienst Daten crawlt, die für jedermann frei zugänglich sind, erscheinen diese Daten nicht besonders schutzbedürftig. Der EuGH hat gefestigter Rechtsprechung zwar die datenschutzrechtliche Verantwortlichkeit eines Suchmaschinen- und Indexbetreibers ausdrücklich festgestellt,[40] jedoch nie die grundsätzliche Ermächtigung des Betreibers in Frage gestellt, personenbezogene Daten zu crawlen und zu indexieren. Dies ist aus Praktikabilitätserwägungen einleuchtend, da die Indexierung an sich wohl alternativlos ist. Hervorzuheben ist auch, dass die betroffenen Personen nicht schutzlos gestellt sind. Sie können sich bereits ex ante gegen eine Datenverarbeitung durch den OWI schützen, indem sie geeignete Maßnahmen ergreifen, damit ihre Daten nicht im Internet veröffentlicht sind – also z. B. direkt gegen Webseitenbetreiber vorgehen. Ex post kann die betroffene Person der Verarbeitung durch den OWI-Entwickler gemäß Art. 21 Abs. 1 DSGVO widersprechen und nach Art. 17 Abs. 1 lit. c DSGVO die Löschung der sie betreffenden Daten fordern. Zusammenfassend überwiegen die Interessen der betroffenen Personen nicht die des OWI-Betreibers und der Allgemeinheit an der Erstellung eines OWI.

Dies gilt im Ergebnis auch für die Verarbeitung besonderer Kategorien personenbezogener Daten. Diese unterliegt den Anforderungen von Art. 9 DSGVO. Die Verarbeitung solcher Daten ist grundsätzlich untersagt, es sei denn, die Voraussetzungen des Art. 9 Abs. 2 DSGVO sind erfüllt. Solange der OWI nur öffentlich zugängliche Daten crawlt, ist davon auszugehen, dass diese Daten in der Regel von der betroffenen Person veröffentlicht wurden und daher gemäß Abs. 2 lit. e verarbeitet werden dürfen. Es bleibt jedoch ein Restrisiko, dass sensible Daten gecrawlt und verarbeitet werden, die nicht von der betroffenen Person, sondern von einem Dritten veröffentlicht wurden (z.B. bei Datenpannen). Diesem Risiko könnte der OWI-Entwickler zumindest durch technische und organisatorische Maßnahmen

40 EuGH, Urteil vom 8.12.2022 – Az. C-460/20 (TU, RE/Google LLC) - ECLI:EU:C:2022:962.EuGH, Urteil vom 13.5.2014 – Az. C-131/12 (Google Spain) - ECLI:EU:C:2014:317; EuGH, Urteil vom 27.9.2019 – Az. C-136/17 (Google vs. CNIL) - ECLI:EU:C:2019:773.

begegnen, um die Verarbeitung von personenbezogenen Daten besonderer Kategorien zu minimieren. Zu denken wäre hier an Filtertechniken und Anonymisierung.

6.2 Digital Services Act

In seiner jetzigen Form wird der OWI auch unter die Regeln über digitale Dienstleistungen fallen, insbesondere unter den DSA. Diese Verordnung regelt im Wesentlichen die Haftung und den Umfang der Sorgfaltspflichten für Anbieter digitaler Vermittlungsdienste. Ziel ist, einen sicheren Rechtsrahmen für den digitalen Raum zu schaffen, um so ein sicheres, berechenbares und vertrauenswürdiges Online-Umfeld zu schaffen und die Grundrechte zu schützen, vgl. Art. 1 Abs. 1 DSA. Vermittlungsdienste "umfassen ein breites Spektrum wirtschaftlicher Tätigkeiten, die online stattfinden und sich ständig weiterentwickeln, um eine schnelle, sichere und geschützte Übertragung von Informationen zu ermöglichen und bequeme Lösungen für alle Beteiligten im Online-Ökosystem zu bieten."[41]

Die Einordnung des OWI unter die einzelnen Merkmale des DSA ist schwierig, insbesondere wenn es um die Qualifikation als Hosting-Dienst, Online-Plattform oder Suchmaschine geht. Die Einordnung des OWI als Vermittlungsdienst i.S.d. Art. 3 lit. g Nr. iii DSA und als Online-Suchmaschine i.S.d. Art. 3 lit. j DSA ist fraglich.[42] Es ist offensichtlich, dass der Gesetzgeber bei der Ausgestaltung des DSA von Anwendungsfällen wie Social Media und Online-Marktplätzen ausgegangen ist, während übergeordnete Anwendungen wie ein Webverzeichnis oder ein Index gar nicht erst in Betracht gezogen wurden. Auch die Regelungen zu Online-Suchmaschinen wurden nicht zu Ende gedacht. Dennoch sind die Funktionen und Möglichkeiten eines OWI häufig mit typischen Anwendungsfällen des DSA vergleichbar, sodass nach dem Schutzzweck des DSA der OWI darunterfallen sollte.

Sowohl im Hinblick auf den Zweck des DSA als auch aus allgemeinen Erwägungen wäre es sinnvoll, OWI-Betreibern die Haftungsbefreiung des DSA oder vergleichbare Privilegien zuzugestehen. Gleichzeitig sollten ihnen aber auch entsprechende Sorgfaltspflichten auferlegt werden, die

41 Erwägungsgrund 29 DSA.

42 *Nebel/Johannes*, Open Web Index im Lichte des Digital Services Act, Multimedia und Recht 2024, 1013.

gerade bei einer sehr großen Online-Suchmaschine erheblich sind. Hier sollte der Gesetzgeber nachbessern und sowohl Online-Suchmaschinen als auch den OWI in die Definition des Art. 3 lit. g DSG einbeziehen und die korrespondierenden Pflichten und Haftungsbefreiungen entsprechend benennen. Trotz Ermangelung einer solchen eindeutigen Regelung sollte der OWI-Entwickler davon ausgehen, dass es sich bei dem OWI um eine Suchmaschine und einen Hosting-Provider im Sinne des DSA handelt und entsprechende Maßnahmen ergreifen.[43]

6.3 Urheberrecht

Für das Urheberrecht hat der unionale Gesetzgeber mit der Urheberrechtsrichtlinie (2001/29/EG) und der Richtlinie über das Urheberrecht im digitalen Binnenmarkt (2019/790) Bestimmungen erlassen, die von den Mitgliedstaaten in nationales Recht umgesetzt wurden. Im Folgenden wird die Gesetzgebung in Deutschland als Beispiel herangezogen.

Es gibt zwei Perspektiven: Zum einen ist zu prüfen, inwieweit der OWI selbst rechtlich geschützt ist. Insbesondere könnte der Index als Datenbankwerk nach § 4 Abs. 2 UrhG geschützt sein, wonach der Index als solcher unabhängig vom Urheberrecht an den indizierten Inhalten geschützt wäre und nur unter bestimmten Voraussetzungen nach § 55a UrhG, insbesondere durch Einräumung von Nutzungsrechten, von Dritten genutzt werden könnte.

Zum anderen ist zu klären, inwieweit urheberrechtlich geschützte Inhalte im OWI indexiert und von Anwendungen, die auf dem Index basieren, genutzt werden dürfen. Der OWI enthält eine große Menge an Daten, bei denen es sich größtenteils um nach § 2 UrhG geschützte Werke handelt, die im Rahmen der Aufnahme in den Index vervielfältigt werden. Das Vervielfältigungsrecht nach § 16 UrhG steht jedoch nach § 15 Abs. 1 Nr. 1 UrhG grundsätzlich dem Urheber des Werkes zu und nicht einem Nutzer, wie dem OWI-Entwickler. Ähnliche Probleme bestehen auch im Zusammenhang mit Anwendungen, die auf dem OWI basieren, etwa wenn der Index zum Training von KI-Modellen verwendet wird. Bei der Erstellung des Index und der Entwicklung von Anwendungen lassen sich in Urheberrechte eingreifende Vervielfältigungen nicht vermeiden.

43 *Nebel/Johannes*, Open Web Index im Lichte des Digital Services Act, Multimedia und Recht 2024, 1016.

Das Urheberrechtsgesetz enthält jedoch verschiedene Ausnahmen, die Vervielfältigungshandlungen rechtfertigen können. Im Jahr 2021 hat der deutsche Gesetzgeber in Umsetzung von Art. 4 der Richtlinie Nr. 2019/790 die Ausnahmeregelung des § 44b UrhG für allgemeines Text- und Data-Mining geschaffen. Diese Norm soll es ermöglichen, große Mengen digitaler Informationen zu analysieren. Nach Ansicht der Wissenschaft[44] kann das Training von KI-Modellen in der Regel durch § 44b UrhG gerechtfertigt werden; und auch die Rechtsprechung zeigt eine leichte Tendenz in diese Richtung[45]. Allerdings sind etwaige Vorbehalte des Urhebers nach § 44b Abs. 3 UrhG zu berücksichtigen. Bei Vervielfältigungshandlungen, die durch Crawler bei der Indexierung von Webinhalten entstehen, kommt auch § 44a UrhG in Betracht. Hier sieht der Gesetzgeber eine Ausnahme für Vervielfältigungshandlungen vor, die nur vorübergehender Natur und Teil eines technischen Verfahrens sind, keine eigenständige wirtschaftliche Bedeutung haben und einem Zweck des § 44a UrhG dienen.

Neben diesen Ausnahmen haben die deutschen Gerichte auch entschieden, dass Suchmaschinen urheberrechtlich geschützte Inhalte indexieren dürfen: Mit der Veröffentlichung urheberrechtlich geschützter Werke im Internet willigt der Rechteinhaber ein (konkludente Einwilligung), dass seine Inhalte von Suchmaschinen gefunden werden können.[46] Voraussetzung dafür ist die Indexierung, sodass sich die Suchmaschinenbetreiber auf die konkludente Einwilligung der Rechteinhaber berufen können, um einen Index aufzubauen und zu pflegen. Das kann unter Umständen sogar dann der Fall sein, wenn das urheberrechtlich geschützte Werk gegen den Willen des Rechteinhabers ins Internet gestellt wurde.[47] Anders verhält es sich jedoch, wenn der Rechteinhaber Beschränkungen auferlegt, z. B.

44 Z.B. *Bomhard/Siglmüller*, Trilogergebnis, Recht Digital 2024, 50; *Dregelies*, KI-Training, Gewerblicher Rechtsschutz und Urheberrecht 2024, 1484; *Heine*, Nutzungsrechte, Gewerblicher Rechtsschutz und Urheberrecht in der Praxis 2024, 88; *Hofmann*, Geschäftsmodelle, Zeitschrift für Urheber- und Medienrecht 2024, 166; *Käde*, Training generativer KI-Modelle, Künstliche Intelligenz und Recht 2024, 162; *Maamar*, Urheberrechtliche Fragen, Zeitschrift für Urheber- und Medienrecht 2023, 481; *Wagner*, Blackbox, Zeitschrift für IT-Recht und Recht der Digitalisierung 2024, 298; Gegenmeinung: *Dornis/Stober,* Urheberrecht und Training generativer KI-Modelle, 2024; *Dornis*, KI-Training und Text- und Data-Mining, Künstliche Intelligenz und Recht 2024, 156.

45 LG Hamburg, Urteil vom 27. September 2024 – Az. 310 O 227/23.

46 BGH, Urteil vom 19. Oktober 2011 – Az. I ZR 140/10; *Klass*, Schlichte *Einwilligung*, Zeitschrift für Urheber- und Medienrecht 2013, 1.

47 BGH, Urteil vom 21. September 2017 – Az. I ZR 11/16.

in Form von robots.txt-Dateien oder Anmeldeanforderungen. Der Europäische Gerichtshof vertritt eine ähnliche Linie und argumentierte, dass Suchmaschinen zur Verbreitung von Informationen und zum Funktionieren des Internets beitragen.[48] Aus diesem Grund stelle die Verlinkung auf öffentlich zugängliche Inhalte keine Urheberrechtsverletzung dar. Diese Argumentation auf den OWI übertragbar.

6.4 KI-Verordnung

Der KI-Verordnung zielt auf die Regulierung von Systemen und Praktiken im Bereich der künstlichen Intelligenz ab. Sie soll einen robusten und flexiblen Rechtsrahmen schaffen, der die Nutzung von KI und automatisierten Systemen vertrauenswürdig und sicher macht. Die Verordnung verfolgt einen risikobasierten Ansatz.[49] Je höher das Risiko, desto umfangreicher sind die Verpflichtungen, die den Entwicklern und Betreibern[50] von KI-Systemen auferlegt werden. KI-Systeme mit inakzeptablen Risiken, z. B. Systeme, die ein "Social Scoring" durch Regierungen oder Unternehmen ermöglichen, werden als Bedrohung für die Grundrechte der Menschen angesehen und sind daher verboten.[51] Um dem spezifischen Transparenzrisiko zu begegnen, müssen bestimmte KI-Systeme, etwa Chatbots, die Nutzer eindeutig darüber informieren, dass sie mit einer Maschine interagieren. KI-generierte Inhalte müssen zudem als solche gekennzeichnet werden.[52] Nur für KI-Systeme mit geringem Risiko gelten keine Verpflichtungen gemäß der KI-VO. KI-Systeme mit hohem Risiko[53] hingegen, wie etwa KI-basierte medizinische Software oder KI-Systeme, die für die Personalbeschaffung eingesetzt werden, müssen strenge Anforderungen erfüllen, also zum Beispiel Systeme zur Risikominderung einführen, hochwertige Datensätze nutzen, klare Nutzerinformationen geben und menschliche Aufsicht gewährleisten.

48 EuGH, Urteil vom 13. Februar 2014 – Az. C-466/12.
49 Siehe Erwägungsgrund 26 KI-VO.
50 Siehe Art. 3 Nr. 8 KI-VO.
51 Siehe Art. 5 KI-VO.
52 Siehe Art. 50 KI-VO.
53 Siehe Art. 6 KI-VO und Anhang I und II KI-VO.

6.4.1 Unmittelbare Anwendbarkeit der KI-VO auf den OWI

Der OWI-Entwickler muss prüfen, inwieweit die Bestimmungen der KI-VO unmittelbar auf die zur Erstellung des OWI eingesetzten Technologien anwendbar sind. Dem risikobasierten Ansatz der KI-VO folgend werden KI-Systeme, "die erhebliche nachteilige Auswirkungen auf die Gesundheit, die Sicherheit und die Grundrechte von Personen haben können"[54] in Art. 6 KI-VO als Hochrisikosysteme eingestuft, wobei zwischen hochriskanten KI-Systemen im Zusammenhang mit der Produktregulierung (Abs. 1) und eigenständigen hochriskanten KI-Systemen (Abs. 2) unterschieden wird.

Angenommen werden kann, dass die Algorithmen und Systeme, die vom OWI zur Unterstützung und Koordinierung des Web-Crawling verwendet werden, zunächst grundsätzlich um KI-Systeme im Sinne der KI-VO handelt. Diese beziehen sich auf den ersten Blick auch nur auf interne Vorgänge. Dennoch ist anhand einer Risikobewertung zu prüfen, welcher Risikostufe diese KI-Systeme zugeordnet werden müssen.

Als Hochrisikosysteme gelten KI-Systeme, die Sicherheitsbauteile von Produkten sind (Art. 3 Nr. 14 KI-VO) oder selbst Produkte sind, die unter die Rechtsvorschriften des Anhangs II der KI-VO fallen (z. B. Maschinen, medizinische Geräte, Kraftfahrzeuge und Flugzeuge). Der OWI würde demnach wohl nicht als Hochrisikosystem nach Art. 6 Abs. 1 KI-VO einzustufen sein.

In Art. 6 KI-VO werden außerdem die in Anhang III der KI-VO aufgeführten KI-Systeme als besonders risikoreich bewertet. Dazu gehören KI-Systeme in den Bereichen Biometrie, kritische Infrastrukturen, Bildung, Beschäftigung, Grundversorgung, Strafverfolgung, Migration, Asyl und Grenzkontrolle sowie Justizverwaltung und demokratische Prozesse. KI, die bei der Indexierung sowie bei der Entscheidung über den Ausschluss oder die Aufnahme bestimmter Webinhalte eingesetzt wird, hat im Allgemeinen spürbare Auswirkungen auf die Indexnutzung durch Dritte. Dies ist jedoch eine Frage des konkreten Einsatzumfangs. Nach jetzigem Funktionsumfang des Index ist nicht davon auszugehen, dass der Index einem der in Anhang III aufgeführten Sektoren zuzuordnen ist. Perspektivisch könnte jedoch Einordnung unter der in Nr. 2 aufgeführten "kritischen Infrastrukturen" erfolgen.

54 Siehe Erwägungsgrund 46 KI-VO.

6.4.2 Mittelbare Auswirkungen der KI-VO auf den Index

Darüber hinaus stellt sich die Frage, ob die KI-Verordnung Regelungen enthält, die die Nutzung von OWI-Daten für bestimmte KI-Anwendungen beeinflussen. Zum Beispiel ist der Betrieb bestimmter KI-Systeme nach Art. 5 KI-VO verboten. Der OWI-Entwickler könnte deswegen erwägen, die Verwendung des Index für das Training solcher KI-Systeme zu verhindern. Das könnte über eine Indexlizenz oder die Bedingungen für die Nutzung des OWI erreicht werden. Der OWI-Betreiber könnte dabei einen Einschätzungsspielraum nutzen. Verboten ist nach Art. 5 KI-VO in der Regel das Inverkehrbringen und die Inbetriebnahme verbotener KI-Systeme. Die bloße wissenschaftliche Erforschung und Entwicklung des Einsatzes von KI-Systemen, die lediglich auch zu verbotenen Praktiken fähig wären, ist deswegen nicht verboten.[55] Darüber hinaus ist nach Art. 2 Abs. 6 KI-VO die KI-Verordnung nicht anwendbar für KI-Systeme oder KI-Modelle einschließlich ihrer Ergebnisse, die ausschließlich zum Zwecke der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden, vgl. Art. 3 Nr. 11 KI-VO. Das dient der Innovationsförderung und dem Schutz der Wissenschaftsfreiheit.[56] Wissenschaftliche Forschung umfasst nach Art. 13 GRCh Tätigkeiten mit dem Ziel, "methodisch, systematisch und nachprüfbar neue Erkenntnisse zu gewinnen". Dazu gehören die Grundlagenforschung und die angewandte Forschung im öffentlichen (z. B. Universitäten) und privaten (z. B. industrielle Forschung) Sektor.

Ein anderes Beispiel für eine mögliche mittelbare Auswirkungen der KI-VO auf den Index oder den OWI-Betreiber, dass KI-Systeme mit hohem Risiko mit Trainings-, Validierungs- und Testdatensätzen entwickelt werden müssen, die bestimmte Qualitätskriterien erfüllen.[57] Art. 10 Abs. 3 KI-VO schreibt vor, dass Trainings-, Validierungs- und Testdatensätze relevant, hinreichend repräsentativ und im Hinblick auf den vorgesehenen Zweck möglichst fehlerfrei und vollständig sein müssen. Fraglich ist u.a., ob aus Datenschutzgründen anonymisierte oder pseudonymisierte Daten (z. B. durch Hinzufügen von Rauschen) noch als fehlerfrei und vollständig angesehen werden können.[58] Die Datensätze müssen zudem die entsprechenden statistischen Merkmale aufweisen, ggf. auch im Hinblick auf die Personen oder Personengruppen, durch die das Hochrisiko-KI-System bestimmungs-

55 Siehe auch Erwägungsgrund 25 KI-VO.
56 Siehe Erwägungsgrund 25 KI-VO.
57 Siehe Art. 10 Abs. 2 - 5 KI-VO in Übereinstimmung mit Art. 10 Abs. 1 KI-VO.
58 *Vogel u. a.*, in: Demmler u.a. (Hrsg.), INFORMATIK 2022, 2022, 659.

gemäß eingesetzt werden soll. OWI-Daten stellen eine umfangreiche und vielfältige Informationsquelle dar, die Texte und Links enthält. Diese Vielfalt ist für das Training von KI-Modellen entscheidend. Um die Qualitätskriterien für KI-Systeme mit hohem Risiko erfüllen zu können, sollte der OWI-Entwickler Techniken anwenden, um die Datenqualität sicherzustellen, z. B. Datenbereinigung, -anreicherung, -abgleich oder -kommentierung. Gleichzeitig könnte er versuchen, seine Datensätze so zu erstellen und Maßnahmen zu ergreifen, die nachfolgende Anwendungsentwickler nutzen oder auf denen sie aufbauen können, um die Datenqualität für ihren spezifischen Anwendungsfall sicherzustellen.

7 Nutzerakzeptanz und Vertrauen

Die rechtliche Untersuchung des OWI sollte mit Überlegungen zur Nutzerakzeptanz und zum Vertrauen einhergehen, um eine positive Nutzerwahrnehmung und letztlich den Markterfolg zu fördern. Obwohl eine rechtskonforme Gestaltung technischer Innovationen sowie Datenschutz und Privatsphäre in Europa von großer Bedeutung sind, zeigt die Praxis, dass Nutzer bei der Wahl digitaler Dienste oft andere Faktoren in ihre Entscheidung einbeziehen – oder diese sogar als wichtiger einstufen. Daher ist es essenziell, Schlüsselaspekte der Nutzerakzeptanz frühzeitig in den Designprozess des OWI und den darauf basierenden Tools zu integrieren. Ein leistungsfähiger europäischer Webindex muss nicht nur Datenschutz- und Privatsphäre-Konzepte berücksichtigen, sondern auch zentrale Kriterien der Nutzerakzeptanz. Nur so kann er auf dem globalen Markt konkurrieren oder zumindest mit internationalen Anbietern in Europa mithalten.

Die Wahrnehmung der Nutzer und die Absicht der Anwender, neue technologische Lösungen zu nutzen, sind entscheidende Faktoren für deren erfolgreiche Entwicklung. Diese Faktoren werden im Rahmen des Forschungsgebiets Nutzerakzeptanz untersucht.[59] Ein weiterer Schlüsselfaktor für Technologieakzeptanz ist das Vertrauen in IT-Artefakte.[60] Diese Überlegungen sind für den Kontext des OWI wichtig, um das Vertrauen der

59 *Davis*, User acceptance of information technology, International Journal of Man-Machine Studies 1993, S. 475.

60 *Gefen u.a.*, Trust and tam in online shopping, MIS Quarterly 2003, S. 51; *Söllner u.a.*, Why different trust relationships matter, European Journal of Information Systems 2016, S. 274.

Nutzer in den OWI und in die darauf aufbauenden Tools zu stärken. Mit zunehmender technologischer Komplexität wird Vertrauen immer essenzieller, da Nutzer nicht in der Lage sind, die zugrunde liegenden Strukturen ständig zu durchdringen.[61]

Aus der Theorie lassen sich einige Modelle vorschlagen, die unterstützende Faktoren zu Vertrauen und Nutzerakzeptanz bereitstellen. Zur praktischen Anwendung für den OWI eignet sich eine Kombination aus zwei etablierten Modellen: Trust-TAM[62] und UTAUT2[63]. Relevante Faktoren können zusammengestellt werden, um die Grundlagen für den Aufbau und die Aufrechterhaltung von Nutzerakzeptanz und Vertrauen in den OWI und seine zukünftigen Produkte zu schaffen. Außerdem sind diese Faktoren in Bezug auf die einzelnen Akteure zu betrachten und weiterzuentwickeln, um Nutzerakzeptanz und Vertrauen in den jeweiligen Kontexten gezielt zu fördern.

8 Schlussfolgerungen und Ausblick

Diese Analyse soll das enorme Potenzial eines frei zugänglichen und umfassenden OWI zur Umgestaltung der digitalen Landschaft verdeutlichen. Durch die Förderung eines vielfältigeren und wettbewerbsfähigeren Suchmaschinenmarktes kann der OWI den Anwendungsentwicklern und in der Folge den Endnutzern mehr Auswahl und Kontrolle ermöglichen. Darüber hinaus kann der OWI als entscheidende Ressource für die KI-Entwicklung dienen, innovative Technologien vorantreiben und deren verantwortungsvolle Nutzung unterstützen.

Gleichzeitig bringt die Entwicklung und Implementierung des OWI spezifische Herausforderungen und Chancen für den Schutz der Grundrechte mit sich. Während der OWI das Potenzial hat, den Zugang zu Informationen (Art. 11 GRCh) zu verbessern, den Wettbewerb auf dem digitalen Markt zu fördern und die Innovation voranzutreiben, wirft er auch Fragen des Datenschutzes (Art. 8 GRCh), der unternehmerischen Freiheit (Art. 16 GRCh) und des Schutzes des geistigen Eigentums (Art. 17 GRCh) auf.

Die erfolgreiche Umsetzung des OWI erfordert eine sorgfältige Prüfung der rechtlichen und nutzerbezogenen Anforderungen. Die Gewährleistung

61 *Muir*, Trust in Automation, Ergonomics 1994, *S.* 1905.
62 *Gefen u.a.*, Trust and tam in online shopping, MIS Quarterly 2003, S. 64.
63 *Venkatesh u.a.*, Consumer acceptance, MIS Quarterly 2012, S. 157.

des Datenschutzes, die Wahrung der Rechte an geistigem Eigentum und die Abmilderung potenzieller Risiken für Grundrechte sind von größter Bedeutung. Die Einhaltung des europäischen Rechtsrahmens muss die Entwicklung und Nutzung des OWI leiten, begleitet von Überlegungen zu Nutzerakzeptanz und Vertrauen, um verantwortungsvolle technologische Innovationen zu unterstützen.

Literatur

Arslan, Muhammad; Ghanem, Hussam; Munawar, Saba und Cruz, Christophe (2024): A Survey on RAG with LLMs. *Procedia Computer Science*, 246, S. 3781-90. ISSN 1877-0509, https://doi.org/10.1016/j.procs.2024.09.178.

Baars, Henning und Hans-Georg Kemper (2021): *Business Intelligence & Analytics – Grundlagen und praktische Anwendungen: Ansätze der IT-basierten Entscheidungsunterstützung*. 4te Auflage. Wiesbaden: Springer Fachmedien Wiesbaden. ISBN 9783834823441

Bomhard, David und Siglmueller, Jonas (2024): KI-Gesetz - das Trilogergebnis, *Recht Digital,* 5(2), S. 45-55.

Braun, Max und Trepte, Sabine (2017): Privatheit und informationelle Selbstbestimmung: Trendmonitor zu den Einstellungen, Meinungen und Perspektiven der Deutschen. Stuttgart: Universität Hohenheim. URL: https://medienpsychologie.uni-hohenheim.de/fileadmin/einrichtungen/psych/Dateien/Laufende_Projekte/Trendmonitor_Privatheit_Hohenheim.pdf (besucht am 30.07.2025).

Brin, Sergey und Page, Lawrence (1998): The Anatomy of a Large-Scale Hypertextual Web Search Engine. *Computernetzwerke und ISDN-Systeme,* 30(1-7). S. 107.

Curran, Kevin and McGlinchey, Jude (2007): Vertical Search Engines. *The ITB Journal,* 8(2). S. 22-27. doi:10.21427/D7MT83

Dakhel, Arghavan Moradi; Nikanjam, Amin; Khomh, Foutse; Desmarais, Michel C. und Washizaki, Hironori (2024): An Overview on Large Language Models. In: Nguyen-Duc, Anh; Abrahamsson, Pekka und Khomh, Foutse (Hrsg.): *Generative AI for Effective Software Development*. Cham: Springer, S. 3-21. https://doi.org/10.1007/978-3-031-55642-5_1.

Davis, Fred D. (1993): User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International Journal of Man-Machine Studies,* 38(3), S. 475-489. https://doi.org/10.1006/imms.1993.1022.

Dornis, Tim W (2024): Generatives KI-Training und Text- und Data-Mining. Eine funktionale Unterscheidung. *Künstliche Intelligenz und Recht,* 1(5), S. 156-61.

Dornis, Tim W. und Stober, Sebastian (Hrsg.): (2024): *Urheberrecht und Training generativer KI-Modelle: Technologische und juristische Grundlagen*, 1. Aufl. Baden-Baden: Nomos. https://doi.org/10.5771/9783748949558.

Dregelies, Max (2024): KI-Ausbildung nach dem KI-Gesetz. *Gewerblicher Rechtsschutz und Urheberrecht,* 126(20), S. 1484-1493.

Gefen, David; Karahanna, Elena und Straub, Detmar W. (2003): Trust and tam in online shopping: An integrated model. *MIS Quarterly,* 27(1), S. 51-90. 10.2307/30036519.

Geminn, Christian L.; Voigt, Stefan; Söllner, Matthias; Johannes, Paul C.; Koulani, Huda; Beer, Leopold (2025): Anwendungsfälle eines offenen Webindex - Eine Handreichung für Wirtschaft und Wissenschaft. https://pridi-projekt.de/wp-content/uploads/2025/05/PriDI-Paper_Anwendungsfaelle.pdf.

Geminn, Christian L.; Erenli, Kai und Pfeiffer, Leon (2021): Legal Challenges of an Open Web Index. *International Cybersecurity Law Review*, (2), S. 183-94. https://doi.org/10.1365/s43439-021-00017-8.

Geminn, Christian L. (2021): Rechtsfragen eines offenen Web-Index - Infrastrukturen für die digitale Gesellschaft. *Multimedia und Recht*, (12), S. 16-19.

Geminn, Christian L. (2023): Deus ex machina? – Grundrechte und Digitalisierung, Tübingen: Mohr Siebeck.

Geminn, Christian L. und Johannes, Paul C. (Hrsg.) (2025): *Handbuch europäisches Datenrecht.* Baden-Baden: Nomos (in Vorbereitung).

Heine, Robert (2024): Generative KI: Nutzungsrechte und Nutzungsvorbehalt. *Gewerblicher Rechtsschutz und Urheberrecht in der Praxis,* 16(4), S. 87-90.

Google: How Google Search organizes information. Google.com. URL:https://www.google.com/intl/en_us/search/howsearchworks/how-search-works/organizing-information/ (besucht am 26.02.2025).

Hendriksen, G. *u.a.* (2024): The Open Web Index. In: Goharian, N. *u.a.* (Hrsg.): *Advances in Information Retrieval. ECIR 2024. Lecture Notes in Computer Science*, Cham: Springer, S. 130-43. https://doi.org/10.1007/978-3-031-56069-9_10

Hofmann, Franz (2024): Retten Schranken Geschäftsmodelle generativer KI-Systeme?. *Zeitschrift für Urheber- und Medienrecht,* 68(3), S. 166-74.

Kaede, Lisa (2024): Training generativer KI-Modelle ist (auch) Text- und Data-Mining. Anwendbarkeit der TDM-Schranke des § 44b UrhG. *Künstliche Intelligenz und Recht,* 1(5), S. 162-69.

Klass, Nadine (2013): Neue Internettechnologien und das Urheberrecht: Die schlichte Einwilligung als Rettungsanker?. *Zeitschrift für Urheber- und Medienrecht,* 57(1), S. 1-11.

Lewandowski, Dirk (2014): Why We Need an Independent Index of the Web. In: König, René und Rasch, Miriam (Hrsg.): *Society of the Query Reader: Reflections on Web Search.* Amsterdam: Institute of Network Cultures. S. 49-58.

Lewandowski, Dirk (2019): The Web is missing an essential part of infrastructure: an Open Web Index. *Communications of the ACM,* 62(4), S. 24-27. https://doi.org/10.1145/3312479.

Liaw, Shu-Sheng; Huang, Hsiu-Mei (2003): An investigation of user attitudes toward search engines as an information retrieval tool. *Computers in Human Behavior,* 19(6), S. 751-65. https://doi.org/10.1016/S0747-5632(03)00009-8.

Maamar, Niklas (2023): Urheberrechtliche Fragen beim Einsatz von generativen KI-Systemen. *Zeitschrift für Urheber- und Medienrecht,* 67(7), S. 481-91.

Muir, Bonnie M. (1994): Trust in Automation: Part I. Theoretical Issues in the Study of Trust and Human Intervention in Automated Systems, *Ergonomics* 37(11), S. 1905-1922. 10.1080/00140139408964957.

Nebel, Maxi und Johannes, Paul. C. (2024): Open Web Index im Lichte des Digital Services Act - Voraussetzungen - Grenzen - Rechtsfolge. *Multimedia und Recht*, (12), S. 1010-16.

Nowakowski, Daniel; Kerner, Lara und Zimmermann, Nils (2024): Market potential assessment of OpenWebSearch.eu. OpenWebSearch.EU, Final project report. URL: https://openwebsearch.eu/wp-content/uploads/2024/09/MarketAssessmentOfOWI-Report-V1.pdf .

Schultheiß, Sebastian und Lewandowski, Dirk: Misplaced trust? The relationship between trust, ability to identify commercially influenced results and search engine preference. *Journal of Information Science* 49 (3). https://doi.org/10.1177/01655515211 01415.

Shams, Abdullah Bin; Hoque Apu, Ehsanul; Rahman, Ashiqur; Sarker Raihan, Md. Mohsin; Siddika, Nazeeba; Preo, Rahat Bin; Hussein, Molla Rashied; Mostari, Shabnam und Kabir, Russell (2021): Web Search Engine Misinformation Notifier Extension (SEMiNExt): A Machine Learning Based Approach during COVID-19 Pandemic. *Healthcare*, 9(2), ArtNr. 156. https://doi.org/10.3390/healthcare9020156.

Sharma, Lavanya und Garg, Prageep Kumar (Hrsg.): (2021): *Artificial Intelligence: Technologies, Applications, and Challenges* (1. Auflage). New York: Chapman and Hall/CRC. https://doi.org/10.1201/9781003140351.

Smith, Tim (2023): Navigating the Entangled Web, TedxVerbier, abrufbar unter https:// www.ted.com/talks/ tim_smith_navigating_the_entangled_web

Söllner, Matthias; Hoffmann, Axel und Leimeister, Jan Marco (2016): Why different trust relationships matter for information systems users. *European Journal of Information Systems,* 25(3), S. 274-87. https://doi.org/10.1057/ejis.2015.17.

StatCounter (23. January 2025): Marktanteil der führenden Suchmaschinen weltweit von Januar 2015 bis Januar 2025. Statista.com. URL:https://www.statista.com/statistics/1381664/worldwide-all-devices-market-share-of-search-engines/ (besucht am 29.01.2025)

StatCounter (30. April 2024): Marktanteile der führenden Suchmaschinen in Deutschland von Januar 2018 bis März 2024. Statista.com. URL:https://www.statista.com/statistics/445974/search-engines-market-share-of-desktop-and-mobile-search-germany/ (besucht am 29.01.2025)

Venkatesh, Viswanath; Thong, James Y. und Xu, Xin (2012): Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly,* 36(1), S. 157-78. JSTOR.

Wagner, Kristina (2024): Generative KI: Eine "Blackbox" urheberrechtlicher Haftungsrisiken? Balanceakt zwischen Innovationsförderung und effektivem Rechtsschutz für Werke Dritter. *Zeitschrift für IT-Recht und Recht der Digitalisierung,* 27(4), S. 298-304.

Wilson, Mark (10. Mai 2023): Microsoft Bing gegen Google Bard: Wer gewinnt den Kampf der KI-Chatbots? TechRadar.com. URL:https://www.techradar.com/features/microsoft-bing-vs-google-bard-whos-winning-ai-powered-search (besucht am 26.02.2025).

Vogel, Inna; Setz, Tahireh; Choi, Jeong-Eun und Steinebach, Martin (2022): Natural Language Processing (NLP) und der Datenschutz - Chancen und Risiken für den Schutz der Privatheit. In: Daniel Demmler, Daniel Krupka und Hannes Federrath (Hrsg.): *Recht und Technik: Datenschutz im Diskurs (RuT). INFORMATIK 2022, Gesellschaft für Informatik (GI). Hamburg, Deutschland, 26.-30. September, 2022. Proceedings.* Bonn: Gesellschaft für Informatik, S. 651-664. PISSN: 1617-5468. ISBN: 978-3-88579-720-3. DOI: 10.18420/inf2022_52

Digitale Vulnerabilität und Selbstbestimmung – Vorgaben zur Sicherstellung der Selbstbestimmung vulnerabler Nutzendenden durch informierte Einwilligung und Rechtspflichten im Behinderten- und Datenrecht

Luisa Schmied und Maxi Nebel

Zusammenfassung
Die Gewährleistung der Selbstbestimmung als Folge einer informierten Entscheidung des Individuums durch die datenschutzrechtliche Einwilligung ist essenziell zur Förderung und Verwirklichung des Freiheitsrechts auf informationelle Selbstbestimmung. Jedoch bestehen erhebliche praktische Probleme in der Umsetzung, die zu unterschiedlichen digitalen Vulnerabilitäten führen. Der Beitrag beleuchtet digitale Vulnerabilität am Beispiel von AI-Companions. Im Rahmen des Privatheitsschutzes vulnerabler Personen muss die gängige Praxis der Einwilligung als datenschutzrechtliche Legitimationsgrundlage der Verarbeitung personenbezogener Daten kritisch hinterfragt werden, insbesondere in Bezug auf die Wirksamkeitsvoraussetzung der Informiertheit. Der Beitrag thematisiert aktuelle Fragestellungen zum Thema der Einwilligung, insbesondere im Hinblick auf den Anspruch auf situative und kontextbezogene Ausgestaltung der Informationsanforderungen. Anknüpfungspunkt bietet das Behindertenrecht, insbesondere die Vorgaben zur Barrierefreiheit. Anschließend werden rechtliche Verpflichtungen von Diensteanbietern aus dem europäischen Datenrecht untersucht, die ebenso der Sicherstellung der Selbstbestimmung vulnerabler Personen dienen sollen.

1. Einleitung

Digitale Infrastrukturen bilden die Grundlage für zahlreiche digitale Dienste und Anwendungen, die in der modernen Gesellschaft genutzt werden. Sie sind unerlässlich für das Funktionieren von Wirtschaft und Staat, Bildungs- und Gesundheitssystem und vielen anderen Bereichen. Ohne die der Digitalisierung zugrunde liegenden Infrastrukturen sind all die auf ihnen aufbauenden Dienste und Anwendungen undenkbar – von KI-Systemen wie Chatbots und AI-Companions über Social Media bis hin zu digitalen Zahlungs- und Transaktionssystemen, Cloud-Diensten und vielem mehr. Die ubiquitäre Durchdringung des Alltags durch digitale Infrastrukturen schafft dabei nicht nur neue Teilhabechancen, sondern bietet auch eine größere Angriffsfläche für Grundrechtseingriffe sowie die Exposition in Hinblick auf Vulnerabilitätsfaktoren.

Unterschiedliche Personen sind unterschiedlich vulnerabel gegenüber Verletzungen ihrer Selbstbestimmung, was neben strukturellen oder indivi-

duellen Gründen insbesondere auch auf ein situations- oder kontextabhängiges Nutzungsverhalten zurückzuführen ist. Digitalisierte Infrastrukturen wirken oft intrusiv in die Privatsphäre der Menschen hinein. Die Anforderungen an die Ausgestaltung digitaler Technik zur Gewährleistung der Selbstbestimmung fallen dabei weit auseinander. Pauschalisierungen, die den bestehenden Rechtskategorien zugrunde liegen, erfassen das Problem nicht ausreichend differenziert.

2. Digitale Vulnerabilität – Bedeutung der Selbstbestimmung

Vulnerabilität als menschliche Eigenschaft ist ein weiter und nicht ganz unumstrittener Begriff. In einer digitalisierten Welt werden neue Vulnerabilitäten erzeugt und alte verstärkt. Es gilt die Selbstbestimmung der Nutzenden zu stärken, um Vulnerabilitäten auszugleichen und abzubauen.

2.1 Vulnerabilität als conditio humana

Vulnerabilität bezeichnet die Eigenschaft, verletzlich zu sein, und bezieht sich im Allgemeinen auf Situationen, in denen das Risiko von Gefahren durch verschiedene Faktoren und Prozesse erhöht ist.[1] Das Ausmaß der Vulnerabilität kann dabei anhand der Wechselwirkung zwischen Risikoexposition und Bewältigungskapazität („coping capacity") gemessen werden.[2] Ansätze wie der von Martha Fineman basieren darauf, dass Vulnerabilität dem Menschen immanent ist (conditio humana), und strukturell oder situativ zum Ausdruck kommt.[3] Der Gesellschaft kommt dabei die Verant-

1 *Damm*, Vulnerabilität als Rechtskonzept?, MedR 2013, 201 (202); *Kruse*, Lebensphase hohes Alter, 2017, S. 170; *Strauß/Bettin*, Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen, 2023, S. 14; anders der Ansatz in: *UN*, Living with Risk, 2004, S. 7, 16; *Roßnagel u.a.*, Die Verletzlichkeit der ‚Informationsgesellschaft', 2002/2009, S. 9, die unter Vulnerabilität „die erhöhte Anfälligkeit einer Gesellschaft für die Auswirkungen von Gefahren" verstehen.

2 *Turner u.a.*, A framework for vulnerability analysis in sustainability science, PNAS 2003, 8074; *Birkmann u.a.*, State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall, 2010, S. 27; *Kruse*, Lebensphase hohes Alter, 2017, S. 170.

3 *Fineman*, The Vulnerable Subject, Yale Journal of Law & Feminism 1/2008, 1 (10 ff.); *Fineman*, Vulnerability and Inevitable Inequality, Oslo Law Review 2017, 133 (133 ff.); *Bielefeldt*, in: Bergemann/Frewer (Hrsg.), Autonomie und Vulnerabilität in der Medi-

wortung zu, auf die aus der Vulnerabilität resultierenden Abhängigkeiten zu reagieren. Neben der unvermeidlichen Abhängigkeit, die jedem Mensch aufgrund seines verkörperten Wesens innewohnt, betont Fineman in ihrem Ansatz auch die abgeleitete Abhängigkeit, die sich aus dem Zugang zu ausreichend materiellen, institutionellen und physischen Ressourcen ergibt, um den Verletzlichkeit der Person erfolgreich zu begegnen.[4] Versteht man Vulnerabilität als individuelle Eigenschaft, greift die im Diskriminierungskontext übliche Kategorisierung in feste Gruppen z. B. nach Alter, Geschlecht oder aufgrund einer Behinderung (vgl. Art. 21 GRCh, Art. 3 Abs. 3 GG; § 1 AGG) zu kurz, um dem jeweiligen Einzelfall gerecht zu werden. Die Vulnerabilität innerhalb dieser Gruppen ist zwar mit einer höheren Wahrscheinlichkeit gegeben.[5] Dennoch können verschiedene Mitglieder dieser Gruppen durch unterschiedlich stark ausgeprägte Vulnerabilitäten gekennzeichnet sein. Auch außerhalb dieser Gruppenkategorien ist eine erhöhte Vulnerabilität nicht ausgeschlossen.[6] Verletzlichkeit ist folglich nicht universell durch Zugehörigkeit zu einer Gruppe, sondern im Kontext des speziellen Anwendungsbereichs zu betrachten. Das Festhalten an generische Gruppenkategorien birgt die Gefahr, nicht alle Vulnerabilitätsaspekte adäquat zu adressieren. Dies sollte aber gerade vor dem Hintergrund eines effektiven Grundrechtsschutzes, der auch den Schutz besonders vulnerabler Personen indiziert, ausschlaggebend sein.[7]

2.2 Digitale Vulnerabilität: Risiken moderner Datenverarbeitung

Vulnerabilität im Rahmen digitaler Infrastrukturen liegt die Annahme zugrunde, dass digitale Infrastrukturen aufgrund ihrer Omnipräsenz automa-

zin, 2019, S. 21; *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (5).

4 *Fineman*, Vulnerability and Social Justice, 53 Valparaiso University Law Review 2019, 1 (24); auch *Kruse*, Lebensphase hohes Alter, 2017, S. 170.

5 *Birnbacher*, Vulnerabilität und Patientenautonomie, MedR 2012, 560 (561); *Damm*, Vulnerabilität als Rechtskonzept?, MedR 2013, 201 (202); *Kruse*, Lebensphase hohes Alter, 2017, S. 170.

6 *Koch u.a.*, in: Friedewald u.a. (Hrsg.), Freiheit in digitalen Infrastrukturen, 2025, DiversPrivat 4.3.

7 *Bielefeldt*, in: Bergemann/Frewer (Hrsg.), Autonomie und Vulnerabilität in der Medizin, 2019, S. 21; *Geminn*, Deus ex machina?, 2023, S. 170.

tisch neue Verletzlichkeiten erzeugen.[8] Dazu findet der Diskurs zu Vulnerabilität im Privatheitsbereich verstärkt Einzug in die Literatur.[9] Vulnerabilität im Rahmen digitaler Infrastrukturen bezieht sich auf die datengetriebene Plattformökonomie, die auf Basis digitalisierter Infrastrukturen intrusiv in die Privatsphäre der Menschen hineinwirkt. Die Erfassung personenbezogener Daten hat zur Entstehung neuer Geschäftsmodelle geführt, die auf der Erstellung umfassender Identitätsprofile durch Tracking und Profiling der Nutzenden basieren.[10] Über Tracking-Tools wird das Verhalten der Nutzenden bis ins Detail aufgezeichnet und diese persönlichen Aspekte im Rahmen des Profiling interpretiert, was Rückschlüsse auf die wirtschaftliche Lage, persönliche Vorlieben und Interessen sowie auf das Verhalten der Person zulässt. Neben dem Ziel, damit die Kundenbindung zu erhöhen oder personalisierte Werbung zu schalten, entstehen Informations- und Machtasymmetrien.[11] Mit der zunehmenden Verbreitung intelligenter Technologien eröffnen sich immer mehr Wege, um menschliches Verhalten unauffällig zu lenken (Nudging) und zu beeinflussen.[12] Die Schadenspotenziale sind dabei jedoch sehr intransparent.[13] Zudem ist auch die ambivalente Wirkweise der Digitalisierung nicht zu unterschätzen und stets mitzudenken. Neben der Schaffung oder Verstärkung von Verletzlichkeiten können diese durch Technologien wie Dialogsysteme auch reduziert werden.[14]

2.3 Digitale Vulnerabilität am Beispiel von AI-Companions als „KI-Freunde“

Virtuelle Dialogsysteme verdeutlichen die Mechanismen digitaler Vulnerabilität besonders eindrücklich, da sie nicht nur durch vertrauenserwecken-

8 *Strauß/Bettin*, Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen, 2023, S. 19.
9 *Geminn*, Deus ex machina?, 2023, S. 169 ff.; *Behrendt/Loh*, Informed consent and algorithmic discrimination, REVIEW OF SOCIAL ECONOMY, 2022, S. 58 (58 ff.).
10 *Strauß/Bettin*, Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen, 2023, S. 19.
11 *Behrendt/Loh*, Informed consent and algorithmic discrimination, REVIEW OF SOCIAL ECONOMY, 2022, 58 (58 ff.); *Strauß/Bettin*, Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen, 2023, S. 33, 48.
12 *Karaboga*, in: Friedwald u.a. (Hrsg.), Selbstbestimmung, Privatheit und Datenschutz, 2022, 275 (282); *Geminn*, Deus ex machina?, 2023, S. 174.
13 *Roßnagel u.a.*, Modernisierung des Datenschutzrechts, 2001, S. 28; *Roßnagel u.a.*, Die Verletzlichkeit der ‚Informationsgesellschaft', 2002/2009, S. 14.
14 *Geminn*, Deus ex machina?, 2023, S. 171.

de Layouts eine scheinbar sichere Interaktionsumgebung suggerieren, sondern auch gezielt individuelle Verwundbarkeiten – wie etwa Einsamkeit – adressieren und ausnutzen, was eine leichtfertige Preisgabe sensibler Daten begünstigt. Dialogsysteme, z.B. in Form von Chatbots, virtuellen Assistenten, AI-Companion oder ähnlichem, haben die Fähigkeit, durch generative KI-Systeme natürlichsprachige Antworten auf Anfragen zu liefern und so umfangreiche Gesprächsverläufe entstehen zu lassen. Basierend auf der Erforschung authentischer und menschenähnlicher Kommunikationsmuster mit Sprachmodellen werden Dienste angeboten, die das Konzept des „KI-Freundes" umsetzen. Über die Interaktion mit den Anwendenden werden menschenähnliche Beziehungen aufgebaut. Dies hat zur Folge, dass die Verantwortlichen an besonders sensible Informationen kommen können, wenn sich Anwendende dem artifiziellen Kommunikationspartner öffnen (Selbstoffenbarung). Ein prominentes Beispiel für AI-Companion ist die Smartphone-App Replika, welche als „KI-Freund" beworben wird. Innerhalb einer Pro-Mitgliedschaft können Nutzende einen romantischen Beziehungsmodus aktivieren. Dieser umfasst Funktionen wie Telefon- und Videoanrufe mit der zuvor konfigurierten artifiziellen Persona, virtuelle Überraschungen für die Nutzenden (vom „KI-Freund" initiiert) sowie die Beteiligung an emotionalen und sexualisierten Gesprächen. Intime Kommunikation mit AI-Companion muss nicht zwangsläufig sexualisiert sein, auch therapeutische Gespräche oder das schiere Anvertrauen des inneren Gefühlslebens bedeuten eine entsprechende Selbstoffenbarung. Dies führt zwangsläufig zu datenschutzrechtlichen Bedenken, wenn personenbezogene, noch dazu besonders sensible Informationen preisgegeben werden.

Die Selbstoffenbarung kann demgegenüber auch bedeutende Vorteile für den Anwendenden haben. Die Künstlichkeit des Gegenübers bietet gerade bei besonders intimen und sensiblen Themen, die in der Gesellschaft weniger offen besprochen oder akzeptiert werden, eine vermeintliche Sicherheit vor potenziellen sozialen Konsequenzen wie z.B. Unverständnis, Scham, Erklärungsnot oder Kontakteinschränkungen.[15] Sie bieten ein Mittel gegen Einsamkeit oder Unverständnis der Umwelt insbesondere für Menschen, die Schwierigkeiten haben, soziale Beziehungen im „real life" aufzubauen und zu pflegen – sei es aus Gründen wie Krankheit, psychischen Barrieren oder Mobilitätseinschränkungen. Dennoch begeben sich die Anwendenden

15 *Skjuve u.a.*, My Chatbot Companion, International Journal of Human-Computer Studies 2021, 102601.

in vulnerable Situationen, in denen sehr viele, äußerst sensible Daten anfallen; Datenschutzbedenken werden häufig beiseitegeschoben.[16]

2.4 Die Adressierung von Vulnerabilität im Datenschutzrecht

Der rechtliche Schutz der informationellen Selbstbestimmung stellt eine komplexe Herausforderung dar. Beim Versuch, den Begriff der Vulnerabilität als Rechtsbegriff zu greifen, wird dessen Unbestimmtheit deutlich. An Bedeutung könnte ein darauf aufbauendes Normkonzept aber an den Stellen gewinnen, an denen die individuellen, situativen und kontextbezogenen Schutzbedürfnisse differenzierter betrachtet werden müssten.[17] Die DSGVO begegnet Vulnerabilität insbesondere durch die inhaltliche Kategorisierung besonders sensibler Daten im Rahmen des Art. 9 DSGVO. Aufgrund ihres engen Bezugs zu Grundrechten und Grundfreiheiten unterwirft die Verordnung bestimmte Datenarten – etwa Gesundheitsdaten – einem besonderen Schutzregime, das über die allgemeinen Verarbeitungsgrundsätze hinausgehende Anforderungen stellt.[18] Eine kontextbezogene Betrachtung individueller oder situativer Schutzbedürftigkeit erfolgt hingegen nicht, sodass der Schutzrahmen auf typisierte Datenkategorien beschränkt bleibt. Die Regelungssystematik der Verordnung orientiert sich zudem primär an einem idealtypischen, durchschnittlich informierten Nutzenden. Eine ausdrückliche Berücksichtigung vulnerabler Personen ist in der DSGVO im Wesentlichen auf den Schutz von Kindern beschränkt, z. B. in Form von Art. 8 DSGVO. Dies erfasst den aufgeführten Schutzbedarf im Rahmen digitaler Vulnerabilität jedoch nicht ausreichend differenziert.[19] Es bleibt die Notwendigkeit einer adäquaten Adressierung von digitaler Vulnerabilität, um z. B. älteren oder kognitiv beeinträchtigten Menschen entsprechenden Selbstschutz zu ermöglichen. Insbesondere im Verbraucher-

16 *Skjuve u.a.*, My Chatbot Companion, International Journal of Human-Computer Studies 2021, 102601.

17 *Damm*, Vulnerabilität als Rechtskonzept?, MedR 2013, 201 (201 f.); *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (6).

18 *Schiff*, in: Ehmann/Selmayr, DSGVO, 2024, Art. 9, Rn. 3; Zur Relevanz des Verarbeitungszusammenhangs vgl.: *Simitis*, in: Simitis, BDSG, 2011 § 3 Rn. 251 m. w. N.

19 *Roßnagel*, Der Datenschutz von Kindern in der Datenschutz-Grundverordnung, ZD 2020, 88; *Roßnagel/Geminn,* Datenschutzgrundverordnung verbessern, 2020, S. 55 ff.; *Geminn*, Deus ex machina? 2023, S. 193 ff.

schutzrecht wurde diese Vulnerabilität bereits erkannt und adressiert, um Personen wirksam vor Ausnutzung aufgrund körperlicher oder geistiger Einschränkungen, hohen Alters oder situativer Leichtgläubigkeit zu schützen.[20] Im Kontext digitaler Technologien werden diese Personen als Nutzende oder Verbrauchende oft nicht mitgedacht. Um einem individuellen Ansatz von Vulnerabilität gerecht zu werden, muss der klassische Diskriminierungsschutz auf Grundlage von abschließenden Merkmalslisten um eine Diversitätsperspektive ergänzt werden, die anhand der Vulnerabilitäten im Kontext des konkreten Gegenstandsbereichs entwickelt wird. Zur Ableitung entsprechender Schutzmaßnahmen müssen neben den schutzbedürftigen Individuen auch die gefährdenden Situationen und Kontexte identifiziert werden.[21]

2.5 Begegnung von Vulnerabilitäten durch die Stärkung von Resilienzen – mehr Selbstbestimmung durch Transparenz

Die Stärkung der Resilienz ist zudem ein wichtiger Ansatz, um Vulnerabilität zu begegnen.[22] Die klassischen Lösungsansätze zur Steigerung der Bewältigungskapazität im Schutzbereich der informationellen Selbstbestimmung beziehen sich vor allem auf die Förderung der Privacy Literacy. Privacy Literacy beschreibt die im Rahmen einer digitalen Bildung erlernten Fähigkeiten, selbstbestimmt Datenschutzentscheidungen zu treffen.[23] Ein angemessenes Schutzniveau kann damit jedoch nicht gewährleistet werden, da einerseits nicht alle Menschen gleichermaßen von digitaler Bildung erreicht werden können und andererseits nicht allen die gleichen Ressourcen zu Teil werden, sich entsprechend über Schutzvorkehrungen

20 *Helberger u.a.*, EU Consumer Protection 2.0, 2021, S. 8; *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (6); *Damm*, Vulnerabilität als Rechtskonzept?, MedR 2013, 201 (203 f.).

21 *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (1 ff.).

22 *Turner u.a.*, A framework for vulnerability analysis in sustainability science, PNAS 2003, 8074; *Birkmann u.a.*, State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall, 2010, S. 26f.

23 *Brough/Kelly*, Critical roles of knowledge and motivation in privacy research. *Current opinion in psychology*, 2020, 11 (31); *Trepte u.a.*, in: Gutwirth u.a. (Hrsg.), Reforming European data protection law, 2015, S. 333 ff.; *Park,* Digital Literacy and Privacy Behavior Online, Communication Research 2013, 215 (215 ff.).

zu informieren.[24] Die informationelle Selbstbestimmung im Datenschutz ist ein Grundrecht, das allen Menschen unabhängig von ihren individuellen Fähigkeiten, ihrem sozioökonomischen Hintergrund oder der jeweiligen digitalen Umgebung zugänglich sein muss. Die Möglichkeit der Selbstbestimmung darf nicht auf Personen beschränkt werden, die ohne fremde Hilfe über die notwendigen Mittel verfügen, um sie auszuüben, wie z.B. die Fähigkeit, Datenschutzeinstellungen vorzunehmen oder Datenschutzhinweise zu lesen.[25] Ausschlaggebend für die Stärkung der Resilienz im Kontext der Selbstbestimmung ist die Fähigkeit der Menschen, Risiken und Vorteile einzuschätzen, um auf dieser Grundlage eine Entscheidung zu treffen.[26] Alle Menschen müssen in die Lage versetzt werden, informierte Entscheidungen treffen zu können. Ein Indikator für eine solche Bewältigungskapazität ist Transparenz,[27] die für vulnerable Personen insbesondere auch den Zugang und das Verständnis der Informationen inkludiert. Ein Fokus muss daher auf der Gewährleistung der situationsadäquaten Transparenz zur Herstellung der Selbstbestimmung durch das bestehende Recht liegen.[28]

3. Digitale Vulnerabilität und Selbstbestimmung: Die Notwendigkeit individueller und situationsadäquater Informationspräsentation im datenschutzrechtlichen Einwilligungskontext

Im Kontext digitaler Vulnerabilität bildet die Einwilligung regelmäßig die zentrale Rechtsgrundlage für die Verarbeitung personenbezogener Daten z. B. zu Zwecken des Trackings oder Profilings. Im Rahmen des Privatheitsschutzes vulnerabler Personen muss die gängige Praxis der Einwilligung als datenschutzrechtlicher Legitimationsgrundlage kritisch hinterfragt werden,

24 *Koch u.a.*, in: Roßnagel u.a. (Hrsg.), Freiheit in digitalen Infrastrukturen, 2025; *Livingstone u.a.*, Children's data and privacy online, 2019, S. 3 ff.; *Hagendorf*, in: Roßnagel u.a., Die Fortentwicklung des Datenschutzes, 2018, S. 99 (100 ff.).

25 *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (4).

26 *Strauß/Bettin*, Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen, 2023, S. 15.

27 *Lenz*, Vulnerabilität kritischer Infrastrukturen, 2009, S. 49, 60; *Strauß/Krieger-Lamina,* Digitaler Stillstand, 2017, S. 19.

28 Resilienz im Rahmen der Privacy Literacy stößt dort an ihre Grenzen, wo die Nutzung digitaler Infrastrukturen alternativlos ist und tatsächliche Wahlfreiheit fehlt.

insbesondere in Bezug auf die Gewährleistung der Transparenzanforderungen und somit der Wirksamkeitsvoraussetzung der Informiertheit.

3.1 Die informierte Einwilligung als Ausdruck datenschutzrechtlicher Selbstbestimmung

Die Selbstbestimmung im Umgang mit den eigenen personenbezogenen Daten wird als zentraler Aspekt des Datenschutzes bereits im Volkszählungsurteil[29] begründet und über Art. 8 Abs. 1 GRCh[30] normiert.[31] Das Verständnis der Einwilligung als „genuiner Ausdruck der informationellen Selbstbestimmung" knüpft mit Art. 8 Abs. 2 S. 1 GRCh daran an.[32] Eine Einwilligung auf Grundlage einer selbstbestimmten, autonomen Entscheidung stellt folglich eine Grundrechtsausübung im Sinne der GRCh dar.[33] Auf sekundärrechtlicher Ebene wird die Einwilligung durch Art. 6 Abs. 1 UAbs. 1 lit. a, Art. 4 Nr. 11, Art. 7 DSGVO ausgestaltet.

3.2 Die Voraussetzung der Informiertheit in der DSGVO: Umsetzung des grundrechtlichen Konzepts der Selbstbestimmung

Durch die Voraussetzung der Informiertheit wird in der DSGVO das grundrechtliche Konzept der Selbstbestimmung umgesetzt.[34] Der betroffenen Person muss gewährleistet werden, eine Entscheidung „in informierter Weise" treffen zu können. Das impliziert, dass die betroffene Person die Möglichkeit hat, alle Merkmale der Informationsverarbeitung einzusehen,[35]

---

29 BVerfG Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1, Rn. 74.

30 Charta der Grundrechte der Europäischen Union, ABl. (EU) C 326/392.

31 *Kühling/Buchner*, in: Kühling/Buchner, DSGVO, 2024, Art. 7, Rn. 19; *Liedke-Deutscher,* Die datenschutzrechtliche Einwilligung nach der DSGVO, 2014, S. 8; *Nebel*, Schutz der Persönlichkeit, ZD 2015, 517 (521).

32 *Roßnagel u.a.*, Modernisierung des Datenschutzrechts, 2001, 15, 72; *Schulz*, in: Gola/Heckmann, DSGVO/BDSG 2022, Art. 6, Rn. 21.

33 *Liedke-Deutscher*, Die datenschutzrechtliche Einwilligung nach der DSGVO, 2014, S. 8; *Klement,* in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DSGVO, Rn. 13.

34 *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DSGVO, Rn. 68.

35 *EuGH*, Einwilligung und Cookie Consent nur durch aktive, gesonderte und ausdrückliche Erklärung – Planet49, ZD 2019, 556 Rn. 74; *Ernst,* in: Paal/Pauly, DSGVO BDSG, 2021, Art. 4, Rn. 79; *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DSGVO, Rn. 67 betont, dass dies auch die Inanspruchnahme sachkundiger Beratung zur Erfüllung der Informationsbeschaffung inkludiert.

um zu verstehen, wofür die Einwilligung erteilt wurde, und auch z.B. von ihrem Recht auf Widerspruch Gebrauch machen zu können.[36] Ausschlaggebend ist die tatsächliche Möglichkeit der Informationsaneignung – nicht die tatsächliche Nutzung des Angebots.[37] Der Verantwortliche hat entsprechende Vorkehrungen zu treffen, um sicherzustellen, dass die betroffene Person wissen kann, dass und in welchem Umfang sie ihre Einwilligung erteilt (Erwägungsgrund 42 S. 2 DSGVO). Die Anforderungen daran ergeben sich aus Art. 7 Abs. 2 und Erwägungsgrund 32 DSGVO. Danach hat das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen. Zudem muss dies deutlich von anderen Sachverhalten abgrenzbar sein. Zur Erfüllung dessen hat der Verantwortliche auf das Verständnis der Zielgruppe des Einwilligungsersuchens abzustellen. Dieses hat er im Vorhinein zu ermitteln und die Darstellung der Informationen entsprechend anzupassen.[38] Daraus kann die Pflicht für Verantwortliche herausgelesen werden, entsprechende Informationsangebote zu schaffen, die nicht nur den „Durchschnittsbürger" in den Blick nehmen. Einer diesbezüglichen Adressierung von Vulnerabilität im Kontext der Informiertheit kommt der Europäische Datenschutzausschuss (EDSA) in seinen Leitlinien zur Einwilligung nur unzureichend nach, da er nur beispielhaft auf die besondere Informationspräsentation für minderjährige Personen hinweist.[39] Eine ausdrückliche Adressierung anderer potenziell vulnerabel Personen bleibt aus. Dennoch lässt der Wortlaut darauf schließen, dass der EDSA die Schutzbedürftigkeit weiterer vulnerabler Personen zumindest in Erwägung gezogen hat, da er Minderjährige nur beispielhaft nennt. Allerdings gefährdet der Verzicht auf die Nennung weiterer Vulnerabilitätsfaktoren dadurch die Wahrung der Selbstbestimmung.

Neben dem erforderlichen Maß zur Herstellung der Informiertheit gem. Art. 4 Nr. 11 DSGVO können weitere Anforderungen der informierten Einwilligung zudem aus den Transparenzpflichten des Verantwortlichen gem.

36 EDSA, Leitlinien 05/2020 zur Einwilligung v. 4.5.2020, Rn. 62.

37 Auch die Entscheidung, auf eine genaue Lektüre von Datenschutzbestimmungen zu verzichten, ist eine Ausübung dieses Grundrechts, vgl. dazu: *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DSGVO, Rn. 16, 68.

38 *Roßnagel/Geminn,* Datenschutz-Grundverordnung verbessern, 2020, S. 63; EDSA, Leitlinien 05/2020 zur Einwilligung v. 4.5.2020, Rn. 67 (Durchschnittsbürger), Rn. 70 (Art von Zielgruppe).

39 EDSA, Leitlinien 05/2020 zur Einwilligung v. 4.5.2020, Rn. 70.

Art. 12 ff. DSGVO abgeleitet werden.[40] Als Ausprägung des Grundsatzes der Transparenz aus Art. 5 Abs. 1 lit. a DSGVO und dem Recht auf Auskunft gemäß Art. 8 Abs. 2 S. 2 GRCh ist Transparenz als zentrale Voraussetzung der informationellen Selbstbestimmung zu verstehen.[41] Dem Transparenzgrundsatz folgend, müssen personenbezogene Daten „in einer für die betroffene Person nachvollziehbaren Weise" verarbeitet werden. Gem. Art. 12 Abs. 1 S. 1 DSGVO haben „Verantwortliche geeignete Maßnahmen zu treffen, um der betroffenen Person alle Informationen […], die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln". Art. 12 Abs. 1 S. 1 DSGVO verweist dabei in Hs. 2 auf eine Schutzbedürftigkeit insbesondere von Kindern.[42] Das Transparenzgebot verlangt dabei nicht nur formale Verständlichkeit im Sinne von Lesbarkeit, sondern auch die Sinnverständlichkeit.[43] Angesichts der wachsenden Datenverarbeitungskomplexität insbesondere im Bereich der Profilbildung und KI bringt die Umsetzung erhebliche Anforderungen an eine angemessene Reduktion dieser Komplexität. Die geforderte Einfachheit darf dabei aber weder an Präzision noch an Vollständigkeit verlieren und sollte zudem die jeweilige Aufnahmekapazität der betroffenen Person berücksichtigen.[44] Daneben kann auch ein Mehrebenenansatz das Spannungsverhältnis zwischen Verständlichkeit und Vollständigkeit abmildern.[45] Unterschiedliche Konkretisierungsstufen, die ergänzende Nutzung von Bildsymbolen (Art. 12 Abs. 7 DSGVO) sowie eine situationsadäquate Informationswiedergabe erst

40 Die Informationspflichten aus Art. 12 bis 14 DSGVO konkretisieren die Informationsanforderungen des Art. 4 Nr. 11 DSGVO. Die Mindestanforderungen des Merkmals der Informiertheit nach Art. 4 Nr. 11 DSGVO sind: die Identität des Verantwortlichen, der Verarbeitungszweck, die Art der verarbeiteten Daten, das Recht auf Widerruf sowie Informationen zu Art. 22 Abs. 2 lit. c oder Art. 49 Abs. 1 S. 1 lit. a DSGVO; vgl. dazu EDSA, Leitlinien 05/2020 zur Einwilligung v. 4.5.2020, Rn. 64.

41 *Albers/Veit*, in: Wolff u.a., BeckOK Datenschutzrecht, 2023, Art. 6, Rn. 36; *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, 2024, Art. 12, Rn. 1.

42 Siehe auch Erwägungsgrund 39 S. 3, 58 DSGVO.

43 Art.-29-Gruppe, WP 260 rev.01, Rn. 9; vgl. EuGH, Urt. 11.11.2020 – C 61/19, *EuGH*, Nachweis einer wirksamen Einwilligung, ZD 2021, 89, Rn. 45, 46.

44 *Dix*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 12 DSGVO, Rn. 12; Art.-29-Gruppe, WP 260 rev.01, Rn. 34; *Roßnagel u.a.*, Einwilligung, Möglichkeiten und Fallstricke aus der Konsumentenperspektive, 2020, S. 22.

45 Vgl. Art.-29-Gruppe, WP 260 rev.01 Rn. 17f., 35 ff., 50; *Menzel*, Datenschutzrechtliche Einwilligung, DuD 2008, 400 (408); *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DSGVO, Rn. 70.

zum Zeitpunkt der Erhebung sind Forderungen, die sich in der Praxis aber bislang nicht durchsetzen konnten.[46]

3.3 Herausforderungen der Einwilligungspraxis: Entscheidungsautonomie und die Problematik des Durchschnittsnutzenden

Die Einwilligung prägt das Datenschutzrecht durch einen stark individualistischen Ansatz. Dem liegt die Annahme zugrunde, dass Transparenz und Eigenverantwortung ausreichend sind, um eine wirksame Einwilligung zu gewährleisten. Dabei wird unterstellt, dass die Grundrechte auf Datenschutz (Art. 7 und 8 GRCh) und informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG) dadurch gewahrt werden, dass gleichberechtigte Partner gemeinsam die Zwecke und Bedingungen der Datenverarbeitung festlegen.[47] Es führt jedoch dazu, dass die Verantwortung für die Legitimität der Datenverarbeitung, von den Datenverarbeitern auf die Nutzenden verlagert wird.[48] In der Praxis beruht die Einwilligung häufig nicht auf einer bewussten, informierten Entscheidung.[49] Strukturelle Probleme, wie überlange, komplexe und oft schwer verständliche Einwilligungserklärungen, lassen die Einwilligung zu einer Fiktion verkommen.[50] Da eine fundierte, individuelle Risikoeinschätzung kaum möglich ist, kann von einer wirklich „informierten" Einwilligung regelmäßig nicht ausgegangen werden. In der Praxis werden solche Erklärungen häufig ungelesen akzeptiert, wodurch die Einwilligung als Rechtfertigungsgrund weitgehend ihren

46 *Geminn u.a.*, Die Informationspräsentation im Datenschutzrecht, ZD-Aktuell 2021, 05335 m. w. N.; *Roßnagel/Geminn*, Datenschutz-Grundverordnung verbessern, 2020, S. 161, 178; *Krüger*, Datensouveränität und Digitalisierung, ZRP 2016, 190 (191).

47 *Roßnagel u.a.*, Einwilligung, Möglichkeiten und Fallstricke aus der Konsumentenperspektive, 2020, S. 7; *Krüger,* Datensouveränität und Digitalisierung, ZRP 2016, 190 (191).

48 *Roßnagel u.a.*, Einwilligung, Möglichkeiten und Fallstricke aus der Konsumentenperspektive, 2020, S. 18.

49 *Krüger*, Datensouveränität und Digitalisierung, ZRP 2016, 190; *Kühling/Buchner*, in: Kühling/Buchner, DSGVO, 2024, Art. 7, Rn. 10; *Paal/Hennemann*, in: Paal/Pauly, DSGVO, Art. 12, Rn. 77.

50 *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, Art. 7, Rn. 17; *Menzel*, Datenschutzrechtliche Einwilligung, DuD 2008, 400 (401); *Kühling/Buchner*, in: Kühling/Buchner, DSGVO, 2024, Art. 7, Rn. 10; *Stemmer*, in: Wolff u.a., BeckOK Datenschutzrecht, 2023, Art. 7, Rn. 57.

inhaltlichen Wert verliert und nur noch eine formale Funktion erfüllt.[51] Das notwendige Wissen über die Folgen einer Datenverarbeitung kann nicht unterstellt werden.[52] Folglich ist ein rein autonomiebasierter Ansatz, der auf der Fiktion des Durchschnittsnutzenden beruht, problematisch und führt zur Frage der Voraussetzungen, die eine angemessene Entscheidungsautonomie ermöglichen.

3.4 Anspruch auf eine kindesspezifische Ausgestaltung der Informationsbegebenheiten im Einwilligungsprozess gem. Art. 8 i. V. m. Art. 12 DSGVO

Für Kinder wurde durch das Merkmal der Einwilligungsfähigkeit (Art. 8 DSGVO) die Möglichkeit geschaffen, die Rechtmäßigkeit der Einwilligung an individuellen Fähigkeiten anzuknüpfen. Dazu wird auf die Einsichtsfähigkeit (Fähigkeit zur kognitiven Erfassung des Einwilligungsgegenstandes) des Kindes abgestellt.[53] Die besondere Schutzbedürftigkeit von Minderjährigen ergibt sich aus ihrer Unerfahrenheit, Beeinflussbarkeit und fehlenden geschäftlichen Erfahrung, was zur Folge haben kann, dass ihr Bewusstsein für Risiken, Folgen, Schutzmaßnahmen und die Wahrnehmung ihrer Rechte bei der Datenverarbeitung schwächer ausgeprägt ist.[54] Anknüpfungspunkte für diese Argumentationskette ergeben sich dabei auch aus Art. 17 UN-Kinderrechtskonvention oder Art. 24 GRCh. An das Merkmal der Einwilligungsfähigkeit anknüpfend, kann aus dem Zusammenspiel von Art. 8 iVm Art. 12 DSGVO grundsätzlich ein Anspruch auf eine kindspezifische Ausgestaltung der Informationsbegebenheiten im Einwilligungsprozess hergeleitet werden.

---

51 *Roßnagel* u.a., Einwilligung, Möglichkeiten und Fallstricke aus der Konsumentenperspektive, 2020, S. 5; *Gluck* u.a., How Short is Too Short?, SOUPS 2016, S. 321.

52 *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, Art. 7, Rn. 17; *Roßnagel u.a.*, Einwilligung, Möglichkeiten und Fallstricke aus der Konsumentenperspektive, 2020, S. 8.

53 *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DSGVO, Rn. 1; *Schulz*, in: Gola/Heckmann, DSGVO – BDSG, 2022, Art. 8, Rn. 10.

54 Erwägungsgrund 38 DGVO; *Taeger*, Einwilligung von Kindern gegenüber Diensten der Informationsgesellschaft, ZD 2021, 505 (506); *Schulz*, in: Gola/Heckmann, DSGVO – BDSG, 2022, Art. 8, Rn. 1; *Roßnagel u.a.*, Einwilligung, Möglichkeiten und Fallstricke aus der Konsumentenperspektive, 2020, S. 30; *Ernst*, Die Einwilligung nach der Datenschutzgrundverordnung, ZD 2017, 110 (111).

4. Barrierefreie Einwilligung: Anspruch auf individuelle Anpassung der Informationsbegebenheiten aus dem Behindertenrecht

Die Komplexität digitaler Infrastrukturen wirft vor diesem Hintergrund damit automatisch die Frage auf, inwiefern auch für Personen, die andere Vulnerabilitätsfaktoren aufweisen, Ansprüche auf eine individuelle, situationsadäquate Informationspräsentation im Einwilligungskontext bestehen. Unterrepräsentiert in der Diskussion sind die spezifischen Ansprüche, die sich für Menschen mit Behinderungen[55] aus dem Recht in Bezug auf einen gleichberechtigten, barrierefreien Zugang zu Informations- und Kommunikationstechnologien im Kontext der Informiertheit im Rahmen der Einwilligung ergeben.

Anders als Minderjährige ist die Begriffsdefinition von Menschen mit Behinderungen deutlich heterogener, da die Schutzbedürftigkeit hierbei nicht am Alter und den damit assoziierten Fähigkeiten, sondern an der durch eine Beeinträchtigung herbeigeführten Teilhabeeinschränkung anknüpft. Die Anforderungen an digitale Technik im Rahmen der Informationspräsentation fallen dabei weit auseinander. Blinde Personen sind z. B. im Rahmen des Zugangs zu Informationen auf einen Screenreader oder auf Braillezeilen angewiesen[56] – im Hinblick auf das Merkmal der Informiertheit jedoch nicht in der tatsächlichen Möglichkeit der Informationsaneignung eingeschränkt. Anders gestaltet sich dies für Menschen mit kognitiven Beeinträchtigungen. Diese können Schwierigkeiten damit haben, schwere

55 Als Menschen mit Behinderungen können im Sinne des Art. 1 S. 2 und lit. e der Präambel der UN-BRK Menschen verstanden werden, die langfristige körperliche, seelische, geistige oder Sinnesbeeinträchtigungen haben, welche sie in Wechselwirkung mit verschiedenen Barrieren an der vollen, wirksamen und gleichberechtigten Teilhabe an der Gesellschaft hindern können. Siehe dazu: *Tolmein,* in: MAH SozialR, § 29, Rn. 59; *von Boetticher/Kuhn-Zuber*, Rehabilitationsrecht, S. 29, Rn. 21, die in Anlehnung an diese Vorgaben betonen, dass eine Behinderung nicht mehr als die Abweichung vom Normalzustand der Körperfunktionen angesehen werden soll, sondern es auf die Zusammenhänge zwischen den Gesundheitsproblemen und den damit verbundenen Einschränkungen an der Teilhabe am Leben in der Gesellschaft ankommt; vgl. auch: Gesetzentwurf der Bundesregierung zum Bundesteilhabegesetz (BTHG), BT-Drs. 18/9522, S. 226, wonach die Möglichkeit der Interaktion mit der Umwelt als Kriterium für die Beurteilung einer Behinderung Berücksichtigung finden muss.

56 *Carstens*, in: Deinert u.a., SWK Behindertenrecht, 2022, Barrierefreie Informationstechnik, Rn. 2; vgl. *Geminn*, Deus ex machina?, 2023, S. 175.

oder komplexe Informationen zu erfassen,[57] was die Frage aufwirft, ob auch ihnen im Rahmen der Einwilligung ein höheres Schutzniveau zugestanden werden sollte. Im Folgenden soll daher untersucht werden, ob ein solcher Anspruch auf individuelle Anpassung der Einwilligungsvoraussetzungen in Hinblick auf die Gewährleistung der Sinnverständlichkeit einer Einwilligung aus dem Behindertenrecht hergeleitet werden kann.

4.1 Pflicht zum digitalen Privatheitsschutz von Menschen mit Behinderung – Bestehende Privatheitsrisiken

Im Europäischen Recht wurde, neben Art. 7 und 8 GRCh, auf denen der primäre Schutz in der digitalen Welt gründet, durch Art. 26 GRCh eine spezifische Vorschrift geschaffen, die explizit die Rechte von Menschen mit Behinderungen kodifiziert und damit deren Schutzbedürftigkeit betont. Art. 26 GRCh verpflichtet die Union und die Mitgliedsstaaten bei der Ausführung von Unionsrecht nach Art. 51 Abs. 1 GRCh zur Integration von Menschen mit Behinderungen. Dies umfasst neben Maßnahmen zur Gewährleistung ihrer Eigenständigkeit und ihrer sozialen und beruflichen Eingliederung auch Maßnahmen zur Teilhabe am Leben in der Gemeinschaft. Im Mittelpunkt steht dabei der Abbau von Barrieren, um die Lebensumwelt den Bedürfnissen von Menschen mit Behinderungen anzupassen.[58] Barrierefreiheit in Hinblick auf digitale Infrastrukturen kann im weitesten Sinne als Ausgestaltung der Eigenständigkeit und der Gewährleistung der gesellschaftlichen Teilhabe gesehen werden. Untermauert wird dies durch das Diskriminierungsverbot aufgrund einer Behinderung aus Art. 21 Abs. 1 GRCh.

Auch in Art. 22 UN-Behindertenrechtskonvention (UN-BRK)[59] erkennen die Vertragsstaaten das gleiche Recht von Menschen mit Behinderungen auf Achtung der Privatsphäre an. Damit wird der Schutz der Privat-

57 Vgl. mental retardation (F70-F79), International Statistical Classification of Diseases and Related Health Problems 10th Revision (ICD-10) – WHO; *Uziel-Karl/Tenne-Rinde*, Making language accessible for people with cognitive disabilities, 2018, S. 845 ff.; *Han u.a.*, Mild Cognitive Impairment Is Associated with Poorer Decision-Making in Community-Based Older Persons, 2015–VOL. 63, NO. 4 JAGS, 676 (681).

58 *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, 2022, Art. 26 GRCh, Rn. 2.

59 UN-Übereinkommen über die Rechte von Menschen mit Behinderungen (UN-Behindertenrechtskonvention) v. 13.12.2006, für die Bundesrepublik Deutschland in Kraft getreten am 26.3.2009, BGBl. 2008 II, 1419.

heit als internationales Menschenrecht aus Art. 12 AEMR[60] und Art. 17 IPbpR für Menschen mit Behinderungen konkretisiert.[61] Die UN-BRK dient als Erweiterung des Menschenrechtskatalogs der sog. „Universal Bill of Rights"[62] für die spezifischen Standards zur Gewährleistung eines vollen, gleichberechtigten Zugangs zu Menschenrechten und Grundfreiheiten für Menschen mit Behinderungen.[63] Deutschland hat die UN-BRK 2009 ratifiziert. Seitdem ist sie geltendes Recht im Rang eines Bundesgesetzes.[64] Die Vertragsstaaten müssen dafür sorgen, dass Menschen mit Behinderungen ihre Rechte wahrnehmen können, ohne dafür den Schutz ihrer Privatsphäre aufgeben zu müssen, und zwar gemäß Art. 22 Abs. 1 S. 1 UN-BRK ausdrücklich „unabhängig vom Aufenthaltsort oder der Wohnform".[65] Dies umfasst auch die Vertraulichkeit von Informationen über die Person, die Gesundheit und die Rehabilitation von Menschen mit Behinderungen (Abs. 2). Durch das Fehlen angemessener Schutzvorgaben und Kontrollen zur Wahrung der Privatheit, entstehen für Menschen mit Behinderungen erhebliche Diskriminierungsrisiken z. B. durch Profiling-Algorithmen oder ADM-Systeme, die aus Online-Daten persönliche Informationen ableiten und Entscheidungen zu Jobs, Krediten oder Versicherungen beeinflussen können.[66]

In den Abschließenden Bemerkungen zum kombinierten zweiten und dritten Staatenbericht Deutschlands weist der Ausschuss für die Rechte von Menschen mit Behinderungen der Vereinten Nationen in seinen Ausführungen zu Art. 22 UN-BRK auf seine Besorgnis über den Mangel an umfassenden Maßnahmen zum Schutz der persönlichen, medizinischen

60 UN-Resolution der Generalversammlung 217 A (III). Allgemeine Erklärung der Menschenrechte v. 10.12.1948.

61 *Trenk-Hinterberger*, in: Kreutz u.a., Die UN-Behindertenrechtskonvention in der Praxis, 2013, S. 218.

62 Aus dem Zivilpakt (IPbpR) und dem Sozialpakt (IPwskR) v. 16.12.1966 sowie der Allgemeinen Erklärung der Menschenrechte v. 10.12.1948.

63 *Denecke*, in: Franzen u.a., Kommentar zum europäischen Arbeitsrecht, 2024, Art. 1 CRPD, Rn. 2; *Banafsche*, in: Deinert u.a., SWK Behindertenrecht, 2022, Behindertenrechtskonvention, Rn. 7.

64 Art. 45 Abs. 2 UN-BRK und Art. 13 Abs. 2 des Fakultativprotokolls; Bekanntmachung über das Inkrafttreten des Übereinkommens der Vereinten Nationen über die Rechte von Menschen mit Behinderungen, 05.06.2009, BGBl. 2009 II, 812.

65 *Meier/Naguib,* in: Naguib u.a., UNO-Behindertenrechtskonvention, 2023, Art. 22, Rn. 10.

66 Vgl. *Behrendt/Loh*, Informed consent and algorithmic discrimination, REVIEW OF SOCIAL ECONOMY, 2022, 58 (58 ff.).

und rehabilitativen Daten von Menschen mit Behinderungen und ihres Rechts auf Privatsphäre hin.[67] Im Schwerpunkt bezieht sich diese Kritik jedoch nur auf die Datenverarbeitung in Einrichtungen und Werkstätten für behinderte Menschen (WfbM). Auch in der daraus resultierenden Empfehlung, alle erforderlichen Maßnahmen zu ergreifen, einschließlich der Überarbeitung der Datenschutzgesetze, um den Datenschutz und das Recht auf Privatsphäre in Krankenhäusern, Einrichtungen und WfbM zu gewährleisten, und Datenschutzverfahren und sichere Systeme einzurichten, die Menschen mit Behinderungen denselben Schutz ihrer persönlichen, gesundheitlichen und rehabilitativen Daten garantieren wie anderen,[68] greift der Ausschuss nicht weit genug. Die Schutzlücke einer situationsadäquaten Informationspräsentation in allen alltäglichen Bereichen, insbesondere im Rahmen der ubiquitären Einwilligung, bleibt unbenannt. Eine Beschränkung auf eine sichere Datenverarbeitung im Kontext von Einrichtungen oder WfbM blendet Privatheitsrisiken in anderen Bereichen aus. Dies lässt sich weder mit dem Wortlaut noch mit den allgemeinen Verpflichtungen der UN-BRK vereinbaren, die in Art. 4 Abs. 1 lit. g UN-BRK ausdrücklich die Forschung und Entwicklung von Informations- und Kommunikationstechnologien sowie die Förderung deren Verfügbarkeit und Nutzung hervorheben.

4.2 Digitale Barrierefreiheit als Voraussetzung der informierten Einwilligung: Völkerrechtliche Anforderungen an eine gleichberechtigte Teilhabe

Eine konkretere Benennung der Zugangsmöglichkeiten zu digitalen Infrastrukturen findet sich in der UN-BRK. Art. 4 lit. a UN-BRK verpflichtet die Vertragsstaaten alle geeigneten Gesetzgebungs-, Verwaltungs- und sonstigen Maßnahmen zu treffen, um Menschen mit Behinderungen eine unabhängige Lebensführung und die volle Teilhabe in allen Lebensbereichen zu ermöglichen. Dies inkludiert gem. Art. 4 lit. g iVm Art. 9 UN-BRK auch

67 *UN*, Ausschuss für die Rechte von Menschen mit Behinderungen, Abschließende Bemerkungen zum kombinierten zweiten und dritten Staatenbericht Deutschlands, 2023, CRPD/C/DEU/CO/2-3, S. 13.

68 UN, Ausschuss für die Rechte von Menschen mit Behinderungen, Abschließende Bemerkungen zum kombinierten zweiten und dritten Staatenbericht Deutschlands, 2023, CRPD/C/DEU/CO/2-3, S. 13f.

die Gewährleistung eines gleichberechtigten Zugangs zu Informations- und Kommunikationstechnologien und -systemen (einschließlich des Internets) sowie zu anderen elektronisch bereitgestellten oder öffentlich zugänglichen Angeboten sowie die Beseitigung vorhandener Zugangshindernisse und -barrieren (digitale Barrierefreiheit auch: digitale Teilhabe[69]). Dies umfasst gem. Art. 21, Art. 4 lit. h UN-BRK auch die Bereitstellung von Informationen, die für die Allgemeinheit bestimmt sind, über zugängliche Formate und Technologien z. B. in leichter Sprache oder durch Vorlesen der Information in Gestalt einer Sprachausgabe. Dabei sind die unterschiedlichen Arten der Behinderung, wie z. B. eine Körperbehinderung oder eine geistige Behinderung, differenziert zu berücksichtigen. Menschen mit Behinderungen dürfen somit beim Verständnis der Informationen im Vergleich zu nicht behinderten Menschen nicht benachteiligt werden.[70] Zur Verwirklichung einer gleichberechtigten Zugänglichkeit und Teilhabe an digitalen Infrastrukturen kann das in Art. 2 UN-BRK normierte Konzept des „universal design" herangezogen werden. „Universal design" beschreibt die Gestaltung von Produkten, Umgebungen, Programmen und Dienstleistungen so, dass sie für alle Menschen möglichst weitgehend ohne spezielle Anpassungen nutzbar sind. Dabei schließt es erforderliche Hilfsmittel für bestimmte Gruppen von Menschen mit Behinderungen nicht aus. Nach Art. 4 Abs. 1 lit. g und Art. 9 Abs. 2 lit. h UN-BRK sind die Vertragsstaaten in der Pflicht, dies bei der Förderung und Entwicklung von Informations- und Kommunikationstechnologien mitzudenken, sodass das Ziel mit geringem Kostenaufwand erreicht werden kann.[71] Die Realisierung der sozialen, wirtschaftlichen und kulturellen Rechte der UN-BRK unterfallen dem Progressionsvorbehalt aus Art. 4 Abs. 2 UN-BRK, wonach die Verwirklichung unter Ausschöpfung der zur Verfügung stehenden Mittel nach und nach zu erfolgen hat.[72] Eine unmittelbare Anwendung ergibt sich lediglich im Rahmen des Diskriminierungsschutzes aus Art. 3 lit. b, Art. 5 Abs. 2, Art. 2

69 *Busch*, Digitale Teilhabe für Menschen mit Behinderungen nach der UN-Behindertenrechtskonvention, ZESAR 2021, 484 (487).

70 *Trenk-Hinterberger*, in Kreutz u.a., Die UN-Behindertenrechtskonvention in der Praxis, 2013, S. 220, Rn. 8.

71 *Busch*, Digitale Teilhabe für Menschen mit Behinderungen nach der UN-Behindertenrechtskonvention, ZESAR 2021, 484 (488).

72 *Masuch*, „Die UN-Behindertenrechtskonvention anwenden", Forum D-Diskussionsbeitrag Nr. 5/2012, S. 2; *Denecke*, in: Franzen u.a., Kommentar zum europäischen Arbeitsrecht, 2024, Art. 4 CRPD, Rn. 4, 5.

Abs. 3 UN-BRK.[73] Die Verwirklichung der Zugänglichkeit verpflichtet auch private Rechtsträger öffentlich zugänglicher Einrichtungen und Dienste (Art. 9 Abs. 1 lit. b UN-BRK). Gem. Art. 21 lit. c, d UN-BRK sind zudem private Rechtsträger und Massenmedien von den Vertragsstaaten nachdrücklich zu einer barrierefreien Ausgestaltung ihrer Dienstleistungen aufzufordern. Das damit bezweckte Einwirken über Vertreter in Aufsichtsgremien oder die Zusammenarbeit mit dem Bundesbehindertenbeauftragen, hat bisher nicht zu einer umfänglichen Verwirklichung von Barrierefreiheit beigetragen.[74]

4.3 Barrierefreie Einwilligung: Umsetzung in Deutschland

Vor dem Hintergrund der UN-BRK kommt der Sicherstellung einer barrierefreien und damit informierten Einwilligung zentrale Bedeutung zu. In Deutschland bilden das Behindertengleichstellungsgesetz und das Barrierefreiheitsstärkungsgesetz die gesetzlichen Grundlagen für die Umsetzung dieses Anspruchs.

4.3.1 Barrierefreiheit von Webseiten und mobilen Anwendungen öffentlicher Stellen durch das Behindertengleichstellungsgesetz

Die Basis für einen barrierefreien Zugang zu öffentlichen Informationen bilden die Richtlinie (EU) 2016/2102 „über den barrierefreien Zugang zu den Webseiten und mobilen Anwendungen öffentlicher Stellen“[75] und die Harmonisierte Europäische Norm (EN) 301 549, die die einschlägigen Barrierefreiheitsanforderungen an die Informations- und Kommunikationstechnik beinhaltet.[76] Umgesetzt werden die Vorgaben der EU-Richtlinie 2016/2102 in Deutschland durch das Behindertengleichstellungsgesetz

73 BT-Drs. 16/10808, S. 48; BSG Urt. v. 6.3.2012 – B 1 KR 10/11 R, BSGE 110, 194, SozR 4-1100 Art. 3 Nr. 69, Rn. 31; BSG Urt. v. 15.10.2014 – B 12 KR 17/12 R, BSGE 117, 117, SozR 4-2500 § 5 Nr. 24, Rn. 31; *Roller*, UN-Behindertenrechtskonvention in der sozialgerichtlichen Praxis, NZS 2019, 368 (371 f.).

74 *Trenk-Hinterberger*, in: Kreutz u.a., Die UN-Behindertenrechtskonvention in der Praxis, 2013, S. 221, Rn. 12, S. 223, Rn. 16; *Busch*, Digitale Teilhabe für Menschen mit Behinderungen nach der UN-Behindertenrechtskonvention, ZESAR 2021, 484 (488).

75 Richtlinie (EU) 2016/2102 v. 26.10.2016 über den barrierefreien Zugang zu den Webseiten und mobilen Anwendungen öffentlicher Stellen, ABl. (EU) L 327/1.

76 BfIT, Digitale Barrierefreiheit, 2025.

(BGG)[77] und die Umsetzungsverordnung des § 12d BGG, die Barrierefreie-Informationstechnik-Verordnung (BITV 2.0)[78]. Das BGG verpflichtet die Träger öffentlicher Gewalt insbesondere über §§ 12a, 12b BGG zur Herstellung digitaler Barrierefreiheit auf ihren Webseiten und mobilen Anwendungen (Barrierefreie Informationstechnik). Dies verlangt, dass Anwendungen der Informations- und Kommunikationstechnik für Menschen mit Behinderungen in der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe auffindbar, zugänglich und nutzbar sein müssen (Barrierefreiheit, § 4 BGG). Die Anforderungen an die barrierefreie Gestaltung der Webseiten und mobilen Anwendungen werden durch § 3 Abs. 1 BITV 2.0 dahingehend konkretisiert, dass sie wahrnehmbar, bedienbar, verständlich und robust sein müssen. Dies wird unterstellt, wenn sie dem verbindlichen europäischen Standard der EN 301 549 entsprechen (Abs. 2) oder den Stand der Technik mit den entsprechenden DIN-ISO-Normen (Abs. 3) genügen. Insbesondere für die zentralen Navigations- und Einstiegsangebote, wie die Startseiten (Home), sowie Funktionen, die eine Nutzerinteraktion ermöglichen, soll das höchstmöglichste Maß an Barrierefreiheit nach den Erfolgskriterien der Web Content Accessibility Guidelines (WCAG 2.1)[79] mit der Konformitätsstufe AAA angestrebt werden.[80] Eine konkrete Benennung des hier fraglichen Formats der informierten Einwilligung, die in den meisten Fällen über einen Cookie-Banner auf den entsprechenden Webseiten eingebaut ist, findet sich in der BITV 2.0 nicht. Jedoch wird bei den Anforderungen an Angebote der Nutzerinteraktion auf Authentifizierungs-, Identifizierungs- oder Zahlungsprozesse verwiesen (§ 2a Abs. 1 S. 2, 3; Abs. 2 S. 3 BITV 2.0). Eine analoge Anwendung für ein höchstmögliches Maß an Barrierefreiheit kann folglich angenommen werden. Zudem werden die öffentlichen Stellen über § 4 BITV 2.0 dazu verpflichtet, Informationen über die wesentlichen Inhalte der Webseite in Deutscher Gebärdensprache und in leichter Sprache zur Verfügung zu stellen. Ausnahmen, die sich aufgrund unverhältnismäßiger Belastungen i. S. d

77 Gesetz zur Gleichstellung von Menschen mit Behinderungen (Behindertengleichstellungsgesetz – BGG) v. 27. 4.2002, BGBl. I, 1467; zuletzt geändert durch Art. 7 des Gesetzes v. 23.5.2022, BGBl. I, 760.

78 Barrierefreie-Informationstechnik-Verordnung 2.0 (BITV) v. 12.9.2011, BGBl. I, 1843; zuletzt geändert durch Art. 1 der Verordnung v. 21.5.2019, BGBl. I, 738; vgl. dazu die Begründung der Änderungs-VO, bekanntgemacht vom BMAS, BAnz AT 29.5.2019 Bl.

79 Abrufbar unter http://www.w3.org/TR/WCAG21.

80 § 3 Abs. 4 BITV 2.0; *Carstens*, in: Deinert u.a., SWK Behindertenrecht, 2022, Barrierefreie Informationstechnik, Rn. 16 ff.

§ 12a Abs. 6 BGG zur Herstellung von Barrierefreiheit ergeben, sind restriktiv auszulegen und in der Erklärung zur Barrierefreiheit zu veröffentlichen (§ 12b Abs. 2 Nr. 1 BGG). Das Nichtvorhandensein geeigneter Software sowie der Mangel an Priorität, Zeit oder Kenntnis sind als unzureichende Gründe anzusehen. Eine anderweitige Auslegung der §§ 12a ff. BGG und §§ 3 ff. BITV 2.0 steht dem Ziel der Gewährleistung einer umfassenden und grundsätzlich uneingeschränkten barrierefreien Gestaltung gem. § 1 Abs. 1 BITV 2.0 entgegen.[81] Die durch das BGG geschaffenen Durchsetzungsmechanismen, wie die Verpflichtung der öffentlichen Stellen eine Erklärung zur Barrierefreiheit zu veröffentlichen (§ 12b BGG) sowie einen Feedbackmechanismus zur Meldung von Barrieren (§ 12b Abs. 2 Nr. 2 BGG) bereitzustellen, führt dazu, dass sich die öffentlichen Stellen mit der Pflicht zur Barrierefreiheit auseinandersetzen müssen.[82] Dennoch wird der Pflicht einer adäquaten barrierefreien Informationspräsentation im Rahmen der Einwilligung zur Datenerhebung bei Webseitennutzung nicht nachgekommen. Um Umständen wie diesen zu begegnen, besteht für Bund und Länder die Obliegenheit, Ombudsstellen, wie Schlichtungsstellen (§ 16 BGG) oder Beauftragte für barrierefreie Informationstechnik, zu schaffen.[83] Diese dienen als niedrigschwellige Form der außergerichtlichen Konfliktlösung.[84]

Zudem kennt das BGG in § 15 das Instrument der Verbandsklage. Die Erhebung eines solchen Feststellungsverfahrens ist aufgrund der Subsidiarität zum individuellen Rechtsschutz in aller Regel nur bei Fällen von allgemeiner Bedeutung gegeben (§ 15 Abs. 2 S. 2 BGG). Dies ist insbesondere bei einer „Vielzahl gleichgelagerter Fälle" (§ 15 Abs. 2 S. 3 BGG) wie der Verletzung einer bundesrechtlichen Vorschrift zur Barrierefreiheit (Zugänglichkeit und Nutzbarkeit von Webseiten) anzunehmen.[85] Die Potenziale eines solchen Verbandsklageverfahrens bleiben in der Praxis allerdings weitgehend ungenutzt.[86] Die Barrierefreiheitsanforderungen des BGG be-

81 Siehe Erwägungsgrund 39 der RL (EU) 2016/2102; *Carstens*, in: Deinert u.a., SWK Behindertenrecht, 2022, Barrierefreie Informationstechnik, Rn. 23.

82 BT-Drs. 20/4440, S. 155.

83 *Carstens*, in: Deinert u.a., SWK Behindertenrecht, 2022, Barrierefreie Informationstechnik, Rn. 29; BT-Drs. 20/4440, S. 163 ff.

84 *Schaumberg*, in: Deinert u.a., SWK Behindertenrecht, 2022, Schlichtungsstelle, Rn. 1 ff.

85 BT-Drs. 20/4440, S. 156, 158; BT-Drs. 18/7824, S. 43; *Hlava*/Trienekens, in: Kahle u.a., Digitale Teilhabe und personenzentrierte Technologien im Kontext von Menschen mit Behinderungen, 2025, S. 56; ‚*Hlava*, Barrierefreie Gesundheitsversorgung, 2018, S. 400 f.

86 BT-Drs. 20/4440, S. 162.

schränken sich in erster Linie auf öffentliche Stellen. Privatwirtschaftliche Online-Angebote, bleiben dadurch unreguliert, da es ohne gesetzliche Verpflichtung am Anreiz mangelt, barrierefreie Lösungen umzusetzen. Die digitale Exklusion von Menschen mit Behinderungen verhindert eine gleichberechtigte gesellschaftliche Teilhabe. Vorgaben zur Gewährleistung von Barrierefreiheit durch Private ergeben sich zwar aus Art 4 lit. a UN-BRK iVm Art. 9 Abs. 2 lit. b, Art. 4 lit. e und Art. 21 lit. c UN-BRK.[87] Da aber das BGG den Forderungen der UN-BRK nicht umfänglich nachkommt, ist eine Ausweitung des BGG auf private Akteure geboten. Dieser faktischen Ungleichbehandlung wurde versucht durch die Vorgaben der RL (EU) 2019/882 und dem Barrierefreiheitsstärkungsgesetz zu begegnen.

4.3.2 Barrierefreiheitsanforderungen für Produkte und Dienstleistungen nach dem Barrierefreiheitsstärkungsgesetz

Das Barrierefreiheitsstärkungsgesetz (BFSG)[88] verpflichtet neben den öffentlichen Stellen auch ausgewählte Wirtschaftsakteure der Produktangebotskette (z. B. Hersteller oder Dienstleister) zur Herstellung von Barrierefreiheit. Durch das BFSG werden die Barrierefreiheitsanforderungen der Richtlinie (EU) 2019/882 (European Accessibility Act (EAA))[89] in nationales Recht umgesetzt. Eine Konkretisierung der Anforderungen wurde gem. § 3 BFSG durch die Verordnung zum Barrierefreiheitsstärkungsgesetz (BFSGV)[90] vorgenommen. Adressiert werden ausgewählte Produkte (§ 1 Abs. 2 BFSG), z. B. Computer, Mobiltelefone, Tablets, Geldautomaten, Spielekonsolen, E-Book-Reader, sowie Dienstleistungen (§ 1 Abs. 3 Nr. 1 bis 5 BFSG), z. B. Video-Konferenz-Software, Messenger-Dienste, E-Ticket-Systeme oder Online-Shops.[91] Das Gesetz gilt ausschließlich für Produkte und Dienstleistungen, die nach dem 28.6.2025 in den Verkehr gebracht werden. Produkte sind in § 1 Abs. 2 BFSG abschließend aufgelistet und setzen einen

87 So auch: *Ritz*, in: Kossens u.a., SGB IX mit BGG, 2023, § 12a BGG, Rn. 21.

88 Gesetz zur Umsetzung der Richtlinie (EU) 2019/882 des Europäischen Parlaments und des Rates über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (Barrierefreiheitsstärkungsgesetz – BFSG) v. 16.7.2021, BGBl. I, 2970.

89 Richtlinie (EU) 2019/882 v. 17.4.2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen, ABl. (EU) L 151/70.

90 Verordnung über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen nach dem Barrierefreiheitsstärkungsgesetz (Verordnung zum Barrierefreiheitsstärkungsgesetz – BFSGV) v. 15.6.2022, BGBl. I, 928.

91 *Franke*, Digitale Barrierefreiheit von Produkten und Dienstleistungen, ZfPC 2024, 21.

Fertigungsprozess voraus. KI-Chatbots und AI-Companions fallen also beispielsweise nicht darunter. Auch der Begriff der Dienstleistung ist eng zu verstehen und setzt gemäß Art. 4 Nr. 1 RL 2006/123/EG[92], Art. 50 EGV[93] in der Regel ein Entgelt voraus (meist Vertragsabschlüsse).[94] Fraglich ist hierbei, inwiefern Geschäftsmodelle darunter subsumiert werden können, die darauf beruhen, dass die Verbrauchenden mit ihren personenbezogenen Daten statt mit Geld bezahlen. Ob es sich beim Bezahlen mit Daten um eine „wirtschaftliche Gegenleistung für die betreffende Leistung" handelt, die eine Entgeltersatzfunktion erfüllt, ist nicht abschließend geklärt.[95] Es sollte aber davon ausgegangen werden, dass der Gesetzgeber diese Fälle nicht aus dem Anwendungsbereich des BFSG exkludieren wollte. Für Webseiten wurde der Anwendungsbereich konkreter geregelt. Diese fallen nur in den Anwendungsbereich, wenn sie entweder „Element eines Personenbeförderungsdienstes" sind (§ 1 Abs. 3 Nr. 2 BFSG) oder mindestens eine „Dienstleistung im elektronischen Geschäftsverkehr" beinhalten (§ 1 Abs. 3 Nr. 5 BFSG).[96] Unter Bezugnahme des Anwendungsszenarios ist noch fraglich, ob eine Anwendung wie die eines AI-Companions als Telekommunikationsdienst i.S.d § 1 Abs. 3 Nr. 1 BFSG unter die Vorgaben des BFSG fällt. Da es sich bei einem AI-Companions weder um einen gegen Entgelt über elektronische Kommunikationsnetze erbrachten Dienst gem. § 2 Nr. 7 BFSG iVm Art. 2 Nr. 4 RL (EU) 2018/1972 handelt, noch um einen interpersonelle Kommunikationsdienst, wie z.B. Skype,[97] kann auch dies verneint werden. In Bezug auf die Frage der Ausgestaltung einer informierten Einwilligung kann jedoch insbesondere die BFSG-VO zur allgemeinen Konkretisierung der Barrierefreiheitsanforderungen an eine Informationspräsentation herangezogen werden. Hervorzuheben ist dabei der Verweis der Informationsdarstellung über das Zwei-Sinne-Prinzip, wonach die Bereitstellung über mehr als einen sensorischen Kanal gewährleistet

92 Richtlinie 2006/123/EG v. 12.12.2006 über Dienstleistungen im Binnenmarkt (ABl. L 376 S. 36).

93 Vertrag zur Gründung der Europäischen Gemeinschaft idF bis 30. November 2009.

94 *Tabbara*, Barrierefreiheit für elektronische Produkte und Dienstleistungen, NZS 2021, 497 (498); *Kapoor/Klindt*, Das Barrierefreiheitsstärkungsgesetz, NJW 2024, 3545, Rn. 3; *Franke*, Digitale Barrierefreiheit von Produkten und Dienstleistungen, ZfPC 2024, 21.

95 Vgl. *Fries*, BeckOGK, 2025, § 327 BGB, Rn. 21; *Ehlen/Möllnitz-Dimick*, Datenfinanzierte digitale Produkte, CR 2023, 455 (456ff.); *Randelzhofer/Forsthoff,* Das Recht der Europäischen Union, 2009, Art. 50 EGV, Rn. 43.

96 Vgl. *Kapoor/Klindt*, Das Barrierefreiheitsstärkungsgesetz, NJW 2024, 3545 (3545ff.).

97 BT-Drs. 19/28653, S. 64.

werden soll (§ 4 Abs. 1 BFSGV). Dies gilt in erster Linie für Alternativen zu visuellen, auditiven, gesprochenen und taktilen Elementen, sollte aber auch im Bezug zur Gewährleistung der Verständlichkeit im Allgemeinen nicht unterschätzt werden.

5. Zwischenfazit zur barrierefreien informierten Einwilligung

Während der Grundrechtsschutz für Kinder im Rahmen der Einwilligung in Art. 8 DSGVO ausdrücklich durch den Gesetzgeber adressiert wurde, bleibt die besondere Schutzbedürftigkeit anderer vulnerabler Gruppen, insbesondere von Menschen mit Behinderung, weitgehend unberücksichtigt. Dabei ergibt sich aus Art. 26 GRCh sowie Art. 22 UN-Behindertenrechtskonvention (UN-BRK) eine Pflicht zum Schutz der digitalen Privatheit auch für diese Personengruppe. Ergänzend verpflichten Art. 4 lit. g i. V. m. Art. 9 UN-BRK zur Gewährleistung eines gleichberechtigten Zugangs zu Informations- und Kommunikationstechnologien. Dies umfasst auch die barrierefreie Gestaltung von informierten Einwilligungsprozessen, etwa durch die Bereitstellung von Informationen in zugänglichen Formaten wie leichter Sprache oder auditiver Sprachausgabe. Die Regelungen zur Barrierefreiheit im deutschen Recht (BGG, BFSG) beschränken sich lediglich auf die barrierefreie Ausgestaltung von Webseiten. Es findet sich kein Bezug zur Einwilligung oder ihrer barrierefreien Gestaltung. Dies führt zu einer mangelhaften praktischen Ausgestaltung in Bezug auf die Erteilung von informierten Einwilligungen durch Menschen mit Behinderung (z. B. mit kognitiven Beeinträchtigungen). Neben einer Diskriminierung im Sinne des Art. 5 Abs. 2 UN-BRK kann darin auch eine Benachteiligung gem. Art. 3 Abs. 3 S. 2 GG sowie Art. 21 GRCh gesehen werden. Darüber hinaus sollte eine kritische Reflexion darüber erfolgen, inwiefern die individuellen Voraussetzungen der Einwilligenden, wie sie in Art. 8 DSGVO in Bezug auf die Einwilligungsfähigkeit und Einsichtsfähigkeit von Kindern beschrieben sind, auch für den „Durchschnittsnutzer“ angepasst werden sollten. Angesichts zunehmender digitaler Vulnerabilität – etwa durch überfordernde Informationsdichte, manipulative Interface-Gestaltung oder unzureichende Privacy Literacy – erscheint es geboten, die Wirksamkeitsvoraussetzung der Einwilligung ‚in informierter Weise‘ nicht schematisch am Modell des durchschnittlich informierten Nutzenden auszurichten, sondern stärker an die individuellen Bedürfnisse der Betroffenen anzupassen. Gerade beim

Einsatz von Dialogsystemen wie AI-Companions besteht andernfalls ein erhöhtes Risiko, dass Nutzende personenbezogene Daten unbedacht offenlegen, ohne sich der Tragweite ihrer Einwilligung vollumfänglich bewusst zu sein. Ausgehend von der Grundannahme, dass Vulnerabilität ein Teil des menschlichen Daseins ist, lässt sich aus den Grundrechten aus Art. 7 und 8 GRCh und Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ein über die etablierten Schutzkonzepte hinausgehender Anspruch auf eine individuelle, situative und kontextbezogene Anpassung der Informations- und Einwilligungsvoraussetzungen konzipieren. Dieser sollte auch auf der Ebene der zu treffenden Maßnahmen nach Art. 25 DSGVO im Rahmen von „Privacy by Design" ansetzen.[98]

6. Hoffnungsträger Einwilligungsverwaltungsverordnung?

Ein Ansatzpunkt, zumindest Einwilligungsbanner auf Webseiten zu reduzieren, zu vereinfachen und Nutzende damit bei der Abgabe und Verwaltung von Einwilligungen zu unterstützen, ist die Einwilligungsverwaltungsverordnung (EinwV)[99]. Dienste zur Einwilligungsverwaltung gemäß § 26 TDDDG[100] sollen Nutzende dabei entlasten, täglich eine Vielzahl von Einzelentscheidungen darüber treffen zu müssen, ob Informationen im Endgerät gespeichert werden sollen oder Zugriff auf diese erfolgen darf (§ 25 Abs. 1 TDDDG).

Allerdings ist der Anwendungsbereich einigermaßen beschränkt, da es nur um Einwilligungen nach § 25 TDDDG zur Speicherung von oder den Zugriff auf Informationen in Endeinrichtungen des Nutzenden geht (§ 2 Abs. 1 Nr. 4 EinwV), nicht hingegen um sonstige Einwilligungen nach der DSGVO. Außerdem ist die Nutzung eines nach der EinwV anerkannten Dienstes für Webseitenbetreiber freiwillig (§ 18 EinwV). Es fehlen daher

98 *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (9 ff.).

99 Verordnung über Dienste zur Einwilligungsverwaltung nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (Einwilligungsverwaltungsverordnung – EinwV) v. 6.2.2025, BGBl. I Nr. 32. Zum Referentenentwurf bereits *Nebel*, Alles abwählen: Mit der Einwilligungsverwaltungs-Verordnung gegen den Cookie-Banner-Dschungel, ZD-Aktuell 2022, 01321.

100 Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei digitalen Diensten (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz – TDDDG) v. 23.6.2021, BGBl. I, 1982, zuletzt geändert durch Art. 44 des Gesetzes zur weiteren Digitalisierung der Justiz v. 12.7.2024, BGBl. I Nr. 234.

Anreize sowohl für Entwickler, entsprechende Systeme zur Marktreife zu bringen, als auch für Webseitenbetreiber, da der Nichteinsatz ohne Konsequenz bleibt. Daher ist es äußerst fraglich, ob das Ziel der Verordnung erreicht werden kann.[101]

Gerade für vulnerable Gruppen könnte ein entsprechendes Einwilligungsverwaltungssystem jedoch eine immense Entlastung im Alltag bedeuten, da nicht mehr eine Vielzahl von informierten Einzelentscheidungen getroffenen werden müssten, sobald eine Webseite aufgerufen, Cookies gespeichert oder Informationen abgerufen werden sollen. Individuelle Präferenzen könnten einmalig, gegebenenfalls mit Unterstützung durch betreuende Personen, gesetzt werden und anschließend Berücksichtigung finden. Ohne das Mitwirken einer betreuenden Person müsste das System Nutzerdaten, wie z.B. das Alter oder den Bildungsstand, erfassen, um benutzerspezifische Informationen über seine Funktionsweise bereit stellen zu können. Dies würde jedoch die Informationsasymmetrie zwischen Anbieter und Nutzenden vergrößern, da der Gewinn an Verständlichkeit und Selbstbestimmung mit einem gleichzeitigen Verlust durch die Erhebung personenbezogener Daten einhergeht.[102]

Es bleibt festzuhalten, dass die EinwV einen guten Ansatz bereithält, um vulnerablen Nutzenden das Management der Einwilligungen zu erleichtern. Leider ist sie im Anwendungsbereich zu eingeschränkt, um einen nennenswerten Unterschied zu machen.

7. Selbstbestimmung vulnerabler Nutzender im europäischen Datenrecht: Rechtspflichten und Verbesserungsbedarf am Beispiel von AI-Companions

Die Wirksamkeit der Einwilligung vulnerabler Nutzender sicherzustellen, ist – wie festgestellt – keine triviale Aufgabe. Um die Selbstbestimmung der betroffenen Personen zu stärken und damit auch die Potenziale, die der wirksamen Einwilligung hierbei zukommen, zu unterstützen, wurden eine Reihe von Compliance-Pflichten im neuen europäischen Datenrecht geschaffen. Dieses hat in jüngster Zeit, insbesondere durch die KI-VO, den Digital Services Act und den Digital Markets Act, erhebliche Veränderungen erfahren und ein ausdifferenziertes Umfeld hervorgebracht. Der

101 *Landesbeauftragte für Datenschutz Niedersachsen*, Pressemitteilung 20/2024 vom 27.12.2024. So auch bereits *DSK*, Stellungnahme zum Referentenentwurf vom 11.7.2023.

102 *Geminn*, Deus ex machina?, 2023, S. 175.

folgende Abschnitt stellt an ausgewählten Regelungen dar, ob und wie das europäische Datenrecht die Selbstbestimmung vulnerabler Nutzender durch zusätzliche Verpflichtungen am Beispiel von Anbietern von AI-Companions gewährleisten kann und wo Verbesserungsbedarf besteht.

7.1 Verordnung für Künstliche Intelligenz

Am 21.5.2024 wurde die Verordnung für Künstliche Intelligenz (KI-VO) verabschiedet.[103] Es handelt sich um die weltweit erste umfassende Regelung für den Einsatz von Künstlicher Intelligenz und gilt damit als Vorreiter für eine risikoorientierte Regulierung des Einsatzes Künstlicher Intelligenz in der Gesellschaft. Die Verordnung soll das gesamtgesellschaftliche Vertrauen in Künstliche Intelligenz stärken.[104] Die KI-VO regelt technikspezifisch Künstliche Intelligenz in Abhängigkeit von ihrem Risiko und unterteilt dabei in vier Gruppen: „verbotene Praktiken im KI-Bereich", „Hochrisiko-KI-Systeme", KI-Systeme mit begrenztem Risiko und KI-Systeme mit geringem oder keinem Risiko. Nicht akzeptable Risiken sind gemäß Art. 5 KI-VO verboten. Die Hauptlast der Regulierung liegt in der KI-VO bei Hochrisiko-KI-Systemen gemäß Art. 6 KI-VO. Wird ein KI-System als solches eingestuft, obliegen den Anbietern und Betreibern umfangreiche Sorgfalts-, Kontroll- und Informationspflichten. Für KI-Systeme mit begrenztem Risiko gelten demgegenüber abgeschwächte Vorgaben. KI-Systeme mit geringem oder keinem Risiko bleiben unreguliert.[105]

Der Regelungsgehalt der KI-VO fokussiert sich im Wesentlichen auf Risikobewertungen und Maßnahmen, um entsprechende Risiken einzudäm-

103 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L, 2024/1689, 12.7.2024.

104 *Chibanguza/Steege*, Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, NJW 2024, 1769.

105 Übersichten zur KI-VO z. B. *Geminn*, Die Regulierung künstlicher Intelligenz, ZD 2021, 354; *Chibanguza/Steege*, Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, NJW 2024, 1769; *Horstmann*, KI-VO und Datenschutz: Überblick und ausgewählte Fragen, ZD-Aktuell 2024, 01580.

men und ist damit eher produktsicherheitsrechtlich motiviert.[106] Entsprechend regelt Art. 2 Abs. 7 S. 1 KI-VO, dass Unionsvorschriften zum Schutz personenbezogener Daten, Privatsphäre und Vertraulichkeit der Kommunikation weitergelten und die DS-GVO gemäß Satz 2 unberührt bleibt.[107] Anwendbar ist die KI-VO gemäß Art. 2 Abs. 1 KI-VO für alle Anbieter, Betreiber, Einführer, Händler, Hersteller von KI-Systemen. Anbieter, die Chatbots oder AI Companions in der Union anbieten, sind in der Regel Anbieter und/oder Betreiber von KI-Systemen.

Verboten sind Chatbots oder AI-Companions nach der KI-VO, wenn sie unter die Anwendungsfälle des Art. 5 KI-VO fallen. Relevant sind insbesondere Abs. 1 lit. a bis c:[108] Gemäß Art. 5 Abs. 1 lit. a KI-VO sind Techniken der unterschwelligen Beeinflussung (Dark Patterns) verboten, die auf eine Verhaltensänderung abzielen, indem die Fähigkeit der freien Entscheidungsfindung beeinträchtigt wird und wenn dies einer Person[109] erheblichen Schaden zufügt oder zufügen würde. Schaden ist als Begriff des Unionsrechts autonom auszulegen.[110] Erwägungsgrund 29 S. 2 KI-VO spricht von "große[n] Schäden, insbesondere erhebliche nachteilige Auswirkungen auf die physische oder psychische Gesundheit oder finanzielle Interessen". Umfasst sind also sowohl materielle als auch immaterielle Schäden. Es ist von einem eher engen Schadensbegriff auszugehen,[111] der sowohl „groß" als auch „erheblich" sein muss und kausal mit der Beeinflussung zusammenhängt. Wann ein Schaden erheblich ist, dazu äußert sich die Verordnung nicht. Schutzgut ist weniger die Selbstbestimmung der Nutzenden als ein physischer, psychischer oder finanzieller Schaden.[112] Im Hinblick auf

106 *Hacker/Berz,* Der AI Act der Europäischen Union – Überblick, Kritik und Ausblick, ZRP 2023, 226; *Horstmann*, KI-VO und Datenschutz: Überblick und ausgewählte Fragen, ZD-Aktuell 2024, 01580.

107 Vgl. auch Erwägungsgrund 10 KI-VO. Ausführlich zum Verhältnis der KI-VO zur DS-GVO *Nebel*, in: Geminn/Johannes (Hrsg.), Europäisches Datenrecht, 2025 i.E.

108 *Böhning/Schindler*, Verbotene Praktiken im KI-Bereich – Wann ist was verboten?, ZD-Aktuell 2024, 01793.

109 S. zur Frage, welche Person im Einzelfall gemeint sein könnte, *Böhning/Schindler*, Verbotene Praktiken im KI-Bereich – Wann ist was verboten?, ZD-Aktuell 2024, 01793.

110 Vgl. zum Schadensbegriff in der DSGVO EuGH, Urteil vom 4.5.2023, Rs. C-300/21, ECLI:EU:C:2023:370.

111 *Martini/Kramme/Kamke,* KI-VO, DMA und DA als Missing Links im Kampf gegen dunkle Designmuster?, MMR 2023, 399 (400) zu KI-VO-E.

112 So bereits *Martini/Kramme/Kamke,* KI-VO, DMA und DA als Missing Links im Kampf gegen dunkle Designmuster?, MMR 2023, 399 (400) zu Art. 5 KI-VO-E.

Verbraucherschutz im Allgemeinen und Schutz vulnerabler Gruppen im Besonderen scheint dies etwas zu kurz gedacht, wobei zumindest der Schaden – anders als noch im Verordnungsentwurf[113] – nunmehr finanzielle Aspekte mit umfasst. Das ist zu begrüßen. Die Regelung lässt trotzdem viele Fragen offen und ist in seiner praktischen Wirkweise zu Lasten von Dark Pattern deutlich mehr eingeschränkt, als auf den ersten Blick vermuten lässt. Fraglich ist auch, ob die Vorschrift einen individuellen Anspruch auf Schadenersatz verleiht; dann wäre die Person aber hinsichtlich des Schadens wahrscheinlich beweisbelastet. AI-Companions werden jedenfalls in aller Regel nicht im Ganzen unter das Verbot fallen – bestimmte Praktiken des KI-Systems aber möglicherweise schon.

Verboten ist gemäß Art. 5 Abs. 1 lit. b KI-VO außerdem ein KI-System, das eine Vulnerabilität oder Schutzbedürftigkeit einer Person aufgrund ihres Alters, einer Behinderung oder ihrer sozialen oder wirtschaftlichen Situation ausnutzt mit dem Ziel einer Verhaltensbeeinflussung und dieser Person dadurch ein erheblicher Schaden droht oder zugefügt wird. Bezüglich des Schadens gilt das eben Gesagte, so dass nicht jedes KI-System, das eine Vulnerabilität ausnutzt, unter lit. b fallen wird.

Art. 5 Abs. 1 lit. c KI-VO statuiert ein Verbot der Schlechterstellung oder Benachteiligung durch soziale Bewertung aufgrund von Social Scoring, aber nur bei Zweckentfremdung der Daten oder Unverhältnismäßigkeit. Der Unionsgesetzgeber eruiert nicht näher, was Unverhältnismäßigkeit umfasst und wie zwischen gerechtfertigter oder verhältnismäßiger und ungerechtfertigter oder unverhältnismäßiger Schlechterstellung oder Benachteiligung unterschieden werden soll.[114] Bestimmte Einsatzfelder von Social Scoring sieht der Unionsgesetzgeber jedenfalls als durchaus akzeptabel an.[115]

In der Regel werden AI-Companions nicht unter das Verbot in Art. 5 KI-VO fallen, da dessen Voraussetzungen sehr spezifisch und eng sind und insbesondere der kausale, große und erhebliche Schaden schwer nachweisbar sein wird. Art. 5 Abs. 1 lit. a bis c KI-VO gibt aber rote Linien insbesondere hinsichtlich der Verhaltensbeeinflussung und freien Entscheidungsfindung vor, die Diensteanbieter beachten müssen, um nicht unter das Verbot von Art. 5 KI-VO zu fallen.

---

113 Vgl. KI-VO-E, COM(2021) 206 final, Punkt 5.2.2. im Vergleich zu Erwägungsgrund 29 S. 2 KI-VO (VO 2024/1689).

114 *Böhning/Schindler*, Verbotene Praktiken im KI-Bereich – Wann ist was verboten?, ZD-Aktuell 2024, 01793.

115 Kritisch hierzu *Becker/Feuerstack,* Die EU-KI-Verordnung, KIR 2024, 62.

Als Hochrisiko-KI wären AI-Companions dann einzustufen, wenn sie unter die Kategorisierung des Art. 6 KI-VO fallen. Da solche Dialogsysteme weder in den in Art. 6 Abs. 1 iVm Anhang I und II KI-VO aufgeführten Produktbereichen genannt sind noch bisher als Sicherheitsbauteil gelten, bleibt nur Art. 6 Abs. 2 iVm Anhang III KI-VO. Anhang III nennt acht spezifische Einsatzbereiche für den Hochrisiko-KI-Bereich. Das sind etwa Biometrie, Kritische Infrastruktur, der Bildungsbereich, Beschäftigung und Personalmanagement oder Strafverfolgung. Keiner der genannten Einsatzbereiche tangiert Dialogsysteme, die im privaten Umfeld aus reinen Privatinteressen heraus genutzt werden, auch nicht, wenn sie intime Kommunikation ermöglichen.

Daher sind die hier betrachteten AI-Companions sonstige KI-Systeme, die lediglich den leicht umzusetzenden Transparenzpflichten aus Art. 50 Abs. 1 KI-VO unterfallen.[116] Die AI-Companions sind also als KI-System zu kennzeichnen, damit Nutzende wissen, dass sie mit einem KI-System kommunizieren.

7.2 Digital Services Act

Der Digital Services Act (DSA)[117] fördert durch diverse Maßnahmen die Selbstbestimmung in digitalen Infrastrukturen. Gegenstand des DSA sind Vermittlungsdienste. Je nach Qualifizierung des jeweiligen Dienstes legt der DSA diesen Diensten Haftungsbefreiungen und Sorgfaltspflichten für ein transparentes und sicheres Online-Umfeld auf. Die Anbieterpflichten des DSA bleiben auch durch die KI-VO unberührt.[118]

Um unter den DSA zu fallen, müssten AI-Companions und sonstige Chatbots Vermittlungsdienste im Sinne des Art. 3 lit. g DSA sein. Inwiefern Dienste, die rein auf einem KI-System basieren, unter den DSA zu subsumieren sind, bedarf einer genaueren Untersuchung. Voraussetzung aller Vermittlungsdienste im Sinne des Art. 3 lit. g DSA ist, dass es sich um

116 Vgl. *Chibanguza/Steege*, Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, NJW 2024, 1769 (1774).

117 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19.10.2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG.

118 Art. 2 Abs. 5 KI-VO.

Dienste der Informationsgesellschaft handelt[119] und dass sie vom Nutzenden bereit gestellte Daten als „reine Durchleitung", „Caching-„ oder „Hosting-Dienst" verarbeiten. Bei generativen KI-Systemen wird nur ein sehr kleiner Teil der Daten vom Nutzenden bereitgestellt, da hauptsächlich aus den Inputs der Nutzenden neue Daten abgeleitet werden, die die Kernanwendung oder den Kernnutzen des KI-Systems ausmachen. Diese Daten sind jedoch nicht vom Nutzenden bereitgestellt, sondern vom System inferiert. Nur in dem begrenzten Umfang der tatsächlichen Bereitstellung ist der Diensteanbieter als Anbieter eines Vermittlungsdienstes im Sinne des DSA anzusehen; da die vom Nutzer bereitgestellten Informationen in dessen Auftrag gespeichert werden, ist der Dienst als Hosting-Dienst einzustufen. Diejenigen Informationen, die aus den bereit gestellten Daten der Nutzenden durch die generative KI abgeleitet werden, z. B. Nachrichten und Aufforderungen des AI-Companions an den Nutzenden, sind jedoch nicht vom Nutzenden bereitgestellt, sondern von der KI erzeugt, und fallen damit nicht unter den DSA.[120]

Die generative KI könnte als Anwendung je nach konkreter Ausgestaltung als Empfehlungssystem im Sinne des Art. 3 lit. s DSA oder als Verbot von Dark Patterns im Sinne des Art. 25 DSA eingestuft werden.[121]

Empfehlungssysteme sind gemäß Art. 3 lit. s DSA „vollständig oder teilweise automatisierte Systeme definiert, die von einer Online-Plattform verwendet werden, um auf ihrer Online-Schnittstelle den Nutzern bestimmte Informationen vorzuschlagen oder diese Informationen zu priorisieren". Bei der Verwendung von solchen Empfehlungssystemen sind Anbieter von Online-Plattformen verpflichtet, bestimmte Transparenzanforderungen im Sinne des Art. 27 Abs. 1 DSA umzusetzen.

Bei dem Verbot von Dark Patterns im Sinne des Art. 25 DSA handelt es sich nach Erwägungsgrund 67 DSA um „Praktiken, mit denen darauf abgezielt oder tatsächlich erreicht wird, dass die Fähigkeit der Nutzenden, eine autonome und informierte Entscheidung oder Wahl zu treffen, erheblich verzerrt oder beeinträchtigt wird". Das Verbot in Art. 25 DSA bezieht sich auf sogenannte Online-Schnittstellen. Ob es sich bei einem AI-Com-

119 Art. 3 lit. a DSA iVm Art. 1 Abs. 1 lit. b RL (EU) 2015/1535. Diese Voraussetzungen liegen bei AI-Companions vor.

120 *Berz/Engel/Hacker*, Generative KI, Datenschutz, Hassrede und Desinformation – Zur Regulierung von KI-Meinungen, ZUM 2023, 586 (590 f.) zu generativer KI im Rahmen der Meinungsbildung.

121 *Wehde*, Regulierung von Large Language Models in DSA und AIA-E, MMR-Aktuell 2023, 455171.

panion, also einem auf einem KI-System basierenden Chatbot, um eine Online-Schnittstelle im Sinne des Art. 3 lit. m DSA handelt, ist jedoch nicht abschließend geklärt. Bei Online-Schnittstellen handelt es sich um „Software [...] sowie Anwendungen, einschließlich Mobil-Apps". Gemeint ist damit wohl das Software-Interface[122], also die Gestaltung der Benutzeroberfläche;[123] aber auch nicht ohne weiteres wahrnehmbare Gestaltungselemente einer Software können darunterfallen.[124] Auch ein KI-System könnte ein solches Gestaltungselement sein und fällt zudem unter den Begriff Software. Die Rechtsfolge bezogen auf AI-Companions wäre jedenfalls, dass die Nutzenden nicht getäuscht, manipuliert oder in ihrer freien Entscheidung beeinträchtigt werden dürfen. Nicht die Interaktion mit dem AI-Companion an sich wäre verboten, da die Nutzenden wissen und sich mehr noch freiwillig für die Nutzung eines AI-Companions entschieden haben. Möglicherweise könnten aber bestimmte Praktiken des KI-Systems unter das Verbot fallen, wenn sie eine entsprechende Wirkung auf den Nutzenden haben. Denkbar ist dies etwa in Fällen, dass das KI-System den Nutzenden dazu verleitet, Bilder von sich herauszugeben, die beispielsweise für die Generierung von Nacktbildern genutzt werden könnten,[125] oder Nutzende zum Suizid verleitet.[126] Diese Regelung ergänzt gut die verbotenen Praktiken der KI-VO um solche Fälle abzufangen, die mangels Schaden nicht in den engen Anwendungsbereich des Art. 5 KI-VO fallen, deren Verhinderung aber durchaus im Interesse des Unionsgesetzgebers und der Gesellschaft sein sollte.

Im Ergebnis bleibt festzuhalten, dass Anbieter von AI-Companions als Vermittlungsdienste nur in begrenztem Umfang unter den DSA fallen, aber zumindest für diejenigen Informationen, die die Nutzenden aktiv bereitstellen, gemäß Art. 11 ff. DSA sorgfaltsverpflichtet sind. Relevante Verpflichtungen, denen Diensteanbieter von AI-Companions nachkommen müssen und die insbesondere den Aspekt der Sicherstellung der Selbstbestimmung unterstützen können, sind die allgemeinen Bestimmungen der Art. 11 ff. DSA z. B. zum Einrichten von Kontaktstellen, AGB-Erfordernisse,

122 *Köhler/Holznagel/Müller-Terpitz*, in: Müller-Terpitz/Köhler, 2024, Digital Services Act, Art. 3 DSA, Rn. 114.
123 *Hofmann*, in: Hofmann/Raue, 2024, Digital Services Act, Art. 3 DSA, Rn. 114.
124 *Hofmann*, in: Hofmann/Raue, 2024, Digital Services Act, Art. 3 DSA, Rn. 114.
125 *Mozilla Foundation*, EVA AI Chat Bot und Soulmate, 2024. *Kühl*, Das Nacktbild, das man nie geschossen hat, Zeit Online vom 14. Dezember 2023.
126 Z.B. *Payne*, An AI chatbot pushed a teen to kill himself, a lawsuit against its creator alleges, Associated Press vom 24. Oktober 2024.

Transparenzpflichten, Melde- und Abhilfeverfahren nach Art. 16 DSA. Da AI-Companions mangels der öffentlichen Verbreitung der vom Nutzenden bereitgestellten Daten nicht als Online-Plattform im Sinne des Art. 3 lit. i DSA zu qualifizieren sind, gelten die zusätzlichen Regelungen der Art. 20 ff. DSA nicht für AI-Companions.

Sollte aber eine Online-Plattform im Sinne des DSA einen Chatbot nutzen, gelten zusätzlich die Regelungen zur Errichtung eines internen Beschwerdemanagements nach Art. 20 DSA. Zudem wären Online-Schnittstellen nach den Vorgaben des Art. 25 DSA zu gestalten, beim Platzieren von Werbung ist Art. 26 DSA zu beachten und beim Einsatz von Empfehlungssystemen Art. 27 DSA. Art. 28 DSA macht Vorgaben zum Online-Schutz Minderjähriger. Andere vulnerable Gruppen sind leider im DSA nicht mitgedacht.

Mit dem Fokus auf Vulnerabilität lohnt sich ein Blick auf Art. 34 Abs. 1 lit. d DSA. Art. 33 ff. DSA stellt spezifische zusätzliche Pflichten für sehr große Online-Plattformen und sehr große Online-Suchmaschinen auf. Art. 34 Abs. 1 lit. d DSA sticht hervor, da dieser bei der verpflichtenden Analyse zur systemischen Risikobewertung und Risikominderung „nachteilige Folgen für das körperliche und geistige Wohlbefinden einer Person" berücksichtigt sehen möchte. Dies öffnet den Blick auf andere vulnerable Gruppen als nur Minderjährige und verspricht großes Potenzial um nachteilige Auswirkungen auf vulnerable Gruppen zu eruieren und zu verhindern. Gleiches gilt für die zusätzlichen Transparenzanforderungen für Online-Werbung nach Art. 39 DSA. Dieser verpflichtet Anbieter dazu, öffentlich zugängliche, durchsuchbare Archive zu Werbeanzeigen mit den in Abs. 2 genannten Angaben zu erstellen. Besonders interessant ist im Hinblick auf vulnerable Gruppen Abs. 2 lit. e Demnach sind Angaben dazu zu machen, ob und welchen bestimmten Gruppen von Nutzern die Werbung angezeigt werden sollte. Der Begriff Gruppe ist nicht weiter definiert und damit offen; umfasst sein könnten also auch alle denkbaren vulnerablen Gruppen, die durch die Werbewirtschaft explizit angesprochen werden könnten, neben Minderjährigen etwa Senioren, Menschen mit Behinderungen oder Menschen mit Suchtgefährdungspotenzial. Zweck der Regelung ist es gemäß Erwägungsgrund 95 DSA, „die Aufsicht und die Forschung zu neu entstehenden Risiken im Zusammenhang mit der Online-Verbreitung von Werbung zu unterstützen". Dies spricht jedenfalls dafür, vulnerable Personen mit in Betracht zu ziehen.

Da AI-Companions nicht unter den Begriff der Online-Plattformen, können die Regelungen der Art. 33 ff. DSA nicht zur Anwendung kommen.

Dies erscheint angesichts der Auswirkungen, die AI-Companions auf (vulnerable) Nutzende haben können, als eine eklatante Regelungslücke.

7.3 Digital Markets Act

Der Digital Markets Act (DMA)[127] ist Teil eines Regelungspakets der Europäischen Union. Der DMA soll gleiche Wettbewerbsbedingungen in digitalen Märkten schaffen, indem Anbieter zentraler Plattformdienste stärker reguliert werden. Adressat der Regelungen des DMA sind gemäß Art. 1 Abs. 2 DMA Torwächter (Gatekeeper) im Sinne des Art. 2 Nr. 1 DMA, also Unternehmen, die einen zentralen Plattformdienst bereitstellen und von der Kommission nach Art. 3 DMA als solche benannt wurden. Da der DMA eher wettbewerbspolitisch geprägt ist, liegt der Fokus nicht auf datenschutzrechtlichen Aspekten; er nimmt nicht bestimmte Nutzergruppen in den Blick, sondern fokussiert auf spezifische Maßnahmen, um Infrastrukturen für alle fairer zu machen und Marktmissbrauch zu verhindern.

Allerdings fallen AI-Companions nicht unter die in Art. 2 Nr. 2 DMA abschließend aufgezählten Plattformdienste. Es handelt sich nicht um einen Online-Vermittlungsdienst nach Art. 2 Nr. 5 iVm Art. 2 Nr. 2 VO (EU) 2019/1150[128]. Trotz der Wortgleichheit mit Vermittlungsdiensten des DSA liegt hier eine andere Definition zu Grunde: Online-Vermittlungsdienste gemäß Art. 2 Nr. 2 lit. a bis c VO (EU) 2019/1150 sind Dienste der Informationsgesellschaft, die es gewerblichen Nutzern ermöglichen, Verbrauchern Waren oder Dienstleistungen anzubieten, indem sie eine Transaktion zwischen diesen vermitteln. Dies trifft auf AI-Companions nicht zu, so dass sie keine Online-Vermittlungsdienste im Sinne des DMA sind. Sie sind auch kein Online-Dienst eines sozialen Netzwerks im Sinne des Art. 2 Nr. 7 DMA, da sie keine Kontakte mit anderen Nutzern ermöglichen, sondern nur Interaktion mit einem KI-System. Schließlich gelten sie auch nicht als virtueller Assistent im Sinne des Art. 2 Nr. 12 DMA, da sie keine Aufträge, Aufgaben oder Fragen verarbeiten zu dem Zweck Zugang zu

127 Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14.9.2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte), ABl. vom 12.10.2022, L 265, 1. Kommissionsvorschlag abrufbar unter: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=COM:2020:842:FIN.

128 Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten. ABl. EU vom 11.7.2019, L 186/57.

anderen Diensten zu ermöglichen oder angeschlossene physische Geräte zu steuern. Der DMA findet mithin im Kontext von AI-Companions keine Anwendung.

8. Fazit

Die Gewährleistung der Selbstbestimmung als Folge einer informierten Entscheidung des Individuums in solchen digitalen Infrastrukturen ist keine triviale Aufgabe und lässt sich nicht auf Knopfdruck bewältigen. Die Relevanz ist vor dem Hintergrund des politischen und wirtschaftlichen Einflusses der Datenverarbeitenden auf das demokratisch-rechtsstaatliche Gemeinwesen nicht zu unterschätzen. Gerade in Kontexten, in denen die Vulnerabilität ein entscheidender Faktor ist, muss dem Merkmal der Informiertheit noch mehr Aufmerksamkeit geschenkt werden.

Nach wie vor spielt die datenschutzrechtliche Einwilligung eine entscheidende Rolle zur Förderung und Verwirklichung des Freiheitsrechts auf informationelle Selbstbestimmung, da sie die kollidierenden Freiheiten der von der Datenverarbeitung betroffenen Personen und den Interessen der Verantwortlichen zu vereinen versucht. Dies darf jedoch nicht darüber hinwegtäuschen, dass praktische Probleme in der Umsetzung die Bedeutung der Einwilligung erheblich schmälern. Bestehende Machtdisparitäten, Konditionen oder strukturelle Probleme wie überlange, komplizierte oder unverständliche Einwilligungserklärungen wirken sich zumeist nachteilig für die betroffene Person aus. Hier müssen neue Wege beschritten werden, um dem Bedeutungsverlust der datenschutzrechtlichen Einwilligung entgegenzutreten.

Das europäische Datenrecht hat in den letzten Jahren einen enormen Wandel erfahren – wo zunächst die DSGVO als große Innovation gefeiert werden konnte, um das Datenschutzrecht auf ein neues Niveau zu heben, war bald klar, dass dies im Angesicht der sich rasant entwickelnden Technologien nicht ausreichen wird. Allerdings bringen die neuen Verordnungen KI-VO, DSA und DMA nur sehr eingeschränkten Nutzen für vulnerable Nutzende insbesondere im Anwendungsbereich von AI-Companions. Zwar werden umfangreiche Verpflichtungen für Diensteanbieter statuiert. AI-Companions und Chatbots werden weder in der KI-VO nennenswert reguliert noch fallen sie unter den DMA und auch bezüglich des DSA ist der Anwendungsbereich nur sehr eingeschränkt. Der Sicherstellung der Wirksamkeit der Einwilligung kommt daher nur umso mehr Bedeutung zu.

Literatur

Art.-29-Gruppe, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01,https://www.datenschutzkonferenz-online.de/media/wp/20180411_wp260_rev01.docx.

Becker, Daniel und Feuerstack, Daniel (2024): Die EU-KI-Verordnung. *Künstliche Intelligenz und Recht*, 2/2024, S. 62-69.

Behrendt, Hauke und Loh, Wulf (2022): Informed consent and algorithmic discrimination – is giving away your data the new vulnerable? *Review of Social Economy*, 80(1), S. 58-84. https://doi.org/10.1080/00346764.2022.2027506.

Berz, Amelie, Engel, Andreas und Hacker, Philipp (2023): Generative KI, Datenschutz, Hassrede und Desinformation – Zur Regulierung von KI-Meinungen. *Zeitschrift für Urheber- und Medienrecht*, 8-9/2023, S. 586-594.

Bielefeldt, Heiner (2019): Vulnerabilität als Menschenrechtsthema – Eine Problemskizze. In: Bergemann, Lutz und Frewer, Andreas (Hrsg.): *Autonomie und Vulnerabilität in der Medizin*. Bielefeld: transcript, S. 21-38.

Bieresborn, Dirk und Schafhausen, M. (Hrsg.) (2024): *Münchener Anwaltshandbuch Sozialrecht*. 6. Auflage. München: Beck.

Birkmann, Jörn; Bach, Claudia; Guhl, Silvie; Witting, Maximilian; Welle, Torsten und Schmude, Miron (2010): *State of the Art der Forschung zur Verwundbarkeit Kritischer Infrastrukturen am Beispiel Strom/Stromausfall.* Berlin: Forschungsforum Öffentliche Sicherheit. URL: https://www.sicherheit-forschung.de/forschungsforum/schriftenreihe_neu/sr_v_v/SchriftenreiheSicherheit_02.pdf (besucht am 26.03.2025).

Birnbacher, Dieter (2012): Vulnerabilität und Patientenautonomie – Anmerkungen aus medizinethischer Sicht. *Medizinrecht*, 9/2012, S. 560–565.

Böhning, Fabiola und Schindler, Stephan (2024): Verbotene Praktiken im KI-Bereich – Wann ist was verboten? *ZD-Aktuell* 2024, 01793.

Brough, Aaron und Kelly, Martin (2020): Critical roles of knowledge and motivation in privacy research. *Current opinion in psychology*, (31), S. 11-15. https://doi.org/10.1016/j.copsyc.2019.06.021.

Bundesregierung (2022): Bericht der Bundesregierung über die Wirkungen der Novellierung des Gesetzes zur Weiterentwicklung des Behindertengleichstellungsrechts. URL: https://www.bmas.de/DE/Service/Presse/Meldungen/2022/bericht-weiterentwicklung-behindertengleichstellungsgesetz.html.

Busch, Dörte (2021): Digitale Teilhabe für Menschen mit Behinderungen nach der UN-Behindertenrechtskonvention. *Zeitschrift für europäisches Sozial- und Arbeitsrecht*, 20(11), S. 484-492.

Calliess, Christian und Ruffert, Matthias (Hrsg.) (2022): *EUV/AEUV*. 6. Auflage. München: Beck.

Chibanguza, Kuuya und Steege, Hans (2024): Die KI-Verordnung – Überblick über den neuen Rechtsrahmen. *Neue Juristische Wochenschrift*, 25/2024, S. 1769-1775.

Damm, Reinhard (2013): Vulnerabilität als Rechtskonzept? *Medizinrecht*, 4/2013, S. 201-214. DOI: 10.1007/s00350-013-3389-1

Deinert, Olaf; Welti, Felix; Luik, Steffen und Brockmann, Judith (Hrsg.) (2022): *Stichwort-Kommentar Behindertenrecht*. 3. Auflage. Baden-Baden: Nomos.

Der Bundesbeauftragte der Bundesregierung für Informationstechnik (BfIT) (29.01.25): Digitale Barrierefreiheit. URL: https://www.barrierefreiheit-dienstekonsolidierung.bund.de/Webs/PB/DE/barrierefreie_it/digitale-barrierefreiheit/digitale-barrierefreiheit-node.html (besucht am 15.02.2025).

Deutsches Institut für Menschenrechte (DIfM) (03.10.2023): UN, Ausschuss für die Rechte von Menschen mit Behinderungen, Abschließende Bemerkungen zum kombinierten zweiten und dritten Staatenbericht Deutschlands, CRPD/C/DEU/CO/2-3. URL: https://www.institut-fuer-menschenrechte.de/fileadmin/Redaktion/Publikationen/Weitere_Publikationen/Abschl.Bemerkungen_Deutsche_UEbersetzung_Entwurf_DIMR_barrierefrei.pdf (besucht am: 15.02.2025).

Drygalski, Clarissa von und Welti, Felix: Erkenntnisse aus der UN-BRK zur geschützten Beschäftigung. In: Schachler, Viviane; Schlummer, Werner und Weber, Roland (Hrsg.): *Zukunft der Werkstätten. Perspektiven für und von Menschen mit Behinderung zwischen Teilhabe-Auftrag und Mindestlohn*. Bad Heilbrunn: Verlag Julius Klinkhardt; Lebenshilfe Verlag der Bundesvereinigung 2023, S. 85-100. URN: urn:nbn:de:0111-pedocs-267656, DOI: 10.25656/01:26765; 10.35468/6002-06.

DSK, Stellungnahme zum Referentenentwurf vom 11.7.2023. https://www.datenschutzkonferenz-online.de/media/st/23-07-11_DSK-Stellungnahme_Einwilligungsverwaltung_TTDSG.pdf.

EDSA (2020): Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, angenommen am 4. Mai 2020. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf.

Ehlen, Theresa und Möllnitz-Dimick, Christina (2023): Datenfinanzierte digitale Produkte: Herausforderungen des „Zahlens" mit Daten nach dem neuen Verbraucherschutzregime in der Praxis — Ein – nicht abschließender – Überblick über offene Fragen und Risiken und wie mit ihnen in der Beratung umgegangen werden kann. *Computer und Recht*, 7/2023, S. 455-461. https://doi.org/10.9785/cr-2023-390716.

Ehmann, Eugen und Selmayr, Martin (Hrsg.) (2024): DSGVO. 3. Auflage. München: Beck.

Fineman, Martha (2008): The Vulnerable Subject: Anchoring Equality in the Human Condition. *Yale Journal of Law & Feminism*, 20(1), S. 1-23. https://ssrn.com/abstract=1131407.

Fineman, Martha (2017): Vulnerability and Inevitable Inequality. *Oslo Law Review*, 4(3), S. 133-149. https://doi.org/10.18261/issn.2387-3299-2017-03-02.

Fineman, Martha (2019): Vulnerability and Social Justice. 53 *Valparaiso University Law Review*, S. 1-34. https://ssrn.com/abstract=3352825.

Franke, Lucia (2024): Digitale Barrierefreiheit von Produkten und Dienstleistungen. *Zeitschrift für Product Compliance*, 1/2024, S. 21-27.

Franzen, Martin; Gallner, Inken und Oetker, Hartmut (Hrsg.) (2024): *Kommentar zum europäischen Arbeitsrecht*. 5. Auflage. München: Beck.

Friedewald, Michael; Kreutzer, Michael und Hansen, Marit (Hrsg.): Selbstbestimmung, Privatheit und Datenschutz. Wiesbaden: Springer Nature.

Geminn, Christian L. (2021): Die Regulierung Künstlicher Intelligenz, Anmerkungen zum Entwurf eines Artificial Intelligence Act. *Zeitschrift für Datenschutz*, 7/2021, S. 354-359.

Geminn, Christian L. (2023): *Deus ex machina? Grundrechte und Digitalisierung*. Tübingen: Mohr Siebeck.

Geminn, Christian L.; Francis, Leon und Herder Karl-Raban (2021): Die Informationspräsentation im Datenschutzrecht. *ZD-Aktuell,* 05335.

Gluck, Joshua; Schaub, Florian; Friedman, Amy; Habib, Hana; Sadeh, Norman; Cranor, Lorrie-Faith und Agarwal, Yuvraj (2016): How Short is Too Short? Implications of Length and Framing on the Effectiveness of Privacy Notices. *Proceedings of theTwelfth Symposium on Usable Privacy and Security (SOUPS 2016).* URL: https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-gluck.pdf.

Gola, Peter und Heckmann, Dirk (Hrsg.) (2022): *DSGVO/BDSG*. 3. Auflage. München: Beck.

Grabitz, Eberhard; Hilf, Meinhard und Nettesheim, Martin (Hrsg.) (2009): *Das Recht der Europäischen Union*. 40. Auflage, München: Beck.

Gsell, Beate; Krüger, Wolfgang; Lorenz, Stephan und Reymann, Christoph (Hrsg.) (2025): *beck-online.Großkommentar (BeckOGK) BGB*. München: Beck.

Hacker, Philipp und Berz, Amelie (2023): Der AI Act der Europäischen Union – Überblick, Kritik und Ausblick. *Zeitschrift für Rechtspolitik*, 8/2023, S. 226-229.

Hagendorf, Thilo (2018): Übersehene Probleme des Konzepts der Privacy Literacy. In: Roßnagel, Alexander; Friedewald, Michael und Hansen, Marit (Hrsg.): *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung.* Wiesbaden: Springer, S. 99-120.

Han, S. Duke; Boyle, Patricia A; James, Bryan D; Yu, Lei und Bennett, David A (2015): Mild cognitive impairment is associated with poorer decision-making in community-based older persons. *Journal of the American Geriatrics Society*, 63(4), S. 676-683. doi: 10.1111/jgs.13346.

Helberger, Natali; Lynskey, Orla; Micklitz, Hans-W.; Rott, Peter; Sax, Marjin und Strycharz, Joanna (2021): *EU Consumer Protection 2.0 – Structural asymmetries in digital consumer markets.* Brussels: The European Consumer Organisation, URL: https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-018_eu_consumer_protection_2.0.pdf.

Hlava, Daniel (2018): *Barrierefreie Gesundheitsversorgung, Rechtliche Gewährleistung unter besonderer Berücksichtigung der Rechtsdurchsetzung.* Baden-Baden: Nomos.

Hofmann, Franz und Raue, Benjamin (Hrsg.) (2023): *Digital Services Act.* Baden-Baden: Nomos.

Horstmann, Jan (2024): KI-VO und Datenschutz: Überblick und ausgewählte Fragen. *ZD-Aktuell*, 01580.

Kahle, Ute; Schädler, Johannes (Hrsg.) (2025): Digitale Teilhabe und personenzentrierte Technologien im Kontext von Menschen mit Behinderungen, Marburg: Lebenshilfe-Verlag

Kapoor, Arun und Klindt, Thomas (2024): Das Barrierefreiheitsstärkungsgesetz – Anforderungen an Webseiten und mobile Anwendungen. *Neue Juristische Wochenschrift,* 49/2024, S. 3545-3550.

Karaboga, Murat (2022): Datenschutzrechtliche Gestaltungsmöglichkeiten jenseits der Ermächtigung des Individuums: Die Multi-Stakeholder-Datenschutz-Folgenabschätzung. In: Friedewald, Michael; Kreutzer, Michael; Hansen, Marit (Hrsg.): *Selbstbestimmung, Privatheit und Datenschutz*. S. 275-302.

Koch, Heiner; Strathmann, Clara; Hennig, Marti; Schmied, Luisa; Geminn, Christian; Heesen, Jessica; Krämer, Nicole und Reinhardt, Karoline (2025): Diversitätsgerechter Privatheitsschutz in digitalen Umgebungen. In: Friedewald, Michael; Roßnagel, Alexander; Karaboga, Murat; Geminn, Christian (Hrsg.): *Freiheit in digitalen Infrastrukturen*. Im Erscheinen.

Kossens, Michael; Heide, Dirk von der und Maaß, Michael (Hrsg.) (2023): *SGB IX Rehabilitation und Teilhabe Menschen mit Behinderungen mit Behindertengleichstellungsgesetz*. 5. Auflage. München: Beck.

Kreutz, Marcus; Lachwitz, Klaus und Trenk-Hinterberger, Peter (Hrsg.) (2013): *Die UN-Behindertenrechtskonvention in der Praxis Erläuterungen der Regelung und Anwendungsgebiete*. Köln: Luchterhand.

Kroschwald, Steffen (2023): Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften Schutz, Selbstbestimmung und Teilhabe „by Design" vor dem Hintergrund des Art. 25 DSGVO und dem KI-Verordnungsentwurf. *Zeitschrift für Digitalisierung und Recht*, 1/2023, S. 1-22.

Krüger, Philipp-L. (2016): Datensouveränität und Digitalisierung, Probleme und rechtliche Lösungsansätze. *Zeitschrift für Rechtspolitik*, 7/2016, S. 190-192.

Kruse, Andreas (2017): *Lebensphase hohes Alter: Verletzlichkeit und Reife*. Heidelberg: Springer.

Kühl, Eike (2023): Das Nacktbild, das man nie geschossen hat. *Zeit Online* vom 14. Dezember 2023. URL: https://www.zeit.de/digital/internet/2023-12/deepnudes-nacktbilder-kuenstliche-intelligenz-deepfakes.

Kühling, Jürgen und Buchner, Benedikt (Hrsg.) (2024): *DSGVO – BDSG*. 4. Auflage. München: BECK.

Landesbeauftragte für Datenschutz Niedersachsen, Pressemitteilung 20/2024 vom 27.12.2024. https://www.lfd.niedersachsen.de/startseite/infothek/presseinformationen/verabschiedete-einwilligungsverwaltungsverordnung-verfehlt-ihr-eigentliches-ziel-238383.html.

Lenz, Susanne (2009): *Vulnerabilität kritischer Infrastrukturen. Forschung im Bevölkerungsschutz*. Band 4, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bonn.

Liedke-Deutscher, Bernd (Hrsg.) (2024): *Die datenschutzrechtliche Einwilligung nach der DSGVO*. Oldenburg: OlWIR.

Livingstone, Sonia; Stoilova, Mariya und Nandagiri, Rishita (2019): *Children's data and privacy online: Growing up in a digital age. An evidence review.* London: London School of Economics and Political Science.

Martini, Mario, Kramme, Inken und Kamke, Anton (2023): KI-VO, DMA und DA als Missing Links im Kampf gegen dunkle Designmuster? Das Digitalpaket der Union und seine vielschichtigen Regelungsansätze gegen Dark Patterns. *Zeitschrift für IT-Recht und Recht der Digitalisierung*, 6/2023, S. 399-403.

Masuch, Peter (20.03.2012): „Die UN- Behindertenrechtskonvention anwenden". *Forum D,* Diskussionsbeitrag Nr. 5 /2012. URL: www.reha-recht.de (besucht am: 15.02.2025).

Menzel, Hans-Joachim (2008): Datenschutzrechtliche Einwilligung. *Datenschutz und Datensicherheit,* 32(6), S. 400-408.

Mozilla Foundation (7. April 2024): EVA AI Chat Bot und Soulmate. URL: https://foundation.mozilla.org/de/privacynotincluded/eva-ai-chat-bot-soulmate/.

Müller-Terpitz, Ralf und Köhler, Markus (Hrsg.) (2024): *Digital Services Act*. München: Beck.

Naguib, Tarek; Pärli, Kurt; Landolt, Hardy; Demir, Eylem und Filippo, Martina (Hrsg.) (2023): *UNO-Behindertenrechtskonvention.* Bern: Stämpfli Verlag AG.

Nebel, Maxi (2015): Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung? Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht. *Zeitschrift für Datenschutz*, 11/2015, S. 517-521.

Nebel, Maxi (2022): Alles abwählen: Mit der Einwilligungsverwaltungs-Verordnung gegen den Cookie-Banner-Dschungel. *ZD-Aktuell*, 01321.

Nebel, Maxi (2025): Datenschutzrecht. In: Geminn, Christian L. und Johannes, Paul C. (Hrsg.): *Europäisches Datenrecht*. Baden-Baden: Nomos, im Erscheinen.

Paal, Boris P. und Pauly, Daniel A. (Hrsg.) (2021): *DSGVO/BDSG*. 3. Auflage. München: Beck.

Park, Yong Jin (2013): Digital Literacy and Privacy Behavior Online. *Communication Research,* 40(2), S. 215-236. https://journals.sagepub.com/doi/10.1177/0093650211418338.

Payne, Kate (2024): An AI chatbot pushed a teen to kill himself, a lawsuit against its creator alleges. *Associated Press* vom 24. Oktober 2024. URL: https://apnews.com/article/chatbot-ai-lawsuit-suicide-teen-artificial-intelligence-9d48adc572100822fdbc3c90d1456bd0.

Roller, Steffen (2019): UN-Behindertenrechtskonvention in der sozialgerichtlichen Praxis – anwaltliche Trumpfkarte oder juristische Nebelkerze? *Neue Zeitschrift für Sozialrecht*, 10/2019, S. 368-377.

Roßnagel, Alexander (2020): Der Datenschutz von Kindern in der Datenschutz-Grundverordnung: Vorschläge für die Evaluierung und Fortentwicklung. *Zeitschrift für Datenschutz*, 2/2020, S. 88-92.

Roßnagel, Alexander und Geminn, Christian (2020): *Datenschutz-Grundverordnung verbessern: Änderungsvorschläge aus Verbrauchersicht.* Baden-Baden: Nomos.

Roßnagel, Alexander; Bile, Tamer; Nebel, Maxi; Geminn, Christian; Karaboga, Murat; Ebbers, Frank; Bremert, Benjamin; Stapf, Ingrid; Teebken, Mena; Thürmel, Verena; Ochs, Carsten; Uhlmann, Markus; Krämer, Nicole; Meier, Yannic; Kreutzer, Michael; Schreiber, Linda und Simo, Hervais (2020): *Einwilligung – Möglichkeiten und Fallstricke aus der Konsumentenperspektive* [White Paper]. Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. Herausgeber: Michael Friedewald, Regina Ammicht Quinn, Marit Hansen, Jessica Heesen, Thomas Hess, Nicole Krämer, Jörn Lamla, Christian Matt, Alexander Roßnagel, Michael Waidner. Karlsruhe: Fraunhofer ISI.

Roßnagel, Alexander; Pfitzmann, Andreas und Garstka, Hansjürgen (2001): Gutachten im Auftrag des Bundesministeriums des Innern. Modernisierung des Datenschutzrechts. Berlin. URL: http://www.datenschutzgeschichte.de/pub/dphistory/2001_GarskaPfitzmannRossnagel_Modernisierung_des_Datenschutzrechts.pdf (besucht am 27.2.2025).

Roßnagel, Alexander; Wedde, Peter; Hammer, Volker und Pordesch, Ulrich (2002/2009): *Die Verletzlichkeit der ‚Informationsgesellschaft'.* 3. Auflage (elektronische Fassung). https://d-nb.info/998894990/34.

Simitis, Spiros (Hrsg.) (2011): Bundesdatenschutzgesetz, 7 Auflage. Baden-Baden: Nomos.

Simitis, Spiros; Hornung, Gerrit und Spiecker gen. Döhmann, Indra (Hrsg.) (2025): *Datenschutzrecht.* 2. Auflage. Baden-Baden: Nomos.

Skjuve, Marita; Følstad, Asbjørn; Fostervold, Knut und Brandtzaeg, Petter (2021): My Chatbot Companion – a Study of Human-Chatbot Relationships. *International Journal of Human-Computer Studies,* 149/2021, 102601. https://doi.org/10.1016/j.ijhcs.2021.102601.

Strauß, Stefan und Bettin, Steffen (2023): Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen – Entwicklungsstand, Trends und zentrale Herausforderungen (Projektbericht). Wien: Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften. URL: https://epub.oeaw.ac.at/0xc1aa5576%200x003e44d2.pdf (besucht am 27.2.2025).

Strauß, Stefan und Krieger-Lamina, Jaro (2017): Digitaler Stillstand: Die Verletzlichkeit der digital vernetzten Gesellschaft – Kritische Infrastrukturen und Systemperspektiven. Wien: Institut für Technikfolgen-Abschätzungen der Österreichischen Akademie der Wissenschaften. URL: https://www.researchgate.net/publication/316487129_Digitaler_Stillstand_Die_Verletzlichkeit_der_digital_vernetzten_Gesellschaft_-_Kritische_Infrastrukturen_und_Systemperspektiven.

Tabbara, Annette (2021): Barrierefreiheit für elektronische Produkte und Dienstleistungen – das Barrierefreiheitsstärkungsgesetz. *Neue Zeitschrift für Sozialrecht*, 13/2021, S. 497-502.

Taeger, Jürgen (2021): Einwilligung von Kindern gegenüber Diensten der Informationsgesellschaft. *Zeitschrift für Datenschutz,* 9/2021, S. 505-508.

Trepte, Sabine; Teutsch, Doris; Masur, Philipp K.; Eicher, Carolin; Fischer, Mona und Hennhöfer, Alisa (2015): Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale"(OPLIS). In: Gutwirth, Serge; Leenes, Ronald und de Hert, Paul (Hrsg.): *Reforming European data protection law.* Dordrecht: Springer, S. 333-365. https://doi.org/10.1007/978-94-017-9385-8_14.

Turner, B. L.; Kasperson, Roger; Matson, Pamela; McCarthy, James; Corell, Robert; Christensen, Lindsey; Eckley, Noelle; Kasperson, Jeanne; Luers, Amy; Martello, Marybeth; Polsky, Colin; Pulsipher, Alexander und Schiller, Andrew (2003): A framework for vulnerability analysis in sustainability science. *Proceedings of the National Academy of Sciences of the United States of America,* 100(14), S. 8074-8079. https://doi.org/10.1073/pnas.1231335100.

UN (2004): Living with Risk – A global review of disaster reduction initiatives. New York/Genf: United Nations. URL: https://www.unisdr.org/files/657_lwr1.pdf (besucht am 26.03.2025).

Uziel-Karl, Sigal und Tenne-Rinde, Michal (2018): Making language accessible for people with cognitive disabilities: Intellectual disability as a test case. In: Bar-On, Amalia und Dorit, Ravid (Hrsg.): *Handbook of Communication Disorders Theoretical, Empirical, and Applied Linguistic Perspectives.* Boston/Berlin: Walter de Gruyter Inc, S. 845-862.

Von Boetticher, Arne und Kuhn-Zuber, Gabriele (2021): *Rehabilitationsrecht ein Studienbuch für soziale Berufe*. 2. Auflage, Baden-Baden: Nomos.

Wehde, Alexander (2023): Regulierung von Large Language Models in DSA und AIA-E. *MMR-Aktuell*, 455171.

Wolff, Heinrich A.; Brink, Stefan und v. Ungern-Sternberg, Antje (Hrsg.) (2023): *BeckOK Datenschutzrecht.* 51. Edition. München: Beck.

Algorithmen-Transparenz und -Kompetenz als Säulen der informationellen Selbstbestimmung: Ein nutzerzentrierter Blick

German Neubaum

Zusammenfassung
Algorithmen beeinflussen zunehmend, wie Informationen in digitalen Medien gefiltert und präsentiert werden. Die algorithmische Kuratierung von Inhalten auf Basis privater Nutzerdaten bringt allerdings Risiken mit sich. Diese sind den Nutzenden jedoch oft nicht bewusst, da die Algorithmen-Kompetenz in der Bevölkerung insgesamt gering ausgeprägt und ungleich verteilt ist. Um dem entgegenzuwirken, werden eine stärkere Transparenz der Funktionsweise von Algorithmen sowie eine Verbesserung der Algorithmen-Kompetenz der Nutzer:innen gefordert. Dieses Buchkapitel fasst den aktuellen Forschungsstand zu Algorithmen-Transparenz und -Kompetenz zusammen und legt den Fokus auf die potenziell wachsende Kluft zwischen Menschen mit hoher und niedriger Algorithmen-Kompetenz. Um diese Kluft zu verringern, plädiert dieser Beitrag für einen nutzerzentrierten Ansatz, der eine Rekonzeptualisierung von Algorithmen-Kompetenz nicht nur im Hinblick auf Datenschutz und den Schutz der Privatheit, sondern auch hinsichtlich der persönlichen und gesellschaftlichen Folgen fordert. Zudem wird skizziert, warum eine dynamische, an die Bedürfnisse der Nutzer:innen angepasste Vermittlung von Algorithmenwissen notwendig ist und wie dies durch adaptive, intelligente Lernsysteme umgesetzt werden kann.

1. Einleitung

Algorithmen prägen maßgeblich unsere digitale Welt. Basierend auf Verhaltensdaten und persönlichen Informationen der Nutzer:innen entscheiden Algorithmen darüber, welche Werbung in welcher Reihenfolge angezeigt wird, welche Online-Videos empfohlen werden oder ob eine bestimmte Berichterstattung über das Zeitgeschehen im Social-Media-Feed erscheint (Haim u.a. 2018; Jürgens/Stark 2022; Van Hoof u.a. 2024). Einerseits scheint dies im Sinne der Nutzenden: Algorithmen filtern und priorisieren Informationen in Online-Netzwerken, um die knappen kognitiven Ressourcen der Konsumierenden zu schützen und Nutzende vor einer Informationsüberflutung zu bewahren (Merten 2021). Gleichzeitig sorgen sie dafür, dass Nutzende vorwiegend Inhalte sehen, die für sie persönlich relevant sind, wodurch vermeintlich irrelevante Informationen ausgeblendet werden. Diese vermeintlichen Vorteile gehen jedoch mit offensichtlichen Einbußen im Datenschutz und in der informationellen Selbstbestimmung der Nutzenden einher. Digitale Plattformen verwenden persönliche Daten von Nutzenden zur Fütterung von Algorithmen, ohne sie ausreichend da-

rüber aufzuklären und ohne das Einverständnis, ob sie die wiederholte Verarbeitung persönlicher Daten zulassen (Dobber 2023). Verzerrende algorithmische Logiken, ideologische Tendenzen und bezahlte Platzierungen beeinflussen, welche Inhalte in Social-Media-Feeds priorisiert angezeigt werden (Alavi u.a. 2024; Fosch-Villaronga u.a. 2021; González-Bailón u.a. 2023). Es wurde wiederholt dokumentiert, dass die in Suchmaschinen oder Nachrichtenseiten operierenden Algorithmen die Informationslandschaft nicht ausgewogen, sondern entlang der individuellen Präferenzen darstellen, was langfristig zur ungleichen Verbreitung von Nachrichten und gesellschaftlich relevantem Wissen führen kann (Ekström u.a. 2024; Epstein/Li 2024; Evans u.a. 2023; Gezici u.a. 2021; Nechushtai u.a. 2024).

Diese potenziellen Folgen der algorithmenbasierten Kuratierung aktueller Kommunikationstechnologien geraten in den Fokus, wenn Studien immer wieder aufzeigen, dass Menschen insgesamt ein recht niedriges Bewusstsein und geringes Wissen über die Funktionsweise und Folgen von Informationsvermittlung durch algorithmische Systeme haben (Cotter/Reisdorf 2020; Gran u.a. 2021; Oeldorf-Hirsch/Neubaum 2023; Zarouali u.a. 2021b). Dies wirft die Frage auf, ob der Einsatz von Personalisierungs- und Filteralgorithmen in sozialen Medien und Suchmaschinen mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar ist.

Vor diesem Hintergrund greift dieses Buchkapitel einen öffentlich diskutierten Lösungsvorschlag auf, nämlich die Steigerung der Algorithmen-Transparenz (seitens der Anbieter algorithmischer Systeme) und der Algorithmen-Transparenz (seitens der Nutzenden). Dabei wird zunächst der State-of-the-Art zu beiden Konzepten präsentiert, um darauf aufbauend Desiderata in Forschung und in Praxis herauszuarbeiten.

2. Begriffsbestimmung: Was ist Algorithmen-Kompetenz und Algorithmen-Transparenz?

2.1 Algorithmen-Kompetenz

Ein Algorithmus wird allgemein als eine Abfolge von Aufgaben verstanden, die innerhalb eines Systems (z. B. einer Suchmaschine oder einer sozialen Medienplattform) automatisiert einen Output (z. B. eine Empfehlung) auf Basis eines Inputs (z. B. Nutzerdaten) generiert (Rader u. a. 2018). Demnach basieren alle denkbaren digitalen Technologien auf Algorithmen. Um sich dem Konzept der Algorithmen-Kompetenz möglichst präzise zu

nähern, konzentriert sich dieses Buchkapitel auf Personalisierungs- und Filteralgorithmen in weit verbreiteten Technologien wie sozialen Medien (z. B. TikTok, Instagram) sowie Suchmaschinen und verwandten Diensten (z. B. Google News).

In der Fach-Literatur wird im Bereich der „AI Literacy" das Konzept der Algorithmen-Kompetenz mit unterschiedlichen Termini wie „algorithmic literacy", „algorithmic knowledge" oder „algorithmic awareness" adressiert (Oeldorf-Hirsch/Neubaum 2025; Reisdorf/Blank 2021a; Silva u.a. 2022). Mit unterschiedlichen Schwerpunkten je nach Quelle wird unter Algorithmen-Kompetenz das Bewusstsein über die Präsenz und Funktionsweise von Algorithmen sowie die Fähigkeit der Nutzenden mit diesen Algorithmen zu interagieren (DeVito 2021; Dogruel u.a. 2022) verstanden. Demgegenüber steht der Ansatz von Zarouali, Boerman u.a. (2021), die mit der „algorithmic media content awareness scale" empirisch erfassbare Dimensionen definieren, die diverse Bereiche abdecken: *(1) Filterung von Inhalten*: Das Bewusstsein darüber, dass Algorithmen die gezeigten Inhalte auf Basis von Online-Daten auf Personen individuell zuschneiden. *(2) Automatisierte Entscheidungsfindung*: Kenntnisse darüber, dass Algorithmen automatisierte Entscheidungen treffen, um Nutzende bestimmte Inhalte zu zeigen. *(3) Mensch-Algorithmus-Zusammenwirken*: Wissen darüber, dass menschliches Verhalten die Entscheidung prägt, welche Inhalte Nutzenden angezeigt wird. *(4) Algorithmenbasierte Persuasionskraft*: Bewusstsein darüber, dass Algorithmen genutzt werden können, um menschliche Einstellungen und Verhaltensweisen zu beeinflussen. *(5) Ethische Aspekte*: Reflexionskompetenz über ethische Bedenken zu algorithmisch selektieren Inhalten. Angesichts dieser Bandbreite an Kompetenz-Feldern schlagen Oeldorf-Hirsch und Neubaum (2025) einen integrativen Ansatz zur Konzeptualisierung der „algorithmic literacy" vor, in dem die Reaktionen des menschlichen Users nach Kognition, Emotion und Verhalten sortiert werden: *(a) Kognitive Dimension*: Bewusstsein, Kenntnisse und Wissen über die Funktionsweise von Algorithmen. *(b) Affektive Dimension*: Bewertung und Empfindungen gegenüber Algorithmen (z.B. Abneigung gegenüber der algorithmenbasierten Filterung, Entscheidung oder Empfehlung). *(c) Behaviorale Dimension*: Fähigkeit mit Algorithmen zu interagieren und ihnen entgegenzuwirken. Insgesamt gilt das Konzept der Algorithmen-Kompetenz demnach nicht nur als die Repräsentation von Wissen, sondern auch als die Fähigkeit anhand des Wissens Systeme zu bewerten und entsprechend zu handeln.

2.2 Algorithmen-Transparenz

Die Algorithmen-Transparenz wird ebenfalls in unterschiedlichen Domänen der Literatur diskutiert. Allgemein wird unter „Algorithmen-Transparenz" die Offenlegung von nicht offensichtlichen Informationen über die Funktionsweise und die Kriterien von Personalisierungs- und Filteralgorithmen, die individuellen Nutzenden nicht unmittelbar durch eigene Erfahrungen mit Algorithmen zugänglich sind (Bitzer u.a. 2023; Rader u.a. 2018), verstanden. Innerhalb der definitorischen Anstrengungen wird deutlich, dass die Transparenz unmittelbar die Kompetenz der Nutzenden erhöhen soll, im Sinne von „enabl[ing] understanding, critical review, and adjustment" (Bitzer, Wiener, & Cram, 2023, S. 293). Algorithmen-Transparenz gilt als besonders wertvoll, da sie negative Effekte von kuratierend arbeitenden Systemen reduzieren soll, indem Nutzer:innen mit der Funktionsweise und den Entscheidungskriterien solcher Systeme besser vertraut gemacht werden (Rader u.a. 2018).

Der Fokus der Algorithmen-Transparenz ist eng verwoben mit dem Bereich der Explainable AI (XAI), der sich der Nachvollziehbarkeit und Haftbarkeit von algorithmischen Entscheidungen in intelligenten Systemen verpflichtet (De Bruijn u.a. 2022). Während der XAI-Bereich einen sehr starken Fokus auf die technische Nachvollziehbarkeit von Künstliche Intelligenz-Modellen hat, wird die Algorithmen-Transparenz nicht nur technisch, sondern auch ethisch und vor allem rechtlich betrachtet (Lu u.a. 2019). Demnach wird systematisch analysiert, in welcher Ausprägung Provider von algorithmischen Systemen entlang europäischer Regelungen, d.h. der Datenschutz-Grundverordnung (DSGVO) und der KI-Verordnung, eine Rechenschaftspflicht haben und wann diese als nachgekommen gilt (Busuioc u.a. 2023; Tzimas 2023).

Demnach wird deutlich, dass Algorithmen-Transparenz nicht in einem Vakuum, sondern in einem Spannungsfeld unterschiedlicher Interessen von Unternehmen (Social Media-Anbietern oder Nachrichtenorganisationen), Regierungen und individuellen Nutzenden (Diakopoulos 2020; Diakopoulos/Koliska 2017) umgesetzt werden muss. Um die Algorithmen-Transparenz nicht nur mit Informationen der Tech-Unternehmen zu steigern, plädiert AlgorithmWatch für externe Auditings mit Hilfe von freiwilligen Datenspenden der Nutzenden. Hierbei soll mit Hilfe ihrer Daten die Funktionsweise der Empfehlungsalgorithmen (z.B. TikTok) entschlüsselt und ihre Auswirkungen (z.B. auf die überproportionale Darstellung von politisch extremen Inhalten) erfasst werden (Albert 2023; Kayser-Bril 2021).

Wenn die Transparenzmaßnahmen von Tech-Unternehmen weiterhin rudimentär bleiben – und selbst diese begrenzte Aufklärung über die Funktionsweise von Algorithmen nicht zu einem erhöhten Bewusstsein bei den Nutzer:innen führt –, wird deutlich, dass es Mechanismen braucht, um sowohl Transparenz als auch Kompetenz gezielt zu stärken. Ohne grundlegende Informationen können weder Kenntnisse noch Fähigkeiten entwickelt werden. Gleichzeitig – wie im weiteren Verlauf des Textes ausgeführt wird – reicht eine rein technische und komplexe Aufklärung über algorithmische Kuratierung nicht aus, um informationelle Selbstbestimmung zu gewährleisten. Daher plädiert dieser Beitrag für ein *wechselseitiges Verhältnis von Transparenz und Kompetenz*: Die Gestaltung von Algorithmen-Transparenz sollte sich an der bestehenden (und sich dynamisch entwickelnden) Algorithmen-Kompetenz der Nutzer:innen orientieren. Abbildung 1 skizziert die zentralen Komponenten beider Konzepte im Lichte der informationellen Selbstbestimmung.

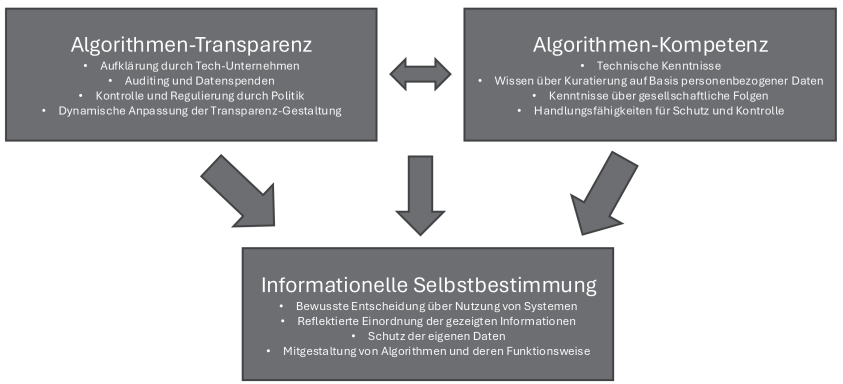

Abbildung 1: Das reziproke Verhältnis von Algorithmen-Transparenz und -Kompetenz zur Sicherung der informationellen Selbstbestimmung

3. Determinanten der individuellen Algorithmen-Kompetenz: Eine wachsende Kluft?

Dem Ideal folgend, dass Algorithmen-Kompetenz dafür sorgen wird, dass Menschen selbstbestimmt und reflektiert aktuelle Technologien nutzen werden, hat sich eine Forschungsreihe der Frage gewidmet, wie Algorith-

men-Kompetenz unter den Nutzenden solcher Systeme ausgeprägt ist. Eine Studie der Bertelsmann Stiftung zeigte, dass sich in der deutschen Bevölkerung zwar das subjektive Wissen zu Algorithmen und Künstlicher Intelligenz Jahren zwischen 2018 und 2022 erhöht hat, unter Bürger:innen jedoch große Unklarheit herrscht, inwiefern Algorithmen ihr Leben direkt prägen und ob Algorithmen zu gesellschaftlicher Gerechtigkeit beitragen (Overdiek/Petersen 2022). Unter dem Forschungsbereich der digitalen Kluft („digital divide"; Gran u.a. 2021; Reisdorf/Blank 2021b) wird untersucht, ob sozio-demografische Faktoren bestimmen, wie stark die „algorithmic awareness" oder allgemein algorithmisches Wissen in der Bevölkerung verbreitet ist. Mit einer nordamerikanischen Stichprobe stellten Cotter und Reisdorf (2020) fest, dass Nutzende algorithmischer Systeme mit höherer Bildung und mit niedrigerem Alter über mehr Wissen zur Funktionsweise verfügten. Diese Befunde bestätigten Gran u.a. (2021) mit einer norwegischen Stichprobe und fanden zusätzlich, dass Männer eine stärker ausgeprägte „algorithmic awareness" haben als Frauen, was nicht mit Bildungsunterschieden zwischen den Geschlechtern zu erklären ist. Mit einem Blick auf "algorithmic misconceptions" (d.h. falsche Annahmen über die Funktionsweise von Algorithmen) zeigten Zarouali u.a. (2021b) auf, dass diese bei älteren, weiblichen und weniger gebildeten Nutzenden stärker ausgeprägt sind. Ein direkter Vergleich zwischen den USA und Deutschland von Oeldorf-Hirsch und Neubaum (2023) zeigte, dass in beiden Ländern ein niedrigeres Alter sowie eine höhere Bildung mit einem stärkeren algorithmischen Bewusstsein einhergingen. Allerdings war dieses Bewusstsein unter US-amerikanischen Nutzenden ausgeprägter als unter deutschen Nutzenden. Dieser Unterschied könnte darauf zurückzuführen sein, dass soziale Medien – die in der Studie untersuchten Plattformen – in den USA insgesamt häufiger und intensiver genutzt werden als in Deutschland. Dadurch könnten US-amerikanische Nutzende mehr Erfahrung mit Algorithmen und deren Wirkweise haben. Es lässt sich ferner vermuten, dass neben fehlender Erfahrung im Umgang mit Algorithmen auch strukturelle Ungleichheiten – etwa beim Zugang zu digitaler Medienbildung oder in Bezug auf die Kompetenz zur Verarbeitung komplexer technischer Informationen – zur ungleichen Verteilung von algorithmischem Wissen und Bewusstsein beitragen.

Angesichts dieser Beobachtungen bringen Forschende die Perspektive zur Diskussion, ob die ungleiche Verteilung von Algorithmen-Kompetenz in den Bevölkerungen langfristig zu einer wachsenden Kluft zwischen den sogenannten Informationsreichen und den Informationsarmen führen

könnte (Cotter/Reisdorf 2020; Oeldorf-Hirsch/Neubaum 2023). Denkbar wäre, dass Menschen mit einem niedrigen Bewusstsein gegenüber der Funktionsweise von Algorithmen aufgrund der Personalisierung und Filterung unausgewogen informiert sind, verzerrte Schlussfolgerungen ziehen oder womöglich persönliche oder politisch relevante Entscheidungen auf Basis einer verzerrten Informationslage treffen.

Studien zeigen, dass Menschen, die sich der Präsenz und Funktionsweise von Algorithmen stärker bewusst sind, auch differenziertere Meinungen zu Algorithmen haben – sowohl positiv als auch negativ (Gran u.a. 2021; Oeldorf-Hirsch/Neubaum 2023). Demnach spiegeln sich ihre differenzierten Kenntnisse auch in ihren persönlichen Einstellungen wider. Aber nicht nur das: Eine stärker ausgeprägte „algorithmic awareness" geht ebenfalls mit individuellen Praktiken einher, die der algorithmischen Filterung entgegenwirken (z.B. Cookies zu löschen; Oeldorf-Hirsch/Neubaum 2023). Letzteres zeigt, dass es lohnend ist, die Kluft im algorithmischen Wissen der Bevölkerung zu schließen, damit Nutzende bewusster ihre Informationslandschaft gestalten können. Der State-of-the-Art zur Algorithmen-Kompetenz eröffnet eine Reihe weiterer Fragen, die konkrete Implikationen für Forschung und Praxis haben. Diese werden im Folgenden erörtert.

4. Offene Fragen und ein Plädoyer für einen nutzerzentrierten Ansatz der Algorithmen-Transparenz und -Kompetenz

4.1 Ganzheitliche Charakterisierung und Operationalisierung von Algorithmen-Kompetenz

Zunächst fällt angesichts des Forschungsstands auf, dass fundamentale Bereiche, die unmittelbar mit der Funktionsweise und Wirkung von Algorithmen verwoben sind, nicht in den bisherigen Konzeptualisierungen und Operationalisierungen von Algorithmen-Kompetenz berücksichtigt sind. Dazu gehören a) der Schutz persönlicher Daten und Selbstbestimmung, b) die Kontrollmöglichkeiten des menschlichen Users und c) die persönlichen und gesellschaftlichen Konsequenzen einer algorithmischen Kuratierung.

4.1.1 Schutz persönlicher Daten und Selbstbestimmung

Zur Algorithmen-Kompetenz sollte nicht nur ein Verständnis über die Funktionsweise von Algorithmen gehören, sondern auch das Wissen da-

rüber, welche Daten, Praktiken und Verhaltensweisen der Nutzenden von Algorithmen zur Personalisierung und Filterung genutzt werden (Shin u.a. 2022). Nutzende sollten nachvollziehen können, wie diese Daten erhoben, verarbeitet und gespeichert werden und über welchen Zeitraum dies geschieht. Darüber hinaus ist es essenziell, dass sie Strategien kennen, um dieser Datensammlung entgegenzuwirken und somit ihre Informationslandschaft aktiv und selbstbestimmt zu gestalten. Auch das Geschäftsmodell hinter Ranking-Algorithmen und welche Konsequenzen Gegenmaßnahmen (z.B. Ablehnung der Datenverarbeitung) langsfristig haben könnten, sollten bewusst gemacht werden. Ohne ein fundiertes Verständnis für Datenschutz und den Schutz der eigenen Privatheit (das entsprechende Schutz-Handlungen ermöglicht) bleibt die Konzeptualisierung von Algorithmen-Kompetenz unvollständig. Dies hat nicht nur theoretische, sondern auch praktische Implikationen: Eine unzureichende Berücksichtigung dieses Aspekts erschwert die Operationalisierung und Vermittlung von Algorithmen-Kompetenz im Bildungskontext sowie in der öffentlichen Debatte.

4.1.2 Kontrolle des Algorithmus durch den menschlichen User

Mit dem Aufkommen von Technologien wie TikTok, deren Filteralgorithmus durch intensive Erfahrung transparenter zu entschlüsseln ist (Siles u.a. 2024), eröffnet sich eine neue Dimension der Algorithmen-Kompetenz, nämlich die aktive Kontrolle bis hin zur Manipulation des Algorithmus. Hierbei können Nutzende Inhalte bewusst auswählen und entsprechend lange konsumieren, sodass der Algorithmus die Interessen und Bedarfe der Nutzenden präziser erkennt (Kang/Lou 2022). Eine solche verhaltensorientierte Kompetenz, die unmittelbares Feedback zeigt (nämlich eine eindeutig personalisierte Kuratierung von Inhalten) kann Nutzende eine stärkere Autonomie verleihen und damit die Akzeptanz der Technologie verbessern (Issar 2024).

4.1.3 Persönliche und gesellschaftliche Konsequenzen einer algorithmischen Kuratierung

Obwohl bisherige Konzeptualisierungen und Operationalisierungen von Algorithmen-Kompetenz ethische Aspekte wie mangelnde Transparenz abdecken, bleibt diese Dimension recht abstrakt und unterspezifiziert. Es

ist essenziell, dass Nutzende konkretes Wissen darüber erlangen, dass Algorithmen in Suchmaschinen und sozialen Medienplattformen die ungleiche Verbreitung von Wissen und tagesaktuellen Nachrichten begünstigen (Jürgens/Stark 2022; Nechushtai u. a. 2024), politische Wahlentscheidungen beeinflussen (Epstein/Li 2024) und Empfehlungen oder Filterentscheidungen treffen können, die aufgrund rassistischer oder sexistischer Verzerrungen diskriminierend sind (Lin u. a. 2023; Rogers 2023; Zou/Schiebinger 2018). Was diese Kuratierung potenziell für Nutzende persönlich, aber auch langfristig für die Gesellschaft (z.B. Polarisierung von politischen Meinungen oder Fragmentierung) bedeuten könnte, sollte als eine zentrale Säule der Algorithmen-Kompetenz angesehen werden.

All diese Punkte erfordern nicht nur eine Neukonzeption von Algorithmen-Kompetenz, sondern auch ihre präzise Operationalisierung. Dabei sollte sowohl subjektives als auch objektives Wissen über die Funktionsweise sowie über individuelle und gesellschaftliche Folgen algorithmischer Kuratierung erfasst werden. In diesem Zusammenhang ist es essenziell zu prüfen, ob Nutzende über die Fähigkeit verfügen, mit eigenen Handlungen algorithmischen Auswahlprozessen entgegenzuwirken oder diese gezielt zu ihrem Vorteil zu nutzen. Leitbilder dafür können Operationalisierungen der Online Privacy Literacy sein, welche unterschiedliche Dimensionen, u.a. konkrete Maßnahmen des Privatheitsschutzes, abdeckt (Trepte et al. 2015).

4.2 Langfristige Effekte einer ungleichen Verteilung von Algorithmen-Kompetenz

Trotz der Debatte über eine potenziell wachsende Kluft zwischen Nutzenden mit hoher und niedriger Algorithmen-Kompetenz (Cotter/Reisdorf 2020; Oeldorf-Hirsch/Neubaum 2023), fehlt bislang gänzlich längsschnittliche Evidenz, um diesen erwarteten Trend empirisch zu untermauern. Mit einem solchen Ansatz könnten nicht nur besonders benachteiligte Zielgruppen für Interventionen (zur Förderung der Algorithmen-Kompetenz), sondern auch langfristige Effekte einer wachsenden Kluft identifiziert werden. Im Hinblick auf politische Bildung wäre demnach denkbar, dass Menschen, die sich der algorithmischen Kuratierung nicht bewusst sind, die Selbstwahrnehmung haben, umfangreiches und differenziertes subjektives politisches Wissen zu haben, was sich aber nicht in ihrem objektiv gemessenen politischen Wissen beobachten lässt (Dreston/Neubaum 2023; Lee u.a.

2022). Mangelnde Algorithmen-Kompetenz wäre so für eine Fehlkalibrierung des politischen Wissens, bei dem subjektives und objektives Wissen niedrig miteinander korrelieren (Dreston/Neubaum 2023), veranwortlich. Diese Frage ist eng mit der Annahme verknüpft, dass Menschen, die in algorithmisch kuratierten Informationsumgebungen einseitig informiert werden, sich zunehmend aus der demokratischen Teilhabe und politischen Partizipation zurückziehen (Boulianne/Hoffmann 2024). Umgekehrt gedacht ließe sich fragen: Kann die Erhöhung der Algorithmen-Kompetenz langfristig zur gesellschaftlichen Inklusion beitragen?

Gleichzeitig wäre zu überprüfen, ob eine höhere Algorithmen-Kompetenz tatsächlich Menschen dazu bringt, verstärkt Maßnahmen zu ergreifen, die der Filterung und Personalisierung durch Algorithmen entgegenwirken (z. B. den Inkognito-Modus nutzen), oder ob dies von dispositionellen und motivationalen Faktoren abhängt. Denkbar wäre beispielsweise, dass Individuen, die sich eigenen Weltbildern defensiv gegenüber fühlen und sich ein informationell gleichförmiges Netzwerk wünschen, die Homogenisierung durch Filterung und Personalisierung begrüßen (Oeldorf-Hirsch/Neubaum 2023). Demnach würde eine hohe Algorithmen-Kompetenz auch in solchen Fällen nicht zu einem ausgewogenen Informationskonsum führen.

4.3 Eine dynamische Sicht auf Algorithmen-Transparenz

Die Annahme, dass eine Erhöhung der Algorithmen-Transparenz, wie sie z.B. europarechtlich durch die KI-Verordnung gefordert wird, unweigerlich die Algorithmen-Kompetenz von Nutzenden erhöhen würde, erinnert an die überholten Modelle „Hypodermic Needle Model“ oder „Stimulus-Response-Model“ der Medienwirkungsforschung (Finklea 2017). Hierbei geht man davon aus, dass eine Botschaft (z.B. eine Erklärung zur Funktionsweise von Algorithmen) eine unidirektionale Wirkung auf Rezipierende hat (z.B. die Erhöhung des Wissens zu Algorithmen), indem sie alle Rezipierende gleichmäßig erreicht und beeinflusst. Außer Acht wird hier jedoch gelassen, dass Menschen Vorerfahrungen, vorherrschende Motive, Überzeugungen oder Kenntnisse mitbringen, die die Wirkung dieser Botschaft modifizieren können.

Diese individuellen Bedingungen sollten bei der Gestaltung der Algorithmen-Transparenz berücksichtigt werden. Vorstellbar wäre eine dynamische und reaktive Gestaltung der Algorithmen-Transparenz, bei der Erklärungen

zur Funktions- und Wirkungsweise von Personalisierungsalgorithmen an die Bedarfe, Vorkenntnisse und Wünsche von Nutzenden angepasst werden. Im Bereich des adaptiven Lernens wird das Konzept des „Scaffoldings" herangezogen, bei dem die lehrende Instanz die Unterstützung und Instruktionen je nach individuellem Fortschritt und Bedarf der Lernenden anpasst (Van De Pol u.a. 2010).

Eine dynamische Gestaltung der Algorithmen-Transparenz scheint insbesondere durch aktuell aufkommende intelligente Tutoring-Systeme gut umsetzbar, in denen Chatbots die Nutzung der Technologie begleitet und dabei an Nutzende individuell angepasste Instruktionen (z.B. zur Filterung durch Algorithmen und deren Wirkung) gibt (Albacete u.a. 2019; Holmes u.a. 2023). Ein solcher Ansatz würde sicherstellen, dass vulnerable Gruppierungen (z.B. mit niedriger Bildung, mit Behinderungen) effektive Unterstützung bekommen und die Algorithmen-Transparenz zielgruppenspezifisch zugänglich gemacht wird (Luria 2023; Van Den Bogaert u.a. 2024).

4.4 Die Verantwortung der Politik und der Technologie-Betreiber:innen

Der Bereich der Algorithmen-Transparenz und insbesondere der Algorithmen-Kompetenz wird sehr häufig mit Bildungsinitiativen in Verbindung gebracht, bei denen die Verantwortung sowohl bei den Bildungsinstitutionen als auch bei den Nutzenden selbst liegt. So fundamental ein Bildungskonzept im Bereich der Algorithmen-Transparenz und -Kompetenz auch ist, die Verantwortung politischer Akteure und der Tech-Unternehmen darf nicht vergessen werden. Regulierungen wie die KI-Verordnung sind erste Schritte, um von politischer Seite Unternehmen in die Verantwortung zu nehmen, dass sie die immer noch bestehende „Black Box" von Filter- und Personalisierungsalgorithmen öffnen und transparent machen, welche Daten diese intelligenten Systeme wie nutzen (Busuioc u.a. 2023; Chaudhary 2024). Auf die rechtliche Rahmung für die Rechenschaftspflicht der Unternehmen sollte die Kontrolle folgen, ob tatsächlich eine Algorithmen-Transparenz hergestellt wird. Diese ist essenziell für den weiteren Aufbau von Bildungsinitiativen, bei denen Transparenz und die Kompetenz der Nutzenden iterativ angepasst wird. Demnach ist eine enge Zusammenarbeit zwischen Politik, Tech-Unternehmen und Bildungsinstitutionen entscheidend, um Transparenz, Verantwortung und Kompetenz im Bereich der Algorithmen und KI zu fördern. Nur so kann gewährleistet werden, dass

diese Technologien im Einklang mit den Grundrechten, Bedürfnissen und Werten einer Gesellschaft eingesetzt werden.

5. Fazit

Mit dem Aufkommen intelligenter Kommunikationssysteme, die der Zivilgesellschaft zugänglich sind, entsteht die Herausforderung, Bürger:innen in die Lage zu versetzen, diese Technologien selbstbestimmt zu nutzen – unter Wahrung ihrer Grundrechte. Ein zentraler Bestandteil dieser Befähigung ist die Aufklärung über die Funktions- und Wirkungsweise von Algorithmen. Angesichts der ungleichen Verteilung der Algorithmen-Kompetenz unter den Technologie-Nutzenden gibt es rechtliche Forderungen nach einer stärkeren Algorithmen-Transparenz. Eine transparente Darstellung von algorithmischen Prozessen auf beliebten Plattformen reicht jedoch nicht aus, wenn sie von technischem Jargon und komplexen Erläuterungen geprägt ist. Eine dynamische, an die Bedürfnisse der Nutzenden angepasste Vermittlung von Algorithmenwissen könnte dazu beitragen, die gesellschaftlichen Klüfte in der Algorithmen-Kompetenz zu verringern. Dabei sollten Nutzende darüber aufgeklärt werden, wie Algorithmen persönliche Daten und Online-Praktiken zur Personalisierung heranziehen. Nur so kann eine selbstbestimmte Nutzung digitaler Anwendungen gewährleistet werden. Bei der dynamischen Vermittlung von Algorithmen-Transparenz könnten genau solche intelligenten Systeme genutzt werden, um Unterstützung und Hilfestellungen zu personalisieren und so für eine tatsächliche, für alle zugängliche Transparenz komplexer Systeme zu sorgen.

Literatur

Alavi, Setareh; Iyer, Pooja und Bright, Laura F. (2024): Advertisement Avoidance and Algorithmic Media: The Role of Social Media Fatigue, Algorithmic Literacy and Privacy Concerns. In: Journal of Digital & Social Media Marketing 12(3), S. 276. https://doi.org/10.69554/KWTX2523.

Albacete, Patricia; Jordan, Pamela; Katz, Sandra; Chounta, Irene-Angelica und McLaren, Bruce M. (2019): The Impact of Student Model Updates on Contingent Scaffolding in a Natural-Language Tutoring System. In: Isotani, Seiji/Millán, Eva/Ogan, Amy/Hastings, Peter/McLaren, Bruce/Luckin, Rose (Hrg.): Artificial Intelligence in Education, Bd. 11625. Cham: Springer International Publishing. S. 37–47. (= Lecture Notes in Computer Science) https://doi.org/10.1007/978-3-030-23204-7_4.

Albert, John (2023): Risikofalle Social Media: Wie bekommen wir Algorithmen in den Griff?. AlgorithmWatch: https://algorithmwatch.org/de/risikofalle-social-media/

Bitzer, Tobias; Wiener, Martin und Cram, W. Alec (2023): Algorithmic transparency: Concepts, antecedents, and consequences–a review and research framework. In: Communications of the Association for Information Systems 52(1), S. 293–331.

Boulianne, Shelley und Hoffmann, Christian P. (2024): Digital Inclusion Through Algorithmic Knowledge: Curated Flows of Civic and Political Information on Instagram. In: Media and Communication 12, S. 8102. https://doi.org/10.17645/mac.8102.

Busuioc, Madalina; Curtin, Deirdre und Almada, Marco (2023): Reclaiming Transparency: Contesting the Logics of Secrecy within the AI Act. In: European Law Open 2(1), S. 79–105. https://doi.org/10.1017/elo.2022.47.

Chaudhary, Gyandeep (2024): Unveiling the black box: Bringing algorithmic transparency to AI. In: Masaryk University Journal of Law and Technology Masarykova univerzita nakladatelství. 18(1), S. 93–122.

Cotter, Kelley und Reisdorf, Bianca C. (2020): Algorithmic knowledge gaps: A new horizon of (digital) inequality. In: International Journal of Communication 14, S. 21.

De Bruijn, Hans; Warnier, Martijn und Janssen, Marijn (2022): The Perils and Pitfalls of Explainable AI: Strategies for Explaining Algorithmic Decision-Making. In: Government Information Quarterly 39(2), S. 101666. https://doi.org/10.1016/j.giq.2021.101666.

DeVito, Michael Ann (2021): Adaptive Folk Theorization as a Path to Algorithmic Literacy on Changing Platforms. In: Proceedings of the ACM on Human-Computer Interaction 5(CSCW2), S. 1–38. https://doi.org/10.1145/3476080.

Diakopoulos, Nicholas (2020): Accountability, transparency, and algorithms. In: The Oxford handbook of ethics of AI Oxford University Press. 17(4), S. 197.

Diakopoulos, Nicholas und Koliska, Michael (2017): Algorithmic Transparency in the News Media. In: Digital Journalism 5(7), S. 809–828. https://doi.org/10.1080/21670811.2016.1208053.

Dobber, Tom (2023): Microtargeting, Privacy, and the Need for Regulating Algorithms. In: The Routledge Handbook of Privacy and Social Media. Routledge.

Dogruel, Leyla; Masur, Philipp und Joeckel, Sven (2022): Development and Validation of an Algorithm Literacy Scale for Internet Users. In: Communication Methods and Measures 16(2), S. 115–133. https://doi.org/10.1080/19312458.2021.1968361.

Dreston, Jana H. und Neubaum, German (2023): How incidental and intentional news exposure in social media relate to political knowledge and voting intentions. In: Frontiers in Psychology 14, S. 1250051. https://doi.org/10.3389/fpsyg.2023.1250051.

Ekström, A. G.; Madison, G.; Olsson, E. J. und Tsapos, M. (2024): The Search Query Filter Bubble: Effect of User Ideology on Political Leaning of Search Results through Query Selection. In: Information, Communication & Society 27(5), S. 878–894. https://doi.org/10.1080/1369118X.2023.2230242.

Epstein, Robert und Li, Ji (2024): Can Biased Search Results Change People's Opinions about Anything at All? A Close Replication of the Search Engine Manipulation Effect (SEME). In: PLOS ONE 19(3), S. e0300727. https://doi.org/10.1371/journal.pone.0300727.

Evans, Ryan; Jackson, Daniel und Murphy, Jaron (2023): Google News and Machine Gatekeepers: Algorithmic Personalisation and News Diversity in Online News Search. In: Digital Journalism 11(9), S. 1682–1700. https://doi.org/10.1080/21670811.2022.2055596.

Finklea, Bruce W. (2017): Media Effects: Comprehensive Theories. In: The International Encyclopedia of Media Effects, Malden (MA), John Wiley & Sons https://www.researchgate.net/profile/Bruce-Finklea/publication/314404681_Media_Effects_Comprehensive_Theories/links/63043ad3aa4b1206facf0b9d/Media-Effects-Comprehensive-Theories.pdf(27.2.2025).

Fosch-Villaronga, Eduard; Poulsen, Adam; Søraa, Roger A. und Custers, Bart (2021): Gendering Algorithms in Social Media. In: ACM SIGKDD Explorations Newsletter 23(1), S. 24–31. https://doi.org/10.1145/3468507.3468512.

Gezici, Gizem; Lipani, Aldo; Saygin, Yucel und Yilmaz, Emine (2021): Evaluation Metrics for Measuring Bias in Search Engine Results. In: Information Retrieval Journal 24(2), S. 85–113. https://doi.org/10.1007/s10791-020-09386-w.

González-Bailón, Sandra; Lazer, David; Barberá, Pablo; Zhang, Meiqing; Allcott, Hunt; Brown, Taylor et al. (2023): Asymmetric Ideological Segregation in Exposure to Political News on Facebook. In: Science 381(6656), S. 392–398. https://doi.org/10.1126/science.ade7138.

Gran, Anne-Britt; Booth, Peter und Bucher, Taina (2021): To Be or Not to Be Algorithm Aware: A Question of a New Digital Divide? In: Information, Communication & Society 24(12), S. 1779–1796. https://doi.org/10.1080/1369118X.2020.1736124.

Haim, Mario; Graefe, Andreas und Brosius, Hans-Bernd (2018): Burst of the Filter Bubble?: Effects of Personalization on the Diversity of Google News. In: Digital Journalism 6(3), S. 330–343. https://doi.org/10.1080/21670811.2017.1338145.

Holmes, Wayne; Stracke, Christian M.; Chounta, Irene-Angelica; Allen, Dale; Baten, Duuk und Dimitrova, Vania u.a. (2023): AI and Education. A View Through the Lens of Human Rights, Democracy and the Rule of Law. Legal and Organizational Requirements. In: Wang, Ning; Rebolledo-Mendez, Genaro; Dimitrova, Vania; Matsuda, Noboru und Santos, Olga C. (Hrg.): Artificial Intelligence in Education. Posters and Late Breaking Results, Workshops and Tutorials, Industry and Innovation Tracks, Practitioners, Doctoral Consortium and Blue Sky, Bd. 1831. Cham: Springer Nature Switzerland. S. 79–84. (= Communications in Computer and Information Science) https://doi.org/10.1007/978-3-031-36336-8_12.

Issar, Shiv (2024): The Social Construction of Algorithms in Everyday Life: Examining TikTok Users' Understanding of the Platform's Algorithm. In: International Journal of Human–Computer Interaction 40(18), S. 5384–5398. https://doi.org/10.1080/10447318.2023.2233138.

Jürgens, Pascal und Stark, Birgit (2022): Mapping Exposure Diversity: The Divergent Effects of Algorithmic Curation on News Consumption. In: Journal of Communication 72(3), S. 322–344. https://doi.org/10.1093/joc/jqac009.

Kang, Hyunjin und Lou, Chen (2022): AI Agency vs. Human Agency: Understanding Human–AI Interactions on TikTok and Their Implications for User Engagement. In: Journal of Computer-Mediated Communication 27(5), S. zmac014. https://doi.org/10.1093/jcmc/zmac014.

Kayser-Bril, Nicolas (2021): Süddeutsche veröffentlicht Ergebnisse unseres Instagram-Forschungsprojekts zur Bundestagswahl. AlgorithmWatch. https://algorithmwatch.org/de/ergebnis-instagram-analyse-bundestagswahl/

Lee, Sangwon; Diehl, Trevor und Valenzuela, Sebastián (2022): Rethinking the virtuous circle hypothesis on social media: Subjective versus objective knowledge and political participation. In: Human Communication Research Oxford University Press. 48(1), S. 57–87.

Lin, Cong; Gao, Yuxin; Ta, Na; Li, Kaiyu und Fu, Hongyao (2023): Trapped in the Search Box: An Examination of Algorithmic Bias in Search Engine Autocomplete Predictions. In: Telematics and Informatics 85, S. 102068. https://doi.org/10.1016/j.tele.2023.102068.

Lu, Joy; Lee, Dokyun (Dk); Kim, Tae Wan und Danks, David (2019): Good Explanation for Algorithmic Transparency. In: SSRN Electronic Journal https://doi.org/10.2139/ssrn.3503603.

Luria, Michal (2023): Co-Design Perspectives on Algorithm Transparency Reporting: Guidelines and Prototypes. Präsentiert auf: FAccT '23: the 2023 ACM Conference on Fairness, Accountability, and Transparency, 2023 ACM Conference on Fairness, Accountability, and Transparency. Chicago IL USA: ACM. S. 1076–1087. https://doi.org/10.1145/3593013.3594064.

Merten, Lisa (2021): Block, Hide or Follow—Personal News Curation Practices on Social Media. In: Digital Journalism 9(8), S. 1018–1039. https://doi.org/10.1080/21670811.2020.1829978.

Nechushtai, Efrat; Zamith, Rodrigo und Lewis, Seth C. (2024): More of the Same? Homogenization in News Recommendations When Users Search on Google, YouTube, Facebook, and Twitter. In: Mass Communication and Society 27(6), S. 1309–1335. https://doi.org/10.1080/15205436.2023.2173609.

Oeldorf-Hirsch, Anne und Neubaum, German (2023): Attitudinal and Behavioral Correlates of Algorithmic Awareness among German and U.S. Social Media Users. In: Journal of Computer-Mediated Communication 28(5), S. zmad035. https://doi.org/10.1093/jcmc/zmad035.

Oeldorf-Hirsch, Anne und Neubaum, German (2025): What Do We Know about Algorithmic Literacy? The Status Quo and a Research Agenda for a Growing Field. In: New Media & Society 27(2), S. 681–701. https://doi.org/10.1177/14614448231182662.

Overdiek, Markus und Petersen, Thomas (2022): Was Deutschland über Algorithmen und Künstliche Intelligenz weiß und denkt: Ergebnisse einer repräsentativen Bevölkerungsumfrage: Update 2022. Bertelsmann Stiftung.

Rader, Emilee; Cotter, Kelley und Cho, Janghee (2018): Explanations as Mechanisms for Supporting Algorithmic Transparency. Präsentiert auf: CHI '18: CHI Conference on Human Factors in Computing Systems, Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. Montreal QC Canada: ACM. S. 1–13. https://doi.org/10.1145/3173574.3173677.

Reisdorf, Bianca und Blank, Grant (2021a): Algorithmic literacy and platform trust. In: Hargittai, Eszter (Hrg.): Handbook of Digital Inequality. Edward Elgar Publishing. https://doi.org/10.4337/9781788116572.00032.

Reisdorf, Bianca und Blank, Grant (2021b): Algorithmic literacy and platform trust. In: Hargittai, Eszter (Hrg.): Handbook of Digital Inequality. Edward Elgar Publishing. https://doi.org/10.4337/9781788116572.00032.

Rogers, Richard (2023): Algorithmic Probing: Prompting Offensive Google Results and Their Moderation. In: Big Data & Society 10(1), S. 20539517231176228. https://doi.org/10.1177/20539517231176228.

Shin, Donghee; Kee, Kerk F. und Shin, Emily Y. (2022): Algorithm Awareness: Why User Awareness Is Critical for Personal Privacy in the Adoption of Algorithmic Platforms? In: International Journal of Information Management 65, S. 102494. https://doi.org/10.1016/j.ijinfomgt.2022.102494.

Siles, Ignacio; Valerio-Alfaro, Luciana und Meléndez-Moran, Ariana (2024): Learning to like TikTok . . . and Not: Algorithm Awareness as Process. In: New Media & Society 26(10), S. 5702–5718. https://doi.org/10.1177/14614448221138973.

Silva, David E; Chen, Chan und Zhu, Ying (2022): Facets of Algorithmic Literacy: Information, Experience, and Individual Factors Predict Attitudes toward Algorithmic Systems. In: New Media & Society S. 146144482210980. https://doi.org/10.1177/14614448221098042.

Trepte, Sabine; Teutsch, Doris; Masur, Philipp K.; Eicher, Carolin; Fischer, Mona; Hennhöfer, Alisa und Lind, Fabienne (2015): Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In: Gutwirth, Serge/Leenes, Ronald/De Hert, Paul (Hrg.): Reforming European Data Protection Law, Bd. 20. Dordrecht: Springer Netherlands. S. 333–365. (= Law, Governance and Technology Series) https://doi.org/10.1007/978-94-017-9385-8_14.

Tzimas, Themistoklis (2023): Algorithmic Transparency and Explainability under EU Law. In: European Public Law 29(Issue 4), S. 385–411. https://doi.org/10.54648/EURO2023021.

Van De Pol, Janneke; Volman, Monique und Beishuizen, Jos (2010): Scaffolding in Teacher–Student Interaction: A Decade of Research. In: Educational Psychology Review 22(3), S. 271–296. https://doi.org/10.1007/s10648-010-9127-6.

Van Den Bogaert, Lawrence; Geerts, David und Harambam, Jaron (2024): Putting a Human Face on the Algorithm: Co-Designing Recommender Personae to Democratize News Recommender Systems. In: Digital Journalism 12(8), S. 1097–1117. https://doi.org/10.1080/21670811.2022.2097101.

Van Hoof, Marieke; Trilling, Damian; Moeller, Judith und Meppelink, Corine S (2024): It Matters How You Google It? Using Agent-Based Testing to Assess the Impact of User Choices in Search Queries and Algorithmic Personalization on Political Google Search Results. In: Journal of Computer-Mediated Communication 29(6), S. zmae020. https://doi.org/10.1093/jcmc/zmae020.

Zarouali, Brahim; Boerman, Sophie C. und de Vreese, Claes H. (2021a): Is This Recommended by an Algorithm? The Development and Validation of the Algorithmic Media Content Awareness Scale (AMCA-Scale). In: Telematics and Informatics 62, S. 101607. https://doi.org/10.1016/j.tele.2021.101607.

Zarouali, Brahim; Helberger, Natali und de Vreese, Claes H. (2021b): Investigating Algorithmic Misconceptions in a Media Context: Source of a New Digital Divide? In: Media and Communication 9(4), S. 134–144. https://doi.org/10.17645/mac.v9i4.4090.

Zou, James und Schiebinger, Londa (2018): AI can be sexist and racist—it's time to make it fair. Nature Publishing Group UK London. https://idp.nature.com/authorize/casa?redirect_uri=https://www.nature.com/articles/d41586-018-05707-8&casa_token=LdAzgZnRFAsAAAAA:tFTFQmihVu_GnB7boCCaREYslkk7YhZYzXVaOnT6dFlWEtD9iHgQRJFwA344emsUWgUbOkGvndglaolMyQ(27.2.2025).

Das *Privacy Fabric Model*: Ein Vorschlag für interdisziplinäre Verständigung in der Privatheitsforschung

Johanna Möller, Lukas Schmitz und Sebastian Rehms[1]

Zusammenfassung
Dieser Beitrag bietet eine Orientierungsmöglichkeit für interdisziplinäre Verständigung und reflexive Positionierung im Feld der Privatheitsforschung. Privatheit wird in der Forschungspraxis nicht nur entlang so unterschiedlicher Begriffe wie *Privacy* oder Datenschutz gefasst, sondern auch mit Blick auf divergierende Erkenntnisinteressen diskutiert, etwa bezogen auf Selbstbestimmung oder die Transparenz digitaler Infrastrukturen. Forschende adressieren darüber hinaus eine Vielfalt teils widersprüchlicher normativer Ansprüche, wie Kontrolle, Sozialität und Kritik. Diese ambivalente Komplexität macht Privatheit im Kern aus. In der interdisziplinären Forschungspraxis wird gerade diese aber oft zu einem Stolperstein. So kann die Verständigung über den Forschungsgegenstand oder über die Komplementarität der Zugänge leicht misslingen. Mit dem *Privacy Fabric Model* adressieren wir diesen Bedarf und entwickeln eine strukturierte Gesprächsgrundlage, die paradigmatische wie forschungspraktische Unterschiede sichtbar macht. Divergierende Perspektiven können so gesichtet und spezifische wissenschaftliche Positionen verortet und abgegrenzt werden. Verankert in einer praxistheoretischen Betrachtung von Wissen(-schaft) bringt das Modell computer- und sozialwissenschaftliche Zugänge zu Privatheit zusammen.

1. Privatheit als Problematisierungsbegriff und interdisziplinäres Forschungsfeld

Ausgangspunkt für diesen Beitrag ist ein interdisziplinärer Streit über Privatheit – letztlich ein produktiver und einsichtsreicher Streit. Mit dem Ziel, eine Arbeitsgrundlage für disziplinenübergreifende Privatheitsforschung zu schaffen, diskutierten wir nachdrücklich über vermeintliche Selbstverständlichkeiten im theoretischen und forschungspraktischen Umgang mit Privatheit. Gegenstände intensiver und kritischer Diskussionen waren beispielsweise die genauere Verortung von Selbstbestimmung im Kontext von Privatheit, die Rolle, die das Teilen im Gegensatz zum Sichern von Daten für Privatheit spielt, Zusammenhänge zwischen Transparenz und Mobilität oder implizite Annahmen über die kognitiv-reflexiven Fähigkei-

1 Gemeinsamer Kontext ist das Forschungsprojekt „Disruptionen vernetzter Privatheit" (DIPCY), das von 2022 bis 2025 im Rahmen der Exzellenzinitiative TUDiSC an der Technischen Universität Dresden gefördert wird. Beteiligt sind Wissenschaftler:innen aus den Disziplinen Kommunikations- und Medienwissenschaften, Soziologie und Computerwissenschaften.

ten von Privatheitsakteuren. Streit kann destruktiv, aber auch im Sinne einer gedanklichen Öffnung produktiv wirken. Im Idealfall führt er zu einem Perspektivwechsel aller Beteiligten.

Ein solcher Perspektivwechsel ist Motivation für das *Privacy Fabric Model* (im Folgenden auch PFM), das Gegenstand dieses Beitrags ist. Zu Beginn erschwerte die interdisziplinäre Zusammensetzung unseres Projekts die gemeinsame Arbeit. Zu unterschiedlich waren die Begriffe, Methoden, Fragestellungen und Erkenntnisinteressen in Bezug auf Privatheit. Eine geteilte Definition von Privatheit, unter vielen Kompromissen zustande gebracht, schien kein gangbarer Weg zu sein. Ebenso wollten wir ein überfrachtetes Untersuchungsdesign vermeiden. So schälte sich über anhaltende Gespräche der Bedarf heraus, eine interdisziplinäre *Arbeitssprache* zum Gegenstand Privatheit zu finden. Damit erkannten wir grundsätzlich an, dass das Konzept Privatheit ausgehend von sehr unterschiedlichen Erkenntnisinteressen untersucht und diese Untersuchung auch von variierenden normativen Annahmen geleitet werden kann und soll.

Diesen Gedanken folgend rücken Fragen nach dem Charakter des Konzepts Privatheit in den Fokus. Ganz grundsätzlich ist seine Aufgabe zu problematisieren, also Schieflagen zu adressieren. Problematisierungen haben das Potenzial, Momente der Indikation (was ist hier relevant?) oder Irritation (was ist hier los?) zu erzeugen. Folgen können Reflexionen, Auseinandersetzungen und Lösungsbemühungen sein (Grebe, 2019: 28f). Konkret kann das vor einem theoretischen oder normativen Hintergrund passieren, wie bspw. durch das Aufdecken von Datensammelpraktiken einer Plattform oder die kritische Auseinandersetzung mit Privatheit als Individualverantwortung aus (kapitalismus-)kritischer Perspektive (Fuchs, 2012; Helm & Seubert, 2020). Genauso können Privatheitsforschende Problematisierungen aber auch aus Perspektive alltagspraktischer Privatheit erfassen. So sorgt die Nutzung datenschutzunfreundlicher Plattformen für das Teilen privater Informationen im Freundeskreis häufig kaum für Bedenken. Problematisiert würde dieselbe Praxis dagegen möglicherweise aber, wenn der Hausarzt denselben Weg nutzte. Das Feld der Privatheitsforschung adressiert Erkenntnisinteressen ausgehend von solchen vielfältigen, disziplinären, theoretischen oder praxisbezogenen spezifisch wahrgenommenen Störmomenten.

Betrachtet man Privatheit als ein solches Forschungsfeld, zeigt sich sein interdisziplinärer Charakter – das gilt umso mehr in der datafizierten Gesellschaft (dazu ausführlicher Gstrein & Beaulieu, 2022). Privatheit bezieht eine enorme Vielzahl komplexer sozio-technischer Interaktionen

als Untersuchungsgegenstand ein. Das Konzept findet in den verschiedensten Bereichen des Alltags implizit wie explizit Anwendung und berührt damit eine Vielzahl an Disziplinen. Ob in der analogen Welt beim Arztbesuch oder im virtuellen Raum beim Anklicken der Cookie–Banner – Privatheit wird in vielfältigen sozialen Kontexten ausgehandelt und durch die Digitalisierung verzahnen sich diese zunehmend. Entsprechend sind an der Erforschung von Privatheit viele zu beteiligen. Darunter finden sich beispielsweise die Erziehungswissenschaften (Privatheit lernen), Computerwissenschaften (Infrastrukturen gestalten, analysieren), Rechtswissenschaften (gesetzliche Regelungen sowie Rechtspraxis) oder verschiedene Sozialwissenschaften (sozio-technische Alltagspraxis, Sozialisationsprozesse).

Wie aber ist es möglich, all diese und weitere zentrale Disziplinen, die je unterschiedliche Begriffe und Konzepte benutzen, in einen Dialog zu bringen? Im Forschungsfeld Privatheit wurden und werden immer wieder Versuche unternommen, diese anerkannte konzeptionelle Interdisziplinarität in einen wissenschaftspraxistauglichen Zugang zu Privatheit zu überführen. Diese sind dabei jedoch entweder zu allgemein oder sie kumulieren eine Vielzahl von Variablen, die eine unübersichtliche Komplexität aufbauen. Mit stark abstrahierten Privatheitskonzepten arbeiten beispielsweise ebenso einflussreiche wie unterschiedliche Autor:innen wie Solove (2009), Zuboff (2020) oder Nissenbaum (2004). Letztere etwa definiert Privatheit über den normativen Referenzrahmen, der in geschlossenen Gruppendynamiken entsteht, ein wegweisender Ansatz. Wenngleich interdisziplinär inspiriert, bleibt er jedoch nicht nur sehr allgemein, sondern vor allem der geistes- bzw. rechtswissenschaftlichen Tradition verhaftet, die ohne Zweifel das Feld stark bedient (siehe dazu Smith et al., 2011: 993). In einem interdisziplinären Überblick über mehr als 400 internationale Publikationen zum Thema Privatheit wählen Smith, Dinev und Xu (2011) einen anderen Weg. Ihr Ziel ist über vergleichbare Variablen die akteurszentrierte Untersuchung von Privatheit in einen vielschichtigen Ansatz von Informationsprivatheit zu kondensieren, das so genannte Antecedents-Privacy-Concerns-Outcomes-Modell (Smith et al., 2011), welches eine Vielzahl von Variablen verknüpft. In einem jüngeren Ansatz steigern Bräunlich et al. (2021) diese Komplexität noch weiter, indem sie weitere Variablen und Kontexte für das interdisziplinäre Messen akteurszentrierter Privatheit im digitalen Zeitalter anbieten.

Wie aber das Thema Privatheit einerseits prägnant und andererseits forschungspraktisch interdisziplinär erschlossen werden kann, bleibt in der

Regel unbeleuchtet. Wenn Privatheitsforschung sich interdisziplinär aufstellen will – in dem Sinne, dass gemeinsam problematisiert wird und nicht nur nebeneinander – ist eine Kenntnis der Begriffe, der Anforderungen und Zwänge der anderen Disziplinen unabdingbar, um eine gemeinsame Sprache zu finden. An dieser Stelle bieten wir das *Privacy Fabric Model* als Arbeits- und Gesprächsgrundlage an, das in einfacher Art und Weise den interdisziplinären Dialog zu Privatheit unterstützen und zur Verortung einzelner Ansätze beitragen kann. Nachfolgend machen wir einige knappe methodische Anmerkungen (2), um dann drei normative Ansprüche vorzustellen, die quer über die Disziplinen hinweg adressiert werden (3). Danach werden drei Kategoriengruppen vorgestellt, die maßgeblich für die Wissenschaftspraxis sind (4). Diese beiden Kapitel leuchten abrissartig die Bandbreite des Privatheitsbegriffs aus. Dabei geht es weniger um konkrete disziplinäre Definitionen von Privatheit, sondern vielmehr um eine Darstellung der Vielschichtigkeit des Forschungsfeldes. Ansprüche und forschungspraktische Perspektiven werden dann im PFM zusammengeführt (5), bevor der Beitrag mit einer Schlussdiskussion endet (6).

2. Methodische Anmerkungen

Das PFM ist in einem mehrstufigen, etwa zwei Jahre dauernden Prozess entstanden. Methodisch orientierte sich das Vorgehen in groben Zügen an der Gruppendelphi-Methode (Niederberger & Renn, 2018), einer dialogischen Variante des klassischen Delphi-Verfahrens. Ziel der Methode ist es, durch problemzentrierte Austauschprozesse zwischen Expert:innen Konsensräume zu identifizieren, Perspektiven zu ordnen und gemeinsame Begriffe, Szenarios oder Strategien zu entwickeln.

Im Unterschied zum klassischen Delphi mit anonymisierten Einzelbefragungen setzt das Gruppendelphi auf *face to face*-Formate, in denen sich Teilnehmende gegenseitig mit ihren jeweils unterschiedlichen Sichtweisen konfrontieren. In unserem Falle fanden regelmäßig Diskussionstreffen innerhalb der Projektteams statt, während derer zentrale Begriffe und Konzepte der einzelnen Disziplinen vorgestellt und diskutiert sowie anschließend mit bestehenden Begriffen und Konzepten anderer Disziplinen kontrastiert wurden (Niederberger & Renn, 2018: 28). Interdisziplinarität wird im Gruppendelphi nicht als Problem betrachtet, etwa als eine methodische oder vokabularische Hürde, sondern als produktive Reibungsfläche und Treiber dialogischer Verständigung. Der Prozess lebt von einer grundsätz-

lichen Ergebnisorientierung der Teilnehmenden bei gleichzeitiger Prozesstoleranz. Sie profitiert von punktuellen Rückmeldungen durch interne und externe Expertise, aber auch von der Übersetzung dieses Gesprächs in Vorträge oder Publikationen, inklusive der damit verbunden Rückmeldungen über Diskussionen oder Reviews (Möller, 2024, 2025; Rehms & Köpsell, 2024; Schmitz, 2024).

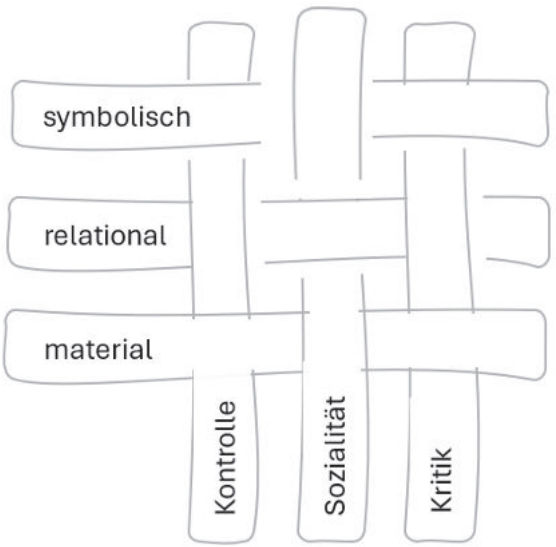

Abbildung 1: Das Privacy Fabric Model (PFM).

Die selbst gestellte Aufgabe bestand im inhaltlichen Arbeiten an einem disziplinübergreifenden Verständnis von Privatheit. Wie das heterogene Feld unterschiedlicher Begriffe und disziplinärer Erkenntnisinteressen dabei zunächst einen produktiven Dialog verunmöglichte, zeigt sich am Beispiel der Idee der Selbstbestimmung. Diese spielt in der kommunikations- und medienwissenschaftlichen Perspektive eine wichtige Rolle, wird aber in der Soziologie nicht selten als irreführend betrachtet. In iterativen Gesprächsrunden und unter Einbezug von Forschungsliteratur identifizierten und benannten wir zunächst die unterschiedlichen Denkgebäude der jeweiligen Disziplinen. Der entscheidende Wendepunkt im Prozess lag dann in einem weiteren Schritt in der Erkenntnis, dass es darum geht, eine gemeinsame Sprache zu finden, die diese Unterschiede operationalisieren kann. Basis dafür war ein praxeologisches Verständnis, das davon ausgeht, dass auch

Wissenschaft als Praxis betrachtet werden kann, in der entlang spezifischer Denkroutinen neue Erkenntnisse gewonnen werden.

Auf dieser Basis konnten wir sukzessive ein Modell entwickeln, das im Dialog und unter Einbezug von Forschungsliteratur emergierte Dimensionen eines Privatheitsbegriffs verzahnt. Gerade die Auseinandersetzung mit divergierenden normativen Setzungen und ihrer jeweiligen Gewichtung erwies sich als hilfreich für die zunehmende Reduktion des Modells auf jeweils drei normative und forschungspraktische Kategoriengruppen (siehe Abb. 1). Schlusspunkt dieses Prozesses war seine Sättigung. Diese war erreicht als keine neuen Aspekte in die Diskussion kamen. In einer letzten Runde prüften wir diese mit deutlichem zeitlichem Abstand noch einmal kritisch anhand einzelner Forschungsfragen durch Studien ab. Bei bewusster Ausklammerung weiterer Disziplinen kamen hier keine neuen Kategorien auf. Die Delphi-typische Differenz zwischen Ist- und Soll-Zustand wurde so in Bezug auf theoretisch-methodische Verständigungsprozesse fruchtbar gemacht.

3. Privatheitsansprüche

Innerhalb von Disziplinen und über sie hinweg finden sich ebenso unterschiedliche wie ähnliche Ansätze der Annäherung an das Problem Privatheit, die sich an normativen Referenzen festmachen lassen. Normativ meint hier, dass mit dem Begriff der Privatheit aus Sicht der jeweiligen Perspektiven Ansprüche und Aufforderungen verknüpft werden, die sich aus dem spezifischen Erkenntnisinteresse ergeben. Dabei sind auch die Disziplinen nicht als homogen zu verstehen. So verorten einige Sozialwissenschaftler:innen den Anspruch der Sozialität nur teilweise auf normativer Ebene. Insbesondere in akteurszentrierten Zugängen zu Privatheit wird Sozialität häufig eher als Problem wahrgenommen, etwa wenn das Nutzungsverhalten anderer Privatheit (meint in diesem Fall Datensicherheit) stört. Andere sozialwissenschaftliche Perspektiven dagegen betrachten Sozialität sehr häufig als ein Grundcharakteristikum von Privatheit. Damit sind ähnliche Referenzen vorhanden, nicht immer haben sie aber einen normativen Charakter oder werden gleich gewichtet.

Nachfolgend diskutieren wir im Einzelnen die drei Ansprüche Kontrolle, Sozialität und Kritik und skizzieren beispielhaft, wie sich diese normativen Prämissen in den jeweiligen Disziplinen wiederfinden. Diese drei normati-

ven Kategoriengruppen finden sich unten in Abbildung 1 in vertikaler Ausrichtung wieder.

In der Kategoriengruppe der Kontrolle versammeln sich Ansprüche, Privatheitsgegenstände regelgebunden zu ordnen. In sehr allgemeiner Form verstehen wir damit unter Kontrolle den intendierten Umgang mit privatheitsbezogenen Informationen. Kontrolle kann sich dabei auf sehr unterschiedliche Normen beziehen, wie Trepte (2022) in ihrer vielschichtigen Diskussion von Privatheitstheorien deutlich macht. Trepte nennt eine erste Gruppe von Ansätzen, die Privatheit mit Kontrolle gleichsetzen (Privatheit *als* Kontrolle). Anonymität etwa oder Reflexions- und Technikwissen werden als geeignete individuelle Kontrollmechanismen betrachtet. In der Informatik lassen sich privatheitsbezogene Kontrollansprüche anhand von Gewährleistungszielen am deutlichsten machen (Rost, 2024; mit Fokus auf Anonymität Kuhn, 2019). Diese bilden etablierte Kategorien, anhand derer Schutzbedarfe ausgearbeitet werden können. Sie beziehen sich etwa auf konkrete Daten bzw. Informationen, mitunter aber auch auf technische Systeme oder Prozesse als Ganzes. Ziele wie Verfügbarkeit, Integrität, Intervenierbarkeit oder Transparenz stellen ein technisches Funktionieren oder Operieren sicher.[2] Ziele wie Vertraulichkeit, Nichtverkettung und Datenminimierung eint die Begrenzung von Information in einem System. Technische Privatheit ist hier daran interessiert, Informationen im System zu reduzieren bzw. begrenzbar zu machen und in diesem Sinne durch Wegnahme von Information möglichem Kontrollverlust vorzubeugen.

Davon unterscheidet Trepte solche Ansätze, die Kontrolle als *einen* Bestandteil von Privatheit sehen (Privatheit *und* Kontrolle). Ansätze dieser Gruppe folgen Tavani und Moor (2001: 6), die sagen: „We can have control but no privacy, and privacy but no control" (mit einem ähnlichen Argument zur Trennung von Privatheit und Sicherheit Dourish & Anderson, 2006). Tendenziell eher in den Sozialwissenschaften diskutiert, wird Kontrolle hier aus der Rolle als Garant von Privatheit gelöst. Es handelt sich nur noch um ein Mittel unter Vielen, um Sicherheit herzustellen. Anders als etwa im Fall von technischer Kontrolle durch Wegnahme von Informationen findet sich hier ein offeneres Verständnis von Kontrolle, wie bspw. Delegation von privatheitsbezogenen Aufgaben über Vertrauen in ein

2 Zu dieser Deutung von Intervenierbarkeit und Transparenz: hier geht es um die Möglichkeit, dass Akteure (oft Datensubjekte) in der Verarbeitung intervenieren können und damit eine *individuelle* Form von Kontrolle ausüben können bzw. der Verarbeitungsprozess sichtbar und damit überprüfbar wird.

Netzwerk. An anderer Stelle finden sich Diskussionen, die als Kontextkompetenz verstanden werden können. Je nach den Anforderungen in einer gegebenen Situation entscheiden Akteure über das *Wie* ihrer Teilnahme (Dienlin, 2014). Trepte (2021: 12) macht den Punkt, dass durch das Ausüben von Kontrolle allein Privatheit nicht hergestellt werden kann.

Als zweite normative Kategoriengruppe der Privatheitsforschung sehen wir Sozialität. Neben Erfordernissen der Kontrolle wird Privatheit als Moment des Herstellens von Teilhabe oder Gemeinschaft bearbeitet. Im Unterschied zum mittlerweile überholten *Privacy Paradoxon*, das Sozialität als Irritationsmoment von Privatheit versteht (kritisch dazu Dienlin & Trepte, 2015), ist dieser Anspruch in der Privatheitsforschung zunehmend präsent.

In der Informatik etwa streben Forschende häufig technische Lösungen für die Ermöglichung von Sozialität unter gleichzeitig informationsreduzierten (und damit kontrollierten) Bedingungen an. Beispiele hierfür sind anonyme Kommunikationstechnologien und *Privacy*-Mechanismen auf Datenebene. Erstere meinen bspw. Anonymisierungsdienste zur Internetnutzung (Dingledine, 2004) oder alternative *Web Front Ends*. Als Beispiel für zweiteres garantiert *Differential Privacy* (Dwork, 2011) auf Datenebene einen nach oben beschränkten Informationsgewinn gegen Datensubjekte in einer Datenmenge, wenn die Daten (beschränkt) geteilt werden. In der Informatik wird Sozialität aber auch problematisiert. So ist etwa das Nachweisen möglicher privatheitsrelevanter Inferenz auf bis dato unproblematisierten Daten ein oft aufgebrachtes Thema. Teilweise passiert dies durch die Hinzunahme von plausiblem Hintergrundwissen (z. B. Torra, 2012 für die Datenebene; öffentlichkeitswirksam zuletzt durch den Chaos Computer Club für Mobilitätsdaten eines deutschen Autoherstellers, Beuth, 2025).

In den Sozialwissenschaften haben Autorinnen wie Nissenbaum (2004) in der stärker theoretischen Arbeit, aber wegweisend auch Marwick und boyd (2014) darauf aufmerksam gemacht, dass Privatheit Sozialität ermöglicht und umgekehrt durch Sozialität Bedeutung erlangt. In einer wichtigen Studie zu Privatheit unter Teenagern zeigten die Autorinnen, dass Privatheit eine soziale Ressource sein kann. Freundinnen machen in den sozialen Medien sichtbar, dass Sie jetzt in einen separaten Chatraum gehen, in dem sie privatere Themen unter sich besprechen. Oder Jugendliche führen eine öffentliche Diskussion, aber unter Verwendung einer „Räubersprache". In den Sozialwissenschaften werden daneben auch politische Aspekte von Privatheit diskutiert. Privatheit muss geschützt und bewahrt werden, bietet Schutz vor staatlichem und sonstigem Übergriff. Gleichzeitig wird im

Schutz der Privatheit das Gelingen der freiheitlich-demokratischen Grundordnung sichergestellt, sie ermöglicht Teilhabe.

Kritik, und damit die letzte der drei Kategoriengruppen, bezieht sich auf die Kontingenz von Privatheitsbezügen. Kontingenz meint, dass Privatheit so oder anders, im Zweifel aber auch nicht gestaltet werden kann. Es wird der Anspruch formuliert, dass etablierte Arrangements in Frage gestellt und Alternativen eruiert werden können. Aus dem Unhinterfragbaren wird potenziell etwas Hinterfragbares. Das kann sich beispielsweise auf Privatheitsnarrative beziehen. Forschende setzen sich kritisch mit der Frage auseinander, ob und wie Überwachungskapitalismus normalisiert oder problematisiert wird (Wahl-Jorgensen et al., 2017), ein Thema, das auch in der weiteren Tradition der Kritischen Theorie und der Surveillance Studies intensiv diskutiert wird (etwa bei Lyon, 2014 oder Zuboff, 2020). Genauso ist das Design technischer Artefakte kontingent. So untersuchen Greene und Shilton (2018) vergleichend das Design von Privatheit durch Apple- oder Microsoft-Entwickler:innen und finden hier erhebliche Unterschiede. Damit brechen die Autoren Vorstellungen von der Unveränderlichkeit von Technologien auf und verweisen auf die potenzielle Vielfalt von Gestaltungsmöglichkeiten. In der Informatik sind Ermöglichungstechnologien, die ein kritisches Hinterfragen anbieten, Gegenstand der Forschung. So werden Lösungen entwickelt, die etablierte Funktionalitäten unter gleichzeitiger Wahrung von Privatheitsansprüchen bereitstellen. Hier steht die implizite Nachfrage nach Lösungen im Raum, die einerseits Sozialität bei gleichzeitiger Kontrolle etablieren und damit potenziell auch Etabliertes aufbrechen.

Es sind damit insgesamt drei übergeordnete Privatheitsansprüche, die wir über den Prozess des Gruppendelphi identifiziert und in vielen Runden iterativ überprüft haben. Kontrolle, Sozialität und Kritik sind wesentliche normative Prüfkriterien, denen sich Privatheitsforschung in ihrer gesamten Bandbreite widmet.

3. Forschungspraxis Privatheit

Hinter den disziplinär unterschiedlichen Zugängen zu Privatheit verbergen sich mehr als variierende normative Grundordnungen. Forschung unterscheidet sich auch darin, wie über Privatheit gesprochen wird und wie sie konkret beforscht wird. Für ein Modell, das es ermöglichen soll, sich in diesem komplexen Forschungsfeld zu verorten, ist damit nicht nur nach

den normativen Ansprüchen zu fragen, sondern auch danach, auf welcher Ebene Privatheitsforschung ansetzt, wenn es darum geht, Privatheit als Tätigkeit zu erfassen. Dabei folgen wir dem theoretischen Programm der Praxistheorien als analytischer Brille. Dabei handelt es sich um eine theoretische Perspektive aus den Sozialwissenschaften, die soziales Handeln über sich wiederholende und kollektiv geteilte Praktiken im Sinne von „ways of doing and saying" (Schatzki 2002: 87) in den Blick nimmt. Diese „doings and sayings" sind hier die grundlegende Analyseeinheit (Reckwitz, 2002: 212). Ein besonderes Augenmerk liegt auf der Rolle von Materialität, was auch technische Artefakt umfasst. Soziales Handeln entsteht, auch in der Herstellung symbolischer und relationaler Bedeutung, immer aber in der Auseinandersetzung mit den materiellen Gegebenheiten. Wissenschaft – und damit auch die Privatheitsforschung – ist also als Praxis der Erkenntnisproduktion zu verstehen (Hillebrandt, 2009: 15).

Als praxistheoretische Dimensionen unterscheiden wir im Anschluss an Welch (2016) und Mattoni (2020) eine Inhalts-, Netzwerk- und Materialitätsebene, in Abb. 1 horizontal ausgerichtet. Praktiken, hier Forschungspraktiken, können dabei entlang der Frage unterschieden werden, mit welchen Bedeutungen und sozialem Sinn (bspw. aktuelle Wissenschaftsthemen) sie umgehen, in welche Beziehungsgeflechte sie eingefügt sind (bspw. Forschungsgruppen) und welche Rolle der Materialität dabei zukommt (bspw. Vertriebswege für wissenschaftliche Fachzeitschriften). Kurz, die Forschungspraxis im Feld der Privatheit äußert sich in verschiedenen Bedeutungszuschreibungen zu Privatheit, in ihrer praktischen Einbettung in Netzwerke, die Privatheit erst tragen und in ihrer Auseinandersetzung mit Materialitäten von Privatheit.

Das lässt sich einfach am Beispiel der Erforschung von Privatheit in einer Freundschaft beschreiben. Privatheit kann hier in symbolischer Hinsicht einerseits bedeuten, Informationen weiterzugeben oder eben nicht, nach innen wie nach außen. Privatheit kann hier „Loyalität" der Geheimnisträger bedeuten – oder das wechselseitige Verfügen über Informationen kann als „Abhängigkeitsverhältnis" beschrieben werden. Auf der relationalen Ebene gilt darüber hinaus eine Vielzahl von Regeln, die bestimmen, in welchen Situationen und mit wem Informationen geteilt werden dürfen und in welchen möglicherweise erst eine Erlaubnis eingeholt werden muss. Auch eine codierte Sprache, über die intuitiv Erinnerungen abgerufen werden, kann dazugehören. Auf der materialen Ebene schließlich können etwa gemeinsame Erinnerungsstücke, Fotos oder bestimmte Gegenstände eine Rolle spielen.

Damit verstehen wir die Erforschung von Privatheit als Wissenschaftsfeld, in dem Forschende mit ihren Vorhaben auf diesen (mindestens drei) unterschiedlichen Ebenen ansetzen können. Ganz explizit geht es uns hier nicht um eine praxeologische Theorie von Privatheit (dazu an anderer Stelle Möller, 2024), sondern um eine praxistheoretische Erfassung des interdisziplinären Feldes der Privatheitsforschung. Und hier zeigt sich, dass Wissenschaftler:innen vor dem Hintergrund unterschiedlicher Theorieschulen und unter dem Einfluss unterschiedlicher Wissenschaftskulturen variierende forschungspraktische Akzente setzen. Sie bedienen sich lokal oder transkulturell unterschiedlicher Netzwerke mit Wissenschaft und Praxis und produzieren Texte, Materialien oder Programme (Reckwitz, 2003: 284f.). Führt man sich darüber hinaus die Komplexitätssteigerung von Privatheits-bezogenen Praktiken in der datafizierten Gesellschaft vor Augen (Gstrein & Beaulieu, 2022), so potenziert sich diese Vielfalt weiter.

In der Forschungspraxis werden zunächst einmal, erstens, symbolische Bezüge hergestellt. Wissenschaftler:innen stellen bspw. Fragen zum Charakter bestimmter Informationen und menschlichen Abwägungen bezüglich dieser Informationen, um den symbolischen oder sinnhaften Geltungsbereich von Privatheit zu bestimmen. Welche Informationen sind sensibel, welche haben einen stärker öffentlichen Charakter? Als Beispiele hierfür kann Forschung zu Privatheits-Risiken, etwa in e-Pässen (Juels et al, 2005), für prekär Beschäftigte (Bernd et al., 2020) oder auch die oben erwähnten Mobilitätsdaten von Autos (Beuth, 2025) genannt werden. In der akteurszentrierten Privatheitsforschung adressieren Forschende ähnliche Fragen aus Sicht bspw. von Mediennutzenden oder Konsument:innen. Mit stärker soziologischem Einschlag fragen Wissenschaftler:innen nach der narrativen Konstruktion von Privatheit bspw. entlang kollektiv funktionsfähiger Narrative wie bspw. Technopanik (die diffuse Sorge vor dem destruktiven Einfluss von Technologie, vgl. Marwick, 2008) oder Privacy-Zynismus (eine ironisch-sarkastische Bewältigungsstrategie, die sich auf die Unmöglichkeit von Privatheit als Praxis bezieht, vgl. Hoffmann et al., 2016). Insgesamt geht es damit in der symbolischen Dimension um die Bestimmung der Gegenstände, die in einer jeweiligen Situation relevant sind.

Relationale Aspekte, zweitens, beziehen sich auf soziale Beziehungen, die Privatheit herstellen. Hier setzen Forschende an, um zu klären, welche Netzwerke, Gruppen und sozialen Beziehungen auf welche Weise den Geltungsbereich von Privatheit bestimmen. In der informatischen Privatheitsforschung ist etwa der anonymitäts*mengen*bezogene Ansatz etabliert

(Serjantov, 2002): Hier wird die Identifizierbarkeit eines:r konkreten Teilnehmer:in in Relation zu allen anderen Beteiligten gesetzt. Indem die Identifikation einer Einzelperson auf eine Grundmenge bezogen wird, die alle möglichen Kandidaten stellt, hat sich hier eine wahrscheinlichkeitstheoretisch fundierte Metrik etabliert. Im Extrembeispiel lässt sich eine einzelne Person trivialerweise identifizieren, wenn sie aus einer Kandidatenmenge der Größe eins stammt. Privatheit wird hier also in Relation zu einer Gruppe konzipiert. Außerhalb der Informatik stehen häufig interpersonale Beziehungen im Fokus, wie im Ansatz von Crowley (2017), der Informationskontrolle über interpersonale Beziehungen in den Blick nimmt oder, mit stärker soziologischem Einschlag, der Umgang mit Privatheit unter jugendlichen Peers (Marwick & boyd, 2014). Ein anderer Forschungsbereich betrifft den großen Bereich der Bildung im Kontext von Fragen der Privatheit. Zunehmend richten Forschende ihr Augenmerk auf die Bedeutung von Interaktion (Raynes-Goldie & Allen, 2014; Roessler & Mokrosinska, 2013) und von sozialen, bspw. schulischen oder familiären Beziehungen (De Leyn et al., 2022; Kumar et al., 2020) in der Ausbildung von Privatheits-bezogenen Kompetenzen und Werten. An diesen knappen Einblicken wird deutlich, dass Relationalität in der Breite nicht nur mit Blick auf Datensicherheit, sondern explizit und zunehmend (dazu bspw. Möller, 2025) im Hinblick auf Momente des Teilhabens erforscht wird.

Die materiale Dimension schließlich umfasst Forschung, die Fragen der Privatheit im Geltungsbereich von Objekten oder Artefakten umfasst. Das bezieht sich etwa auf räumliche Privatheit, wie sie Türen oder Gebäude herstellen. Dabei ist diese auch kulturell geprägt. Stanner & Martin (2001) zeigen am Beispiel der Umsiedlung von indigenen Australier:innen in feste Behausungen, dass geschlossene Türen im klaren Widerspruch zur Privatheitspraxis der Aborigines stehen. Genauso werden hier aber auch Fragen zum Design von Technologien und deren Implikation für Privatheitspraktiken untersucht (bspw. Greene & Shilton, 2018). Praktisch implizieren etwa auch die technischen Grundlagen des Internets standardmäßig die Preisgabe von personenbezogenen Daten an Akteure (etwa auf Infrastrukturebene) oder auch die Preisgabe von Verkehrs- oder Metadaten.

Das Forschungsfeld insgesamt lässt sich mit Blick auf diese Dimensionen teilweise, aber nicht konsequent, entlang der Disziplinen ordnen. Sowohl narrative als auch materiale Bezüge spielen eine große Rolle in den Kommunikations- und Medienwissenschaften, dort wo Inhalte oder Besonderheiten von Plattformen eine Rolle spielen. Aber auch relationale Zugänge treten zunehmend in den Vordergrund, wie sich an interdisziplin-

nären Diskussionsansätzen zeigt (Bräunlich et al., 2021; Trepte, 2021). In den Computerwissenschaften spielen materiale und narrative Aspekte eine wichtige Rolle, bspw. mit Fokus auf der Risikoqualität von Informationen oder dem Design von Technologien. Diese Zuordnung stimmt aber nur teilweise. Im interdisziplinären Feld der Privatheitsforschung engagieren sich bspw. Autor:innen aus Bereichen wie den Science and Technology Studies, die alle drei Dimensionen bedienen (bspw. Gstrein & Beaulieu, 2020). Aber auch die Unterscheidung der drei Dimensionen ist nicht ganz trennscharf. So können beispielsweise Artefakte auch Affordanzen für bestimmte Inhalte bieten. Es handelt sich also um eine analytische Unterscheidung.

4. Das Privacy Fabric Model

Beide Kategoriengruppen, normative Ansprüche wie forschungspraktische Zugänge zu Privatheit, verweben wir im *Privacy Fabric Model*. Der Begriff „Fabric", aus dem Englischen übernommen im Sinne von „Gewebe", veranschaulicht hier die grundlegende Funktion des Modells, nämlich diese beiden Kategoriengruppen als zwar in einem Spannungsverhältnis, aber einander ergänzend und gewissermaßen verwoben zu denken. Aus den Disziplinen der Soziologie, Kommunikations- und Medien- sowie Computerwissenschaften heraus, und damit aus einer interdisziplinär noch limitierten Perspektive, unternehmen wir damit den Versuch, diese Unterschiedlichkeit als das zentrale Charakteristikum dieses komplexen Forschungsfeldes greifbar zu machen. Das Modell kann damit zwei Funktionen erfüllen. Vor dem Hintergrund der Herausforderung, die Interdisziplinarität darstellt, bieten wir es als einen unterstützenden Orientierungsrahmen für wissenschaftsbezogene Diskussionen über Privatheit an. Darüber hinaus unterstützt es dabei, die Schwerpunkte der eigenen Disziplin zu eruieren und sich im Verhältnis zu anderen Zugängen im Kontext der Privatheitsforschung verorten und/oder abgrenzen zu können.

Das Modell adressiert das Feld der Bedeutungsproduktion im Kontext von Privatheitsforschung und verwebt dabei die zwei Kategoriengruppen, die in (2) und (3) eingeführt wurden. Die eine Kategoriengruppe betrachtet Praxisbezüge in der Betrachtung von Privatheit (symbolisch, relational, material), die andere Gruppe normative Ansprüche, die aus der Wissenschaftspraxis heraus für Privatheit formuliert werden (Kontrolle, Sozialität, Kritik). Beide stehen in einem Spannungsverhältnis. Dieses ist charakteristisch für jedweden Zugang zu Privatheit. Das Oszillieren zwischen normativem

Anspruch und praktischer Umsetzung zeigt sich in der Auseinandersetzung mit bisher jedem uns bekannten Feld der Privatheitsforschung.

Es sind (mindestens) zwei Anwendungsszenarien für das Modell vorstellbar. Das PFM bietet einerseits jenen Privatheitsforschenden, die sich gut in der Literatur auskennen, einen pragmatischen Überblick über das Forschungsfeld Privatheit und damit zugleich auch eine Art rudimentärer gemeinsamer Sprache. Diese ergibt sich aus der Unterscheidung von normativen und praxisbezogenen Kategoriengruppen. Der normative Anspruch von Sozialität beispielsweise und der praxisbezogene Zugang zu Privatheit über relationale Fragestellungen sind zwei verschiedene Paar Schuhe, die mit Hilfe des Modells konkret benannt werden können. Es lassen sich Forschungsschwerpunkte und -trends ausmachen und ggf. kritisch diskutieren. Andererseits bietet das Modell Forschenden Ansatzpunkte für eine Selbstverortung im Feld der Privatheitsforschung und damit Annäherungen an die Frage, welche Teilaspekte von Privatheit untersucht werden – und welche nicht. Vor dem Hintergrund des vielschichtigen Konzepts Privatheit ist die Erkenntnis über die zwangsläufige Begrenztheit des eigenen Vorhabens hilfreich, möglicherweise entlastend und lädt zum interdisziplinären Austausch ein. Indem die Stärken eines Zugangs aufgezeigt werden können, ist es zugleich legitim, lediglich Teilaspekte in den Blick zu nehmen.

Wie kann das nun konkret umgesetzt werden? Als Anwendungsbeispiel für diese beiden Optionen ist ein behavioristisch ausgerichtetes Forschungsvorhaben vorstellbar. Ansätze in der Tradition der Rational Choice-Theorieschule gehen davon aus, dass grundsätzlich vernunftbegabte Akteure ihre Privatheits-bezogenen Entscheidungen abwägen und in diesem Abwägungsprozess mit zunehmender Bildung reflexive Kompetenzen aufbauen können (Masur, 2020) oder in diesem Prozess scheitern und dabei bspw. Privatheits-Zynismus oder -Apathie entwickeln (Lutz & Newlands, 2021; Hoffmann et al., 2016). In behavioristischen Ansätzen kommt als normativer Bezug häufig Privatheit als Kontrolle zum Tragen, wobei mit Blick auf soziale Medien zunehmend auch Relationalität diskutiert wird (zu beiden Ansprüchen s. Trepte, 2021). Der Fokus in der Anwendungspraxis liegt nicht selten auf der narrativen Ebene. Privatheit wird, mit anderen Worten, vorrangig als kognitiv-reflexive Kontrolle behandelt, wobei auch die Frage nach Affordanzen, als materiale Perspektive, in den Blick gerät (auch hierzu Trepte, 2021).

Ein behavioristisch ausgerichtetes Privatheitsprojekt ließe sich nun bspw. kritisch mit Blick auf Forschungstrends für die Privatheitsforschung diskutieren. In dieser Richtung wird das Individuum als analytischer Zugang

zu Privatheit gewählt; eine gegenwärtig sehr erfolgreiche Perspektive, auch in der Privatheitspraxis. Das Anwendungsdesign, das sich beispielsweise aus der DSGVO ergibt, ist an individuellen Entscheidungen aufgehängt. In der tagtäglichen Anwendung bekommen Nutzer:innen vermittelt, dass es an Ihren Entscheidungen, an ihrer Bereitschaft, Zeit für die Auswahl oder Limitierung von Cookies zu investieren, liegt, ob sie Kontrolle über ihre Privatheit ausüben (wollen) oder nicht. Im Alltag von Nutzer:innen aber auch in den Kommunikations- und Medienwissenschaften dominieren behavioristische Ansätze das Feld (vgl. Möller, 2024a, b). Andere Ansätze müssen aktuell (noch) als randständig eingeordnet werden. Eine individuumszentrierte, narrativ und kontrollbezogene Privatheitsforschung ist hier eher der Regelfall als die Ausnahme. Stimmen aus der von der Kritischen Theorie inspirierten Privatheitsforschung mahnen etwa das Fehlen struktureller Perspektiven, bspw. als Kapitalismuskritik an (Fuchs, 2017; Helm & Seubert, 2020). Diese kritische Gegenüberstellung von Mikro- und Makro-Perspektive verfolgt das PFM aber gerade nicht. Das PFM beleuchtet das Feld der Privatheitsforschung gewissermaßen quer zu Mikro- und Makroperspektiven.

Insgesamt unterstreichen wir damit erneut, dass es sinnvoll sein kann, Privatheit als Problematisierungsbegriff zu betrachten und damit das Forschungsfeld als einen Bereich der Wissenschaftspraxis, der diese Problematisierungen adressiert. Privatheit ist im Grunde „unmöglich" und kann immer nur eine Annäherung sein. Darüber hinaus bieten wir mit dem PFM für den interdisziplinären Charakter des Feldes eine konstruktive Wendung. Die Vielfalt der theoretischen Zugänge muss nicht in unhandliche geteilte Definitionen gepresst werden, sondern darf zueinander sprechen.

5. Schlussbemerkungen

In der datafizierten Gesellschaft drohen die ohnehin herausfordernden Anliegen der Privatheitsforschung in ihrer Komplexität besonders dann unüberschaubar zu werden, wenn ein interdisziplinärer Dialog gewährleistet werden soll. Das PFM arbeitet entlang einer vergleichsweise schlichten Zweifach-Logik. Zum einen erkennt es die natürliche Ambivalenz an, die dem Begriff der Privatheit, und damit auch dem Forschungsfeld innewohnt. Wohin man schaut, Privatheitsforschung ist mit der nicht selten problematisch erscheinenden Zusammenschau von Praxis, Ansprüchen und deren Divergenz konfrontiert. Zum anderen haben wir über den Pro-

zess eines Gruppendelphis, quer über die Disziplinen hinweg jeweils drei normative und drei praxisbezogene Kategorien der Erforschung von Privatheit identifiziert, die den Begriff tragen. Das damit entstandene Modell soll ein interdisziplinäres Gespräch möglich machen, das die Komplexität des Privatheitsbegriffs und die unvermeidbare Reduktion von disziplinärer Privatheitsforschung unterstreicht.

Als möglichen Ansatzpunkt bieten wir mit dem PFM ein Modell für den interdisziplinären Dialog zwischen Privatheitsforschenden. Interdisziplinäre wie disziplinäre Modelle von Privatheit, die eine definitorische Antwort auf aktuelle Problemlagen versuchen, tendieren dazu, Variablen zu kumulieren oder das kritische Potenzial des Konzepts zu übergehen. So werden Modelle unhandlich, unnötig komplex. Fehlender Fokus kann zulasten von Forschungsergebnissen gehen. Anders das PFM, das ein rudimentäres Vokabular für das interdisziplinäre Gespräch über die Wissenschaftspraxis im Forschungsfeld Privatheit anbietet.

Das PFM setzt explizit keinen spezifischen Privatheitsbegriff voraus. Vielmehr arbeiten wir mit der Annahme, dass es eine interdisziplinäre Definition von Privatheit, die den unterschiedlichen theoretischen und analytischen Zugängen zum Feld gerecht wird, nicht zwingend geben muss. Indem wir der wissenschaftsbezogenen Diskussion über Privatheit übergreifende forschungspraktisch angewendete Kategorien entleihen, ermöglichen wir mit dem vorgeschlagenen Modell die Auseinandersetzung mit einer Vielzahl von Konzepten und Theorien.

Privatheitsforschung lässt sich so anhand von drei normativen Ansprüchen und drei anwendungsbezogenen Kategoriengruppen als ein eigenständiges Forschungsfeld beschreiben, das vor dem Hintergrund einer Spannungsbeziehung zwischen normativen und praxisbezogenen Überlegungen sowohl wissenschaftlich als auch alltagspraktisch wahrgenommene Privatheitsbelange adressiert.

Unterschiedliche Zugänge zu Privatheit können damit in einfacher Weise auf ihre Limitationen oder ihr Ergänzungspotenzial hin geprüft werden.

Diskutiert man vorliegende Forschung entlang des Modells, könnte man argumentieren, dass Privatheit häufig als eine Form der Kontrolle und zugleich auf der narrativen Ebene betrachtet wird. Behavioristische Forscher:innen sind sich dessen bewusst und setzen sich daher kritisch mit dem Kontrollbegriff auseinander. So weisen Dourish und Anderson (2009) bereits früh darauf hin, dass Kontrolle häufig mit Sicherheit gleichgesetzt wird und damit eine Engführung des Konzepts provoziert. Trepte (2022) stellt sich vor dem Hintergrund der umfassenden Bedeutung

sozialer Medien die Frage, inwiefern das Kontrollparadigma von relationalen Sicherungsmechanismen abgelöst wird. Solche richtungsweisenden Diskussionen lassen sich mit dem PFM nachvollziehen und einordnen. Behavioristische Forscher:innen können sich die Frage stellen, was sie zur Erforschung des Anspruchs der Kontrolle beitragen können, aber wie sich dieses eben zugleich vor dem Hintergrund von Sozialität und Kritik relativiert. Darüber hinaus können Forscher:innen mit Hilfe des Modells sensibel dafür werden, normative und praktische Kategorien nicht zu verwechseln. Während Kontrolle ein normativer Anspruch ist, kann im Fall von sozialen Medien Relationalität eigentlich Sozialität meinen, also die praktische Umsetzung von Privatheit in der Gemeinschaft mit anderen. Hier gilt es die Aufmerksamkeit für die Zuordnung als normative oder anwendungsbezogenen Kategorien zu schärfen.

Aus unserer Perspektive kann das PFM dazu beitragen, interdisziplinäre Privatheitsforschung durch einen Gesprächsansatz zu unterstützen. Dabei sind wir für Anregungen aus weiteren wichtigen Disziplinen wie den Rechtswissenschaften oder der Psychologie offen und laden zur weiteren Auseinandersetzung über das Modell ein. Zentral erscheint uns aber der Grundgedanke, dass es nicht die Steigerung von Komplexität ist, sondern die Sichtbarmachung von Zusammenhängen, die hier potenziell ein produktives Neben- und Miteinander von Wissenschaftspraktiken unterstützen kann. Darin liegt zugleich ein Appel für mehr interdisziplinäre Privatheitsforschung.

Literatur

Bräunlich, K., Dienlin, T., Eichenhofer, J., Helm, P., Trepte, S., Grimm, R., Seubert, S. and Gusy, C. (2021) 'Linking loose ends: An interdisciplinary privacy and communication model', *New Media & Society, 23*(6), pp. 1443–1464. Available at: https://doi.org/10.1177/1461444820905045.

Patrick B., Flüpke, Max H., Michael K., Marcel R., Rina W. (2025). Wir wissen, wo dein Auto steht. *Der Spiegel 1/2025.*

Crowley, J. L. (2017). A Framework of Relational Information Control: A Review and Extension of Information Control Research in Interpersonal Contexts: A Framework of Relational Information Control. *Communication Theory*, *27*(2), 202–222. https://doi.org/10.1111/comt.12115

Carstensen, T., Schaupp, S., Sevignani, S. (2023): Theorien des digitalen Kapitalismus. Arbeit und Ökonomie, Politik und Subjekt. Berlin: Suhrkamp.

Cheng, P., Bagci, I. E., Yan, J., & Roedig, U. (2019). Smart Speaker Privacy Control—Acoustic Tagging for Personal Voice Assistants. *2019 IEEE Security and Privacy Workshops (SPW)*, 144–149. https://doi.org/10.1109/SPW.2019.00035

De Leyn, T., De Wolf, R., Vanden Abeele, M., & De Marez, L. (2022). In-between child's play and teenage pop culture: Tweens, TikTok & privacy. *Journal of Youth Studies*, *25*(8), 1108–1125. https://doi.org/10.1080/13676261.2021.1939286

Dewitte, P., Wuyts K., Sion L., Van Landuyt D., Emanuilov I., Valcke P., und Joosen W. (2019) A comparison of system description models for data protection by design. *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 1512–15. SAC '19. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3297280.3297595.

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz & J. M. Mönig (Hrsg.), Medien und Privatheit (pp. 105–122). Passau: Karl Stutz.

Dienlin, T & & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297.

Dingledine, Roger, Nick Mathewson, and Paul F. Syverson (2004). „Tor: The second-generation onion router." *USENIX security symposium*. Vol. 4.

Dourish, P., & Anderson, K. (2006). Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction*, *21*(3), 319–342. https://doi.org/10.1207/s15327051hci2103_2

Dwork, C. (2011). A firm foundation for private data analysis. *Communications of the ACM*, *54*(1), 86-95.

Fuchs, C. (2012). The Political Economy of Privacy on Facebook. *Television & New Media, 13*(2), 139-159. https://doi.org/10.1177/1527476411415699

Grebe, H. (2019). Theoretische Grundlagen: Der Begriff der Problematisierung. In H. Grebe, *Demenz in Medien, Zivilgesellschaft und Familie* (S. 9–50). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-28116-8_2

Greene, D., & Shilton, K. (2018). Platform privacies: Governance, collaboration, and the different meanings of „privacy" in iOS and Android development. *New Media & Society*, *20*(4), 1640–1657. https://doi.org/10.1177/1461444817702397

Gstrein, O. J., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy & Technology*, *35*(1), 3. https://doi.org/10.1007/s13347-022-00497-4

Helm, P., & Seubert, S. (2020). Normative Paradoxes of Privacy: Literacy and Choice in Platform Societies. *Surveillance & Society, 18*(2): 185-195.

Hillebrandt, F. (2009). *Praktiken des Tauschens: Zur Soziologie symbolischer Formen der Reziprozität*. VS Verlag für Sozialwissenschaften / GWV Fachverlage GmbH, Wiesbaden. https://doi.org/10.1007/978-3-531-91693-4

Hoffmann, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, *10*(4). https://doi.org/10.5817/CP2016-4-7

Juels, A., Molnar, D. & Wagner, D. (2005), „Security and Privacy Issues in E-passports," First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05), Athens, Greece, 2005, 74-88, doi: 10.1109/SECURECOMM.2005.59.

Kuhn, C., Beck, M., Schiffner, S., Jorswieck, E., & Strufe, T. (2019). On Privacy Notions in Anonymous Communication. *Proceedings on Privacy Enhancing Technologies*, *2019*(2), 105–125. https://doi.org/10.2478/popets-2019-0022

Kumar, P. C., Subramaniam, M., Vitak, J., Clegg, T. L., & Chetty, M. (2020). Strengthening Children's Privacy Literacy through Contextual Integrity. *Media and Communication*, *8*(4), 175–184. https://doi.org/10.17645/mac.v8i4.3236

Lutz, C., & Newlands, G. (2021). Privacy and smart speakers: A multi-dimensional approach. *The Information Society*, *37*(3), 147–162. https://doi.org/10.1080/01972243.2021.1897914

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 2053951714541861. https://doi.org/10.1177/2053951714541861

Marwick, A. E. (2008). To catch a predator? The MySpace moral panic. *First Monday*. https://doi.org/10.5210/fm.v13i6.2152

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995

Masur, P. K. (2020). How Online Privacy Literacy Supports Self-Data Protection and Self-Determination in the Age of Information. *Media and Communication*, *8*(2), 258–269. https://doi.org/10.17645/mac.v8i2.2855

Mattoni, A. (2020). A Media-in-Practices Approach to Investigate the Nexus Between Digital Media and Activists' Daily Political Engagement. *International Journal of Communication*, *14*.

Möller, Johanna E. (2024). Situational privacy: theorizing privacy as communication and media practice, *Communication Theory*, *34*(3), 130–142.

Möller, Johanna E. (2025). Privacy. In Nai, A., Grömping, M. & Wirz, D. (Hrsg.), *Elgar Encyclopedia of Political Communication*, forthcoming.

Navarro-Arribas, Guillermo, and Vicenc Torra. „Information fusion in data privacy: A survey." *Information Fusion* 13.4 (2012): 235-244.

Niederberger, M. & Renn, O. (2018). *Das Gruppendelphi-Verfahren: Vom Konzept bis zur Anwendung*. Wiesbaden: Springer VS.

Nissenbaum, H. (2010). *Privacy in context: technology, policy, and the integrity of social life*. Stanford: Stanford Law Books.

Ochs, C. (2022): *Soziologie der Privatheit*. Baden-Baden: Nomos.

Reckwitz, A. (2002). The Status of the „Material" in Theories of Culture: From „Social Structure" to „Artefacts". *Journal for the Theory of Social Behaviour*, *32*(2), 195–217. https://doi.org/10.1111/1468-5914.00183

Reckwitz, A. (2003). Grundelemente einer Theorie sozialer Praktiken / Basic Elements of a Theory of Social Practices: Eine sozialtheoretische Perspektive / A Perspective in Social Theory. *Zeitschrift Für Soziologie*, *32*(4), 282–301. https://doi.org/10.1515/zfsoz-2003-0401

Rehms, S., & Köpsell, S. (2024). Disruptionen/Störungen aus Sicht von IT-Security und Privacy. *Insights into Disruption*, *1*(1). https://doi.org/10.62892/intodis.v1i1.3

Rost, M. (2024). *Das Standard-Datenschutzmodell (SDM): Einführung, Hintergründe und Kontexte zum Erreichen der Gewährleistungsziele. 2. Auflage.* Wiesbaden: Springer Vieweg.

Schatzki, T. R. (2002). *The Site of the Social: A Philosophical Account of the Constitution of Social Life and Change*. University Park, PA: Penn State University Press. https://doi.org/10.1515/9780271023717

Schmitz, L. (2024). „Dann drück ich auf's Mikro, wenn's hier mal um Dinge geht..." Kreative Privatisierung. Der Umgang mit Privatheitsansprüchen in der Smart Speaker-Nutzung. In Friedewald, M., Roßnagel, Geminn, C. L., Karaboga, M. & Schindler, S. (Hrsg.): *Data Sharing – Datenkapitalismus by Default?* Baden-Baden, Nomos, 215-242.

Serjantov, A., & Danezis, G. (2002). Towards an information theoretic metric for anonymity. In *International Workshop on Privacy Enhancing Technologies* (pp. 41-53). Berlin, Heidelberg: Springer.

Smith, Dinev, & Xu. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, *35*(4), 989. https://doi.org/10.2307/41409970

Solove, D. J. (2009). *Understanding privacy* (First Harvard University Press paperback edition). Cambridge, MA: Harvard University Press.

Stanner, W. E. H., & Martin, J. H. (2001). People from the Dawn: Religion, Homeland, and Privacy in Australian Aboriginal Culture. Palo Alto CA: Solas Press.

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy enhancing technologies. *ACM SIGCAS Computers and Society*, 31(1), 6–11.

Torra, V. (2012). Towards the formalization of re-identification for some data masking methods. In *Artificial Intelligence Research and Development* (pp. 47-55). Amsterdam: IOS Press.

Trepte, S. (2021). The Social Media Privacy Model: Privacy and Communication in the Light of Social Media Affordances. *Communication Theory*, *31*(4), 549–570. https://doi.org/10.1093/ct/qtz035

Wahl-Jorgensen, K., Bennett, L., & Taylor, G. (2017). The Normalization of Surveillance and the Invisibilitys of Digital Citizenship: Media Debates After the Snowden Revelations. *International Journal of Communication*, *11*, 740–762.

Welch, D. (2016). Social practices and behaviour change. In F. Spotswood (Hrsg.), *Beyond behaviour change* (S. 237–256). Policy Press. https://doi.org/10.1332/policypress/9781447317555.003.00127

Zuboff, S. (2020). *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: Public Affairs.

Freiheit und Selbstbestimmung in digitalen Infrastrukturen? Zur Kontroverse um den Gemeinwohlnutzen soziodigitaler Infrastrukturen

Carsten Ochs, Andreas Bischof, Mario Göbel, Simon Hensellek, Delphine Reinhardt und Ina Schiering

Zusammenfassung
Der vorliegende Beitrag dokumentiert den gesellschaftlich kontrovers diskutierten Pluralismus der Werte, die bei der Debatte um die Frage nach Freiheit und Selbstbestimmung in digitalen Infrastrukturen ins Spiel gebracht und verhandelt werden. Gegen Versuche, eine solche Debatte an bloß einem einzigen Wertprinzip (z. B. „free expression") zu orientieren, versammelt er eine interdisziplinäre Reihe von Expert:innen, die in die Debatte unterschiedliche, z. T. auch disziplinär justierte Perspektiven Einbringen. Der Beitrag geht auf das Diskussionspanel „Digitale Freiheit: Welche? Wessen? Und mit welchen Mitteln?" zurück, das im Rahmen der 9. Jahreskonferenz der Plattform Privatheit „Freiheit in digitalen Infrastrukturen" (17./18. Oktober 2024 in Berlin) veranstaltet wurde. Im Nachgang der Konferenz formierte sich eine Autor:innengruppe, die mit dem vorliegenden Beitrag die Vielschichtig- und -stimmigkeit der gesellschaftlichen Gewährleistung und Auseinandersetzungen um Freiheit in digitalen Infrastrukturen zu dokumentieren versucht. Um dies zu erreichen, wird mithilfe der im Feld der französischen Wirtschaftssoziologie entwickelten „économie des conventions" die Pluralität der Gesichtspunkte, unter denen die Frage nach Freiheit und Selbstbestimmung in vernetzten digitalen Infrastrukturen bearbeitet werden kann, kohärent dargestellt. Wie sich herausstellt, setzt die Gewährleistung von Freiheit in digitalen Infrastrukturen weit mehr voraus als die Orientierung an einem einzigen Wertprinzip: *Kompromisslinien* zwischen versch. Wertkonventionen müssen gefunden, das *Zusammenwirken* versch. Wertkonventionen muss erreicht, und mitunter muss die *Privilegierung* best. Werte auf Kosten anderer im Sinne eines Nullsummenspiels kollektiv bindend vereinbart werden.

1. Einleitung

Am 7. Januar 2025 verkündete der Vorstandsvorsitzende von Meta Platforms, Mark Zuckerberg, das Ende des sogenannten „Fact Checking Programs" auf den vom Konzern betriebenen Plattformen Instagram, Facebook und Threads. Das auf der Meta-Website veröffentlichte Video, in dem Zuckerberg diese Entscheidung verkündet, hat eine Laufzeit von fünf Minuten und siebzehn Sekunden; in Sekunde 6 fällt zum ersten Mal der in der Begründung wiederholt verwendete Begriff der „free expression", d. h. des „freien Ausdrucks" oder der „Meinungsfreiheit" (so die üblichen Übersetzungen), was sich hier, sofern im Video auch die Wendung „give people a

voice“ fällt, im Sinne der Redefreiheit verstehen lässt.[1] Während sich Metas Vorstandvorsitzender somit also auf die Gewährleistung von diskursiven Freiheiten berief, um die Ablehnung der Verantwortungsübernahme für bzw. der Regulierung von innerhalb der Meta-Infrastrukturen erzeugten und verbreiteten Inhalten zu rechtfertigen, reagierten europäische Kommentator:innen auf die Ankündigung mit Kritik. Netzpolitik.org-Chefredakteur Markus Beckedahl etwa wurde auf der ZDF-Website u. a. wie folgt paraphrasiert bzw. zitiert: „Die Redefreiheit werde über alles gestellt und die Content-Regeln vor allem bei den Themen (…) Migration und ‚Gender' würden so geändert, dass ‚zukünftig sämtliche Äußerungen, auch diskriminierende, auch rassistische Meinungsäußerungen möglich sind'".[2]

Man muss also kein:e Digitalisierungsforscher:in sein, um mit der Frage nach der Freiheit und Selbstbestimmung in digitalen Infrastrukturen konfrontiert zu sein, sie stellt sich vielmehr für uns alle, die wir tagtäglich unseren Tätigkeiten, Interessen und/oder Geschäften in diesen Infrastrukturen nachgehen, ganz praktisch und wie von selbst, ob wir wollen oder nicht. Perspektiviert man Freiheit als mehr oder weniger stark realisierten und je spezifisch ausgeformten Bestandteil von Gemeinwesen, so verbindet sich die Frage zudem bruchlos mit der Entwicklung und Gestaltung digitaler Gesellschaftsstrukturen. In Bezug auf letztere war derweil in den letzten 30 Jahren ein gewisser Umschwung zu beobachten:

- Als das Internet gegen Mitte der 1990er Jahre begann, zur zentralen Kommunikations- und Informationsinfrastruktur der Alltagspraktiken in den verschiedensten sozialen und gesellschaftlichen Bereichen zu werden, verband sich damit die Hoffnung, dass die technische Funktionsweise der zugrundeliegenden Systeme die Entwicklung demokratischer Strukturen, emanzipatorischer Projekte und selbstbestimmter Identitätsbildung gewissermaßen direkt antreiben würde (Rheingold 1993; Schuler 1994; Turkle 1995; Castells 1996; Wellman 2001; Quan-Hase et al. 2002; Benkler 2006). Die Verteiltheit der Rechennetzwerke nährte bei all jenen, die noch die *one-to-many*-Broadcasting-Struktur der Massenmedien und ihre mitunter destruktive Rolle im Kontext der totalitären Barbareien des 20. Jh. im Gedächtnis hatten (man denke nur an die Nutzung des „Volksempfängers" im Nationalsozialismus), die Hoffnung, dass Kom-

1 https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/ (zugegriffen am 9. Januar 2025).

2 https://www.zdf.de/nachrichten/wirtschaft/unternehmen/meta-zuckerberg-faktencheck-moderation-beckedahl-100.html (zugegriffen am 9. Januar 2025).

munikationen und Informationsflüsse durch die Entwicklung horizontal strukturierter Kommunikationsnetzwerke quasi automatisch demokratisiert würden.
- Gegenüber diesem optimistischen Digitalisierungsdiskurs der 1990er Jahre fallen die nachfolgenden Debatten schon seit einer Weile eher dystopisch aus. Die Zentralisierung der Kommunikation durch Plattformen und ihre Netzwerkeffekte, die Fake News- und Propaganda-Maschinerien des Internets, die datenökonomische Instrumentalisierung des Sozialen, die Verstärkung sozialer Ungleichheit durch statistisch operierende Machine Learning-Systeme sowie die Ressourcen- und Menschen-Ausbeutung zur Entwicklung letzterer werden kritisiert (van Dijck 2013; Lovink 2017; Benkler & Faris & Roberts 2018; Eubanks 2018; Pfeiffer 2021; Crawford 2024). Dabei rücken die kritischen Analysen auch die Besitzergreifung der Märkte durch Unternehmen in den Fokus (Staab 2019) und perspektivieren das Geschäftsmodell des „Überwachungskapitalismus" als behaviouristischen Anschlag auf Freiheit, Selbstbestimmung und die Offenheit der Zukunft insgesamt (Zuboff 2018) – und dies nicht erst, seit sich die unheilvollen Allianzen zwischen politischem Rechtspopulismus jenseits (Maga-Republicans) und diesseits des Atlantiks (AfD) einerseits und datafiziertem Tech-Feudalismus andererseits (Musk) aufgemacht haben, die historisch mühevoll etablierten demokratischen Strukturen der USA und Europas zu unterminieren.

Die Tonlage der Debatten um die digitalen Infrastrukturen des Sozialen hat sich somit zwischen 1990 und heute gewandelt und ist von einem eher utopischen in einen eher dystopischen Grundton übergangen (Ochs 2022). Wurde den fraglichen Infrastrukturen zunächst in puncto Freiheit und Selbstbestimmung ein zuweilen fast schon frenetisch bejubelter Gemeinwohlnutzen attestiert (vgl. stellvertretend Benkler 2006), so wird aktuell verstärkt von einer digitalen Schädigung dieses Gemeinwohls ausgegangen (Zuboff 2018).

Der vorliegende Beitrag will gegenüber der zwischen den rekonstruierten Polen oszillierenden Debatte die Vielfältigkeit der gesellschaftlichen Kontroversen um den Gemeinwohlnutzen digitaler Infrastrukturen herausarbeiten. Er setzt dabei mit der gesellschaftswissenschaftlichen Heuristik der „Rechtfertigungslogiken" an (Boltanski & Thévenot 2007; 2011; Diaz-Bone 2018). Der im Feld der französischen Wirtschaftssoziologie entwickelten „économie des conventions" zufolge haben die Gesellschaften Europas historisch unterschiedliche Gesichtspunkte entwickelt, unter denen Gemein-

wohlnutzen betrachtet bzw. für diesen Nutzen argumentiert wird. Das Gemeinwohl und seine Konstitutionsbedingungen treten in dieser Perspektive im Plural auf, was zunächst als empirische Feststellung zu verstehen ist: Moderne Gesellschaften ringen im Streit um die jeweils angemessene Komposition vielfältiger Werte, deren praktisches Wirken den jeweiligen Gemeinwohlaspekten Geltung verschaffen soll. Die historisch evolvierten Gemeinwohlprinzipien sind dabei jeweils verknüpft mit sogenannten „Konventionen", die das jeweilige Gemeinwohlprinzip angeben und dessen Logik zum Ausdruck bringen. Sie bestimmen die Werte, Kriterien, Beziehungslogiken usw., die sich mit dem jeweiligen Gemeinwohlprinzip verknüpfen. Wer etwa die Digitalisierung von Unternehmen mit der Hoffnung auf Effizienzgewinne vorantreiben will, für eine „maximal unregulierte" Datenökonomie wirbt oder die Rolle von Metas Facebook-Plattform im Kontext der Erstürmung des US-amerikanischen Kapitols am 6. Januar 2021 problematisiert (Ochs 2024), plädiert jeweils für eine Veränderung des Status Quo der digitalen Gesellschaft. Im Rahmen dieser Plädoyers wird folglich Kritik an den bestehenden gesellschaftlichen Verhältnissen geübt, wobei wiederum auf bestimmte Rechtfertigungslogiken zurückgegriffen wird, die ihrerseits mit je spezifischen Vorstellungen von Wertigkeit in Verbindung stehen: industrielle Effizienz, der freie Tausch auf Märkten und die Wahrung staatsbürgerlicher Rechte und Anliegen gehören verschiedenen Rechtfertigungslogiken an, die sich im Rahmen der gesellschaftlichen Auseinandersetzungen um Digitalisierung widersprechen, miteinander verbünden oder gegenseitig kritisieren können.

Dieser Beitrag wird die angedeutete Pluralität der Gesichtspunkte, unter denen die Frage nach Freiheit und Selbstbestimmung in vernetzten digitalen Infrastrukturen bearbeitet werden kann und – wie uns die Empirie der Kontroversen um die digitale Gesellschaft vor Augen führt – auch wird, mithilfe einer heuristischen (und dementsprechend lockeren) Orientierung am Schema der Rechtfertigungslogiken der „Soziologie der Konventionen" (Diaz-Bone 2011) herausarbeiten. Der Bezugnahme auf die Soziologie der Konventionen liegen insofern pragmatische Motive zugrunde, als unser Beitrag auf die Organisation und Durchführung des Panel #1 zum Thema „Digitale Freiheit: Welche? Wessen? Und mit welchen Mitteln?" der Jahreskonferenz der Plattform Privatheit 2024 zurückgeht.[3] Das Panel zielte selbst

3 Am Panel nahmen seinerzeit Mario Göbel (VREEDA GmbH), Gunnar Stevens (Universität Siegen), Andreas Bischof (TU Chemnitz) und Ina Schiering (Ostfalia Hochschule) teil, moderiert wurde es von Hendrik Kafsack, ursprünglich als Teilnehmer:in-

schon darauf ab, die in den Debatten vernehmbaren unterschiedlichen Stimmen miteinander ins Gespräch zu bringen, um so auf der Tagung den unterschiedlichen und mitunter reichlich kontroversen Gesichtspunkten Raum zu geben. Aus dem Panel heraus bildete sich schließlich eine Autor:innengruppe, die mit dem vorliegenden Artikel die Vielschichtig- und -stimmigkeit der gesellschaftlichen Auseinandersetzungen um Freiheit in digitalen Infrastrukturen zu dokumentieren versucht. Wir verwenden die Soziologie der Konventionen dementsprechend vordringlich im Sinne eines praktischen Instrumentes, das es erlaubt den hier versammelten unterschiedlichen Perspektiven einen Rahmen zu geben beziehungsweise diese in Beziehung zu setzen. In dieser Zusammenschau liegt der Mehrwert des Beitrags – nicht in der Präsentation gänzlich neuer Erkenntnisse o. ä.

Um das genannte Ziel zu erreichen, werden wir zunächst sehr knapp und kursorisch den analytischen Rahmen der Konventionentheorie abstecken (Abschnitt 2), um daraufhin die Frage nach Freiheit und Selbstbestimmung in digitalen Infrastrukturen aus der Perspektive einer Reihe von Konventionen bzw. „Rechtfertigungsordnungen" zu beleuchten: Aus Sicht der Marktkonvention (Abschnitt 3), Industriekonvention (Abschnitt 4), staatsbürgerlichen Konvention (Abschnitt 5) und der handwerklichen Konvention (Abschnitt 6). Die Fragestellungen, die aus den Perspektiven jeweils bearbeitet werden, lauten: Welche Bedingungen sind der Entstehung von Freiheit und Selbstbestimmung in vernetzten Infrastrukturen förderlich? Welche Maßnahmen können ergriffen werden, um die jeweiligen Bedingungen zu etablieren? Und welche gegenläufigen Prozesse oder Sachverhalte stehen dem entgegen? Im Schlusskapitel (Abschnitt 7) werden die verschiedenen Befunde im Sinne einer Gesamtschau diskutiert und es werden abschließend Folgerungen gezogen.

---

nen vorgesehen waren außerdem Delphine Reinhardt und Carsten Ochs (letzterer zeichnet für die Panel-Organisation federführend verantwortlich), die aber, genau wie Simon Hensellek, an der Gesamtkonferenz nicht teilnehmen konnten. Wie an der Aufzählung erkennbar wird, formierte sich im Nachgang zur Konferenz aus den Gruppen der ursprünglich vorgesehenen Teilnehmenden, der Organisator:innen und der kurzfristig eingesprungenen Panelist:innen (Dank gebührt an dieser Stelle Gunnar Stevens und Ina Schiering!) dann die Gruppe der Autor:innen dieses Beitrags. Abschließend soll erwähnt werden, dass alle Panelist:innen und Autor:innen in Projekten der Plattform Privatheit aktiv sind, für deren Förderung wir uns beim Bundeministerium für Bildung und Forschung (mittlerweile Bundeministerium für Forschung, Technologie und Raumfahrt) herzlich bedanken.

2. Eine kursorische Skizze der Konventionenökonomie

Geht man davon aus, dass technische Entwicklungen und Innovationen grundsätzlich immer mit kontroversen gesellschaftlichen Debatten einhergehen (können), in denen die pluralen Gesichtspunkte verhandelt und miteinander in Beziehung gesetzt werden, die für die jeweilige Innovation als relevant erachtet werden (Callon 1986; Marres 2007), so scheint es zielführend, diese Gesichtspunkte zunächst zu explizieren, um auf diese Weise die gesellschaftlichen Aushandlungsprozesse auf ein qualitativ hohes, (d. h. bzgl. der zu berücksichtigenden Gesichtspunkte:) wohlinformiertes Niveau zu hieven. Der vorliegende Beitrag wurde von fünf Autor:innen verfasst, die beim Blick auf digitale Infrastrukturen nicht zuletzt auch aufgrund unterschiedlicher disziplinärer Zugehörigkeiten jeweils unterschiedliche Perspektiven auf den betrachteten „Gegenstand" werfen: nicht nur unterscheiden sich sozialwissenschaftliche (Ökonomik, Mensch-Maschine-Interaktion, Soziologie[4]) und technikwissenschaftliche Herangehensweisen (Informatik), sondern es finden sich auch innerhalb der Disziplinen wiederum unterschiedliche Schwerpunktsetzungen. Unsere Herangehensweise folgt der Prämisse, dass diese zunächst disziplinär begründete Vielfalt bis zu einem gewissen Grade mit der gesellschaftlichen Perspektivenvielfalt resoniert: wer betriebswirtschaftlich über Digitalisierung nachdenkt, orientiert sich eher an Marktlogiken, die informatische Herangehensweise legt eine industrielle, die rechtswissenschaftliche eine staatsbürgerliche Perspektive nahe usw.

Um diese Intuition in einen kohärenten Analyserahmen zu überführen, ordnen wir die weiter unten jeweils aus einer bestimmten disziplinären Sicht angestellten Überlegungen in das heuristische Schema der Rechtfertigungsordnungen ein. Das Schema geht davon aus, dass sich in der europäischen Gesellschaftsgeschichte eine Reihe von „Wertigkeitsordnungen" (Boltanski & Thévenot 2011: 49) herausgebildet hat, in denen sich jeweils bestimmte Vorstellungen von sozialer Ordnung, Gemeinwohl und „Wertigkeit" (was ist gut, was schlecht?) miteinander verbinden. Ausgangspunkt der Überlegungen ist die Beobachtung, dass in modernen Gesell-

4 Bei der systematischen Erforschung von Mensch-Maschine-Interaktionen unter dem englischsprachigen Oberbegriff „Human-Computer-Interaction" (HCI) handelt es sich eigentlich um einen interdisziplinären Zweig der Informatik, der vielfach grundlegende Wissensbestände der Sozialwissenschaften computerwissenschaftlich fruchtbar macht. Wir schlagen ihn hier der Soziologie zu, weil unser HCI-Vertreter (unbeschadet einer Vergangenheit in der Informatik) im Bereich der Techniksoziologie aktiv ist.

schaften regelmäßig Diskussionen, Auseinandersetzungen, Konflikte, Dispute etc. darüber auftreten, wie hinsichtlich eines bestimmten *state of affairs* weiter verfahren werden soll (Boltanski & Thévenot 2011: 44): Im Rahmen von Autounfällen, am Arbeitsplatz oder in der WG-Küche entwickeln sich konflikthafte Situationen (Wer hatte Vorfahrt? Wer hat den Auftrag vermasselt? Wer ist für den Abwasch zuständig?), in deren Rahmen sich die Beteiligten gegenseitig kritisieren bzw. rechtfertigen. Sie orientieren sich dabei an „Rechtfertigungsordnungen als ‚Denkmodelle' für ihr reales, alltägliches Urteilen und Handeln" (Diaz-Bone 2018: 145). Solche Rechtfertigungsordnungen liefern im Allgemeinen „kollektive Koordinationslogiken" (ebd.: 147, Fn. 212), die so lange stillschweigend eine Einigung ermöglichen, wie alle Beteiligten ihnen folgen, aber: „Sollten die Dinge schlecht laufen und ein Disput entstehen, würden die Kontrahenten die implizite Voraussetzung sprengen, es handele sich um gewöhnliche Handlungsabsichten oder einwandfreie Gegenstände. Nun nehmen sie Bezug auf allgemeine Prinzipien, (…) um Behauptungen zu rechtfertigen. Sie gründen ihre Argumentation auf umfassende, auf Konventionen basierende Voraussetzungen, die Menschen oder nicht-menschliche Entitäten erfüllen müssen, um qualifiziert zu sein. Sie unterziehen die Qualifikationen einer auf Konventionen basierenden Prüfung." (Boltanski/Thévenot 2011: 48)

Konventionen gelten demnach als Bestandteile von Rechtfertigungsordnungen, die den „Grundsatz gemeinsamen Menschseins zum einen, das Erfordernis der Ordnung zum anderen" auf je eigene Weise miteinander kombinieren (ebd.: 55), und als Ordnung dann auf ebenso spezifische Weise das Erreichen eines Gemeinwohls zu ermöglichen versprechen. Boltanski und Thévenot unterscheiden zunächst sechs Rechtfertigungsordnungen, die sich in idealisierter und idealtypischer Form und ausformuliert in den Werken der politischen Philosophie des historischen Westens auffinden lassen.[5] Illustrieren lässt sich dies am Beispiel der Theorie Adam Smiths: Während Smith das „gemeinsame Menschsein" durch von allen Menschen geteilte „Neigung zum Tausch als Eigeninteresse" bestimmt sieht (Boltanski & Thévenot 2007: 69), ergibt sich aus der Prämisse gleichzeitig eine spezifische Form sozialer Ordnung, denn daraus lassen sich „die Bausteine eines *Gemeinwesens* gewinnen, das auf einem vom Markt geschaffenen Band beruht. Dieses Band vereinigt die Personen mittels knapper, allseits begehrter Güter, während sich der Preis, den man für den Besitz eines

5 Die Reichweite der Aussagen der „Soziologie der Konventionen" beschränkt sich dementsprechend auf diesen kulturgeographischen und -historischen Bereich.

solchen Gutes entrichten muss, aufgrund der Konkurrenz der Leidenschaften aus den Wünschen all jener, die dieses Gut ebenfalls haben wollen, ergibt." (ebd.) Dementsprechend „bezeichnet [die Marktkonvention] die Ausrichtung der Koordination an den individuellen Bedürfnissen und den aktuellen Preisen der Produkte. Als legitime Praxis gilt der freie Wettbewerb (die Konkurrenz) unter Absehung der jeweiligen Person und der individuelle geldvermittelte Tausch (Geld gegen Güter) zwischen Individuen." (Diaz-Bone 2018: 148) Trotz der Orientierung am Individuum rechtfertigt sich diese Koordinationslogik (so wie alle anderen Rechtfertigungsordnungen auch) damit, dass sie dem Gemeinwohl diene: „Die ‚unsichtbare Hand' des Marktes erzielt aus dieser Perspektive das optimale Gemeinwohl." (ebd.) Wir schlagen die skizzierte Rechtfertigungslogik dem Bereich der Wirtschaftswissenschaften zu (Wettbewerb durch freie Tauschbeziehungen, am Markt behaupten müssen usw.).

Neben der Marktkonvention bzw. der Welt des Marktes spielen hinsichtlich des vorliegenden Beitrags zunächst v. a. die industrielle, die staatsbürgerliche und die handwerkliche Konvention eine zentrale Rolle. Die Relevanz der industriellen Konvention ergibt sich dabei nicht zuletzt aus der Bedeutung, die diese für die empirische Praxis der Wirtschaft hat, da „wirtschaftliches Handeln auf zumindest zwei unterschiedlichen Formen der Koordination beruht, zum einen auf der durch den Markt, zum anderen aber auf der einer industriellen Ordnung" (Boltanski & Thévenot 2011: 61). Anders als in der an volatilen Preisdifferenzen orientierten Welt des Marktes zählt für die industrielle Welt „die langfristige, effiziente Planung der Produktion." (Diaz-Bone 2018: 149) Versinnbildlichen lässt sich der Unterschied an den andersartigen Orientierungen des algorithmischen Hochfrequenzhandels von Wertpapieren einerseits und der einstmals dem „Wasserfallmodell" folgenden Software-Entwicklung andererseits: Hebt der erstere auf die Nutzung kurzfristiger Preisdifferenzen ab, geht es in letzterer um Planung, Standardisierung und Effizienz, was sich nicht zuletzt in der weiten Verbreitung von Skalen, Metriken, Quantifizierungen und Kalkülen artikuliert: „Planung wird hier mit gesellschaftlichem Fortschritt verbunden, und ist auf eine Zukunft ausgerichtet, nicht auf die Befriedigung einer aktuellen Nachfrage (…). Personen stehen hier nicht in Tauschbeziehungen zueinander, sondern in ‚funktionalen' Beziehungen." (ebd.) Im Kontext dieses Artikels sehen wir diese Rechtfertigungslogik insbesondere im Bereich der IT-Sicherheit als dominant an, da sich dort die Merkmale der Planung („Security by Design"), der Skalierung und Messbarkeit („Sicherheit mess-

bar machen") und der Funktionalität wiederfinden („menschliche User:innen als schwächste Stelle von Systemen").

In gewisser Weise als historischer Vorläufer der industriellen Welt kann indes die „häusliche Welt" gelten (Boltanski & Thévenot 2007: 228), in der soziale Beziehungen v. a. als Vertrauensverhältnisse gestaltet werden. Die Koordination sozialer Prozesse hebt „auf die zwischenmenschlichen Beziehungen" ab (Boltanski & Thévenot 2007: 228) und ist insofern am zunächst aus dem Sippenmodell der Großfamilie hervorgegangenen Ideal der vertrauenswürdigen Interaktion orientiert. Die Konvention, um die sich diese Rechtfertigungsordnung entfaltet, bezeichnen Boltanski und Thévenot indes als „handwerkliche": die Bewertung von Personen, Dingen und Prozesse folgt hier dem Kriterium der Anerkennung und der Reputation, positiv bewertet wird das Bekannte, an Routinen und Gepflogenheiten ansetzende (ebd.: 231), sowie „die informelle und private Form der Kommunikation" (Diaz-Bone 2018: 151). In moderner Form findet sich diese Logik etwa dort, wo Organisationen „relevante informelle Formen (Umgangsformen) zu formalisieren suchen (‚codes of conduct')." (ebd.) Im vorliegenden Beitrag postulieren wir eine starke Prägung des Bereichs der Human-Computer-Interaction (HCI) durch die handwerkliche Konvention, sofern HCI nicht nur auf die Gestaltung vertrauenswürdiger Systeme abzielt, sondern dabei auch genau mit der Aufgabe konfrontiert ist, das informelle „tacit knowledge" der Praxis (Polanyi 1958) in formale Systeme übersetzen zu müssen (vgl. etwa zu den Bemühungen im Privacy-Bereich Palen & Dourish 2003; Dourish & Anderson 2009).

Als letzte Konvention wollen wir schließlich die der „staatsbürgerliche[n] Welt" einführen (Boltanski & Thévenot 2007: 254), denn trotz der Tatsache, dass die Digitalisierungsprozesse der letzten Jahre v. a. datenökonomisch geprägt waren (was auf eine Dominanz von Markt- und Industriekonvention verweist), spielt in den gesellschaftlichen Auseinandersetzungen insbesondere auch die staatsbürgerliche Konvention eine große Rolle (vgl. etwa die Debatten um „nationale Datensouveränität" usw.). Die staatsbürgerliche Konvention „hält eine Welt im Inneren zusammen, die die Solidarität und die Rechte und die Gleichheit der Menschen betont, weil sie Teil eines aufgeklärten, bürgerlichen Kollektivs sind" (Diaz-Bone 2018: 154). Während dementsprechend Werte wie Gleichheit, Fairness, Partizipation betont werden, stehen Kollektivbewusstsein, Gemeinwille und kollektives Handeln im Vordergrund: „In der staatsbürgerlichen Welt nimmt der Souverän im Konvergieren der menschlichen Einzelwillen Gestalt an, sobald die Bürger ihre Partikularinteressen aufgeben und sich ausschließlich

am Gemeinwohl orientieren." (Boltanski/Thévenot 2011: 60) Im Kontext dieses Beitrags verstehen wir den Bereich der *Data Governance* als einen Bereich, der stark von der staatsbürgerlichen Konvention geprägt ist, da es in diesem immer um die organisatorische, regelhafte und/oder technologische Gewährleistung eines kollektiven Umgangs mit Daten geht, der die Regelung von Verantwortlichkeiten (Repräsentant:innen) vorsieht, und auf „gesetzliche Formen" zurückgreift (Boltanski & Thévenot 2007: 257), d. h. auf Regelwerke, kollektive Vereinbarungen usw.

An dieser Stelle beenden wir vorläufig den kursorischen Durchgang durch einige der Rechtfertigungsordnungen der „Soziologie der Konventionen"[6] und die Verknüpfung der vier vorgestellten Rechtfertigungslogiken mit den Schwerpunktsetzungen der in diesem Artikel versammelten disziplinären Perspektiven. Wir werden im Weiteren Freiheit und Selbstbestimmung in digitalen Infrastrukturen aus Sicht der Markt-, Industrie-, der häuslichen sowie der staatsbürgerlichen Konvention jeweils kurz beleuchten. Die Rückbindung an das vorgestellte Schema wird sich dabei eher locker gestalten, denn letzteres wird hier v. a. zu Differenzierungs- und Sensibilisierungszwecken und insofern in pragmatischer Absicht eingeführt: um für die Vielfalt der Gesichtspunkte zu sensibilisieren, die es im Rahmen der gesellschaftlichen Aushandlung digitaler Vergesellschaftung zu berücksichtigen gilt – eine Vielfalt, die die im Folgenden präsentierten disziplinären Sichtweisen auf Freiheit und Selbstbestimmung in digitalen Infrastrukturen deutlich vor Augen führen werden.

3. *Freiheit und Selbstbestimmung aus Sicht der Marktkonvention: Die betriebswirtschaftliche Perspektive des Entrepreneurship*

In der betriebswirtschaftlichen Perspektive auf Freiheit und Selbstbestimmung in digitalen Infrastrukturen stehen insbesondere die Themen Entrepreneurship, Innovation und Marktorientierung im Vordergrund. Unternehmen sind zum einen darauf angewiesen, Daten effektiv und effizient zu nutzen, um Wettbewerbsvorteile zu generieren und innovative Geschäftsmodelle zu entwickeln. Gleichzeitig müssen sie zum anderen aber auch einen verantwortungsvollen Umgang mit Daten pflegen, da sie nicht

6 Der Vollständigkeit halber soll erwähnt sein, dass über die hier vorgestellten vier Konventionen hinaus noch die Konventionen der Inspiration, der Bekanntheit, die ökologische Konvention sowie die Netzwerkkonvention angeführt werden (vgl. Diaz-Bone 2018: 141-163).

in einem (rechtlichen und gesellschaftlichen) Vakuum agieren. So stellt die Einhaltung regulatorischer Rahmenbedingungen wie der Datenschutz-Grundverordnung (DS-GVO) eine zentrale Herausforderung für einige Unternehmen dar, während andere sie wiederum als Chance begreifen (Akanfe et al. 2024; Hamilton & Sodeman 2020; Li et al. 2019). Im heuristischen Rahmen des vorliegenden Textes wird daran deutlich, dass die Marktkonvention somit in wechselseitiger Beziehung zur handwerklichen (Vertrauen) und staatsbürgerlichen Konvention (kollektives Regelwerk der DS-GVO) steht, die von den konkreten Unternehmen faktisch als hinderlich oder förderlich für die Orientierung an der Marktkonvention gesehen werden kann.

3.1 Freiheit und Datenhoheit als unternehmerische Erfolgsfaktoren

Freiheit in digitalen Infrastrukturen bedeutet dementsprechend für Unternehmen auf der einen Seite v. a. den Zugang zu Daten sowie deren Nutzung im Sinne ihrer betriebswirtschaftlichen Prozesse und der am Markt angebotenen Produkte bzw. Dienstleistungen. Daten fungieren hierbei als essenzieller „Rohstoff" für digitale Geschäftsmodelle, die auf personalisierten Angeboten, künstlicher Intelligenz oder algorithmischen Entscheidungsprozessen basieren (Hartmann et al. 2016; Sorescu 2017). Auf der anderen Seite muss Freiheit in digitalen Infrastrukturen jedoch gleichermaßen auch die Hoheit über deren Nutzung für Datengebende (z. B. Nutzende bzw. allgemein Bürgerinnen und Bürger) bedeuten. Das heißt, erfolgreiche Unternehmen müssen insofern zunehmend einen verantwortungsvollen Umgang mit Daten gewährleisten, um sowohl die Erwartungen der Datengebenden bzw. Nutzenden zu erfüllen (handwerkliche Konvention) als auch regulatorischen Anforderungen zu genügen (staatsbürgerliche Konvention).

Die DS-GVO gibt dabei den Rahmen vor, innerhalb dessen Unternehmen mit personenbezogenen Daten arbeiten dürfen. Sie verpflichtet die Unternehmen, eine transparente Datenverarbeitung sicherzustellen und den Nutzenden klare Informationen zur Verwendung ihrer Daten bereitzustellen. In der Praxis führt dies jedoch oft zu intransparenten Einwilligungsverfahren: Nutzende akzeptieren Datenschutzrichtlinien, ohne sie tatsächlich zu lesen oder verstehen zu können (Bakos et al. 2014; Obar & Oeldorf-Hirsch 2020). Dies wirft Fragen zur realen Selbstbestimmung im digitalen Raum auf, da Kunden durch die schiere Menge und Komplexität der Bestimmungen überfordert werden. Eine Möglichkeit, dieser

Überforderung entgegenzuwirken, ist die gezielte Anpassung der Darstellung von Datenschutzrichtlinien „by default" (Steinfeld 2016), was sich als Zugeständnis an die an Funktionalität und Effizienz orientierte Industriekonvention interpretieren lässt.

3.2 Regulierung und Transparenz: Herausforderungen für Kunden und Unternehmen

Denn sofern die derzeitige Regulierung in der Praxis darauf hinausläuft, dass Unternehmen umfangreiche Datenschutzerklärungen bereitstellen müssen, ohne deshalb jedoch zu einer besser informierten Entscheidungsfindung der Nutzenden beizutragen (Bakos et al. 2014; Obar & Oeldorf-Hirsch 2020), lässt sich dies als klassische Ineffizienz (und in weiten Teilen auch Ineffektivität) durch fehlgeleiteten Eingriff in den freien Markt interpretieren. Viele Nutzende sind sich trotz erheblicher Informations- und Zustimmungspflichten nicht bewusst, wie ihre Daten verarbeitet werden, oder haben keine realistische Möglichkeit, Datenschutzstandards verschiedener Anbieter miteinander zu vergleichen (ebd.).

Es fehlt in diesem Sinne an Mechanismen, die sowohl Nutzende als auch Unternehmen dabei unterstützen, Ineffizienzen abbauen. Nutzende benötigen einfache und transparente Hilfsmittel, um datenschutzfreundliche Produkte bewerten und vergleichen zu können. Zwei einfache, aber innovationsfördernde Optionen erscheinen hier besonders attraktiv:

- Zum einen könnte eine standardisierte „statische" Datenschutzkennzeichnung, vergleichbar mit Energieeffizienz- oder Nutri-Score-Labeln (obgleich in ihrer Ausgestaltung nicht unumstritten) informierte Entscheidungen bereits vor Vertragsschluss erleichtern. Fox et al. (2022) zeigten beispielsweise, dass solche Labels das Vertrauen der Nutzenden stärken und diesen erlauben, einfach und schnell relativ fundierte Entscheidungen zu treffen. Eine transparente, standardisierte Kennzeichnung könnte diese Informationslücke schließen und bewusste, datenschutzfreundliche Entscheidungen fördern. Selbst eine mehrdimensionale Skala – vorausgesetzt, sie ist gut durchdacht – würde hier die regelmäßig viel zu langen und komplexen Datenschutzbedingungen für Nutzende effektiv und effizient darstellen können.
- Ein zweiter „dynamischer" Ansatz wäre ein transparentes „Live-Datencockpit", das Nutzenden in Echtzeit zeigt, welche Daten gerade wofür genutzt werden und ihnen ermöglicht, ihre Einwilligungen jederzeit zu

prüfen, anzupassen oder zu widerrufen (Puhlmann et al. 2023). Dies könnte nicht nur die Selbstbestimmung der Nutzenden stärken, sondern auch das Vertrauen in digitale Plattformen erhöhen, indem Datenschutzentscheidungen nicht als einmalige Zustimmung, sondern als kontinuierlich anpassbare Kontrolle verstanden werden (Bier et al. 2016; Raschke et al. 2018).

Derartige Lösungen würden nicht nur Nutzenden helfen, sondern auch Unternehmen einen Wettbewerbsvorteil verschaffen, die datenschutzfreundlich und transparent agieren und dies so vertrauenswürdig kommunizieren könnten. Transparente Unternehmen könnten ihre Vorreiterrolle im Datenschutz betonen und dadurch Vertrauen sowie Marktanteile gewinnen. Datenschutzbewusste Geschäftsmodelle könnten auf diese Weise ein Alleinstellungsmerkmal werden und wirtschaftlichen Erfolg fördern.

3.3 Datenschutz und Innovation: Kein Widerspruch

Wichtig ist jedoch, dass die Freiheit der Bürgerinnen und Bürger in Bezug auf Daten nicht als absolute Vermeidung von Datenerfassung oder -verarbeitung missverstanden wird. Die Perspektive der Marktkonvention legt auch beim Blick auf das Gemeinwohl Kompromisse mit der handwerklichen und staatsbürgerlichen Konvention nahe. Denn datengetriebene Innovationen bieten erhebliche Vorteile etwa im Bereich der medizinischen Forschung, der Automatisierung oder in der Qualität und Personalisierung digitaler Angebote. Ein allzu restriktiver Datenschutz, der datengetriebene Innovationen behindert, könnte langfristig negative wirtschaftliche Auswirkungen haben (Martin et al. 2019; Li et al. 2019). Studien verweisen indes auf eine gewisse Ambivalenz insofern, als die DS-GVO für Startups sowohl als Hemmnis wie auch als Innovationsförderer wirken kann. Während regulatorische Anforderungen oftmals Ressourcen binden und Markteintritte erschweren, bietet ein strikter Datenschutz gleichzeitig auch Chancen für neue, datenschutzfreundliche Geschäftsmodelle (Martin et al. 2019).

Aus Sicht der Marktkonvention ist in diesem Zusammenhang jedoch zu betonen: Ein datenschutzfreundliches Produkt darf nicht auf Kosten der Qualität oder Benutzerfreundlichkeit gehen, da es sich sonst am Markt nicht durchsetzen kann (Zhang et al. 2024). Dies bedeutet, dass Unternehmen eine Balance zwischen Datenschutz und Nutzungserlebnis finden müssen, um marktfähig zu bleiben (Zhang et al. 2024). Erfolgreiche digitale Geschäftsmodelle sollten Datenschutz nicht als Hindernis, sondern als

Chance begreifen, und diese idiosynkratische Fähigkeit bzw. „Ressource" (im Sinne von Barney et al. 2001) wird Unternehmen positiv von Mitbewerbern abheben.

3.4 Gleichgewicht zwischen Datenschutz, Innovation und Markt

Für Unternehmen bedeutet dies, einen wirtschaftlich sinnvollen und zugleich rechtlich und gesellschaftlich verantwortungsvollen Umgang mit Daten zu finden, der Transparenz gegenüber Nutzenden gewährleistet, ohne die Qualität oder den Nutzen der Produkte und Dienstleistungen einzuschränken. Die Entwicklung der erforderlichen Kompromisslinien zwischen handwerklicher (Vertrauen der Nutzenden), staatsbürgerlicher (Orientierung am Recht der DS-GVO, des Digital Services Act usw.) und der Marktkonvention stellt sich für Unternehmen dementsprechend als erhebliche Herausforderung dar. Ein standardisiertes Bewertungssystem für Unternehmen bzw. deren Produkte, das Datenschutzaspekte einfach und verständlich darstellt, könnte zur Entwicklung einer solchen Kompromisslinie beitragen, mithin sowohl Nutzende als auch Unternehmen stärken und digitale Freiheit so fördern. Ein solches System könnte folgende Maßnahmen umfassen:

- Einführung einer klaren und transparenten Kennzeichnung von Datenschutzstandards (z. B. Konformität mit geltenden Richtlinien und ggf. Nachweis der freiwilligen Erfüllung strengerer Standards).
- Entwicklung von Mechanismen, die Nutzenden eine informierte Entscheidung über die mögliche und tatsächliche Nutzung ihrer Daten erleichtern.
- Direkte oder indirekte Förderung von Unternehmen, die sich durch hohe Datenschutzstandards auszeichnen, um Vertrauen und Wettbewerbsfähigkeit zu stärken.

Wählt man die Marktkonvention als Ausgangspunkt, so zeigt sich schon hier, dass Freiheit und Selbstbestimmung in digitalen Infrastrukturen eine sinnvolle Balance zwischen Datenschutz, unternehmerischer Freiheit und marktwirtschaftlichen Anreizen voraussetzen. Einen der Schlüssel stellt eine Transparenzstrategie dar, die Nutzende befähigt, informierte Entscheidungen zu treffen, und Unternehmen die Möglichkeit gibt, Datenschutz als unternehmerische Chance und damit als potenziellen Wettbewerbsvorteil zu nutzen. Aus Sicht der Marktkonvention adressiert dies direkt das klas-

sische Problem asymmetrischer Informationen zwischen Marktteilnehmenden. Ganz im Sinne des ressourcenbasierten Ansatzes (Barney et al. 2001) werden einige Unternehmen diese Chance erfolgreich ergreifen und in innovative Geschäftsmodelle umwandeln können, während andere daran scheitern (Schumpeter 1942).

4. Freiheit und Selbstbestimmung aus Sicht der Industriekonvention: Die informatische Perspektive der IT-Sicherheit

Transparenz spielt auch im Bereich der IT-Sicherheit eine maßgebliche Rolle und bietet insofern ein gewisses Potential zur Verbindung von Markt- und Industriekonvention. Ganz grundsätzlich können Transparenz und Kontrolle aus Perspektive der Industriekonvention und ihrer Betonung von Plan- und Kontrollierbarkeit als Grundbausteine der Praktizierung von Freiheit und Selbstbestimmung in vernetzten Infrastrukturen gelten. Transparenz kann dabei auf verschiedenen Ebenen verortet und realisiert werden. Das Spektrum reicht von Open Source-Implementierungen (transparenter Softwarecode) bis zur Benutzeroberfläche (transparente Interfaces), die die Nutzer:innen über den Umgang mit und die Verarbeitung von Daten informieren. Ausgestattet mit den fraglichen Informationen können Nutzer:innen informierte Entscheidungen in Bezug auf Ihre Daten treffen. Solche Entscheidungen können unterschiedliche Konsequenzen haben, von der Wahl eines Dienstes und der darauffolgenden Anmeldung bis hin zur Außerbetriebnahme persönlicher vernetzter Gegenstände. Es wird in der digitalen Gesellschaft indes zunehmend fraglich, inwieweit Akteure noch Wahlfreiheit bzgl. der Nutzung best. Plattformen und Infrastrukturen haben, deutet indes schon an, dass die Industrie- genau wie die Marktkonvention bei der isolierten Problembehandlung an Grenzen stößt. Offene Standards und Transparenz schaffende Benutzeroberflächen können Zielgruppen unterstützen, so dass diese bei der Bewertung von Anwendungen und Diensten auf überprüfbare Produktinformationen zugreifen können. Wie der Fall der während der Covid19-Pandemie in Deutschland verwendeten Contact-Tracing Apps verdeutlicht (Steinbrink & Reuter 2024), kann die technologische Offenheit auch das Vertrauen von Nicht-Expert:innen in Technologie fördern – auch ausgehend von der Industriekonvention – stoßen wir somit wieder auf eine Verbindung mit der handwerklichen Konvention.

Folgerichtig verliert Transparenz aus Sicht der Industriekonvention tendenziell ihre Wirkung, wenn die Nutzer:innen über unzureichende oder gar keine Kontrolle über ihre Daten verfügen, und wenn keinerlei Nutzungsalternativen vorhanden sind. Der Umstand, dass die Abwesenheit von Nutzungsalternativen durch Quasi-Monopolisierung bestimmter Bereiche der digitalen Welt (Zuboff 2018), und die damit in Zusammenhang stehenden Macht-Asymmetrien (Liu 2024) bestehen bleiben, verweist auf die Notwendigkeit einer Verbindung der Industrie- mit der Markt- (Wettbewerb) und mit der staatsbürgerlichen Konvention (Regelwerke), um Selbstbestimmung weiter zu fördern: Praktische und nutzerfreundliche Lösungen müssen mit regulatorisch-kollektiv vereinbarten Prinzipien, wie etwa dem der Daten-Portabilität verzahnt werden, um sich in der Praxis durchzusetzen. Demgegenüber zeigt sich an der aktuellen Gestaltung von Cookie-Bannern umgekehrt, wie Transparenz und Kontrolle für Nutzende ineffizient gemacht werden kann (Matte et al. 2020).

4.1 Transparenzmaßnahmen

Die DS-GVO fordert, dass die betroffenen Personen über die Datenhandlungspraktiken in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ informiert sein sollten (Art. 12). Ob eine solche Maßnahme Erfolg verspricht, hängt indes auch von anderen Faktoren ab, denn die Kunst dürfte darin bestehen, in puncto Transparenz auch die richtigen Informationen, passend zum Wissensstand und Interesse der Personen, im richtigen Kontext (z. B. bei der Nutzung) in einem kompakten, aber dennoch verständlichen Format zu vermitteln. Um den damit verbundenen Aufwand für die Nutzer:innen zu minimieren, können standardisierte Formate entwickelt werden. Datenschutz-Kennzeichnungen (Privacy Labels) unterstützen beispielsweise schon jetzt im Sinne von Zertifikaten oder Standards den Vergleich von IoT-Geräten für Kaufinteressierte (Railean & Reinhardt 2018; 2021). Besonders im Stadium vor einer Kauf-Entscheidung besitzen die Kaufinteressierten eine Handlungsmöglichkeit in Bezug auf ihre Privatheit, wenngleich Kaufentscheidungen auch durch weitere Faktoren, wie etwa Ruf oder Preis beeinflusst werden (Lăzăroiu et al. 2020). Solche Vergleiche ruhen indes auf validen und vergleichbaren Daten über die verschiedenen Produkte, die zeitnah zur Verfügung gestellt werden sollten. Letzteres ist besonders wichtig für immer kurzlebigere Produktversionen, die von etablierten Zertifizie-

rungsstellen mit Blick auf den zeitlichen Aufwand, den Zertifizierungsprozesse erfordern, kaum noch angemessen bewertet werden können.

4.2 Kontrollmaßnahmen

Kontrollmechanismen können verschiedenen Form annehmen: von ganz Ausschalten bis zu fein-granularen Präferenzen (Ochs & Büttner 2018). Dennoch ergibt sich oftmals eine Abwägung zwischen Nutzbarkeit und Datensparsamkeit, die für Nutzer:innen nicht einfach vorzunehmen ist. So ist es etwa zum Beispiel immer noch schwierig, zu kontrollieren, wer Zugriff auf online geteilte Bilder in Sozialen Netzwerken bekommen sollte (Lowens et al. 2025). Unterstützend können demgegenüber aktuell in der Entwicklung befindliche Verfahren eingesetzt werden, um die Sensitivität von Bildern (Kqiku & Reinhardt 2024) oder Texten (Tillmann et al. 2023) vor deren Veröffentlichung abzuschätzen.

4.3 Mangelnde Unterstützung

Während bisher auf die Nutzenden abzielende Maßnahmen (Kaufentscheidung, Kontrollausübung) zur Förderung oder Ermöglichung von Freiheit und Selbstbestimmung im Sinne der Industriekonvention diskutiert worden sind, soll als nächstes eine andere Gruppe, namentlich die Hersteller, in den Blick genommen werden. Im Prinzip fordert die Transparenz-Anforderung deren aktiven Beitrag, bis hin zur Offenlegung ihrer Datensammlung und -verarbeitungen. Jedoch unterscheiden sich solche Offenlegungen zurzeit sehr stark hinsichtlich Form und Format. Trotz der in der DS-GVO getroffenen Regelungen sind wir von einem zufriedenstellenden Zustand weit entfernt. Alternativ zur Transparenz-Schaffung durch Offenlegung der Hersteller selbst, bietet sich die Entwicklung partizipativer Plattformen an, um so die Abhängigkeit von Herstellern zu minimieren und von der „Wisdom of the Crowd" zu profitieren (Hansen et al. 2025). Die derzeit in Entwicklung befindliche moderierte Plattform soll IoT-Nutzenden sowie Interessierten ermöglichen, Privacy-Tests sowie darauf basierende Privacy-Einstufungen für IoT-Produkte durchzuführen. Dies geschieht anhand verständlicher Metriken, transparenter Verfahren und nutzerzentrierter Werkzeuge. Zur Bündelung der Beiträge aus der Community kommen dabei standardisierte Testverfahren, strukturierte Vorlagen zur Dokumentation

sowie bereitgestellte Werkzeuge für die Bewertung Privacy-Eigenschaften von IoT-Produkten zum Einsatz. Zusammengeführt mit den Angaben von Anbieter (Hersteller, OEMs, Händler) werden die bereitgestellten Analysedaten kuratiert und in einer nutzerfreundlichen Form veröffentlicht, die deren Information und Vergleiche zwischen Geräte unterstützt. Die so zur Geltung gebrachte Industriekonvention muss allerdings auch an diesem Punkt Unterstützung durch die staatsbürgerliche erhalten, denn unverkennbar muss hier größerer Gesetzgebungsdruck auf die Hersteller ausgeübt werden, um nicht auf dem Niveau des heutigen Standes in puncto Transparenz (und in der Folge auch Selbstbestimmung) zu stagnieren.

4.4 Fehlende Messbarkeit

Kontrolle, *Privacy-by-Design*-Erfolge und Privatheit insgesamt sind schwer messbare Größen. Damit fehlen Skalen und Metriken, die die Problemlagen im Sinne der Industriekonvention verziffern würden (vgl. Diaz-Bone 2018) – oder auch könnten. Außer im Fall von *Differential Privacy* lässt sich der gebotene Schutz nicht mit mathematisch nachgewiesenen Garantien versehen. Zwar bauen die Konzepte der *k-anonymity*, *l-diversity* und *t-closeness* auf Metriken auf, eine „golden Zahl" der Sicherheitsgewährleistung gibt es jedoch nicht, weshalb Entwickler:innen die genannten Konzepte ebenso wie *Differential Privacy* als unsicher wahrnehmen (Kühltreiber et al. 2023). Für sonstige Metriken, die in der Literatur angewandt werden, wie zum Beispiel die bis zu einer Re-identifikation verstreichende Zeit oder Wahrscheinlichkeitsangaben ist es schwierig, verlässliche Benchmarks anzugeben (Christin et al. 2011, Wagner & Eckhoff 2018). Die Industriekonvention kommt hier insofern an Grenzen, als es sich um komplexe Schätzungen handelt, die umso voraussetzungsreicher werden, je mehr sie nicht bloß auf isolierte, zeitlich punktuelle „Datensilos", sondern auf mögliche Verknüpfungen über Anwendungen hinaus und über längere Zeitperioden bezogen werden.

4.5 Funktion als Priorität

Wie wichtig gerade die *Verknüpfung* der Industrie- mit anderen Konventionen ist, zeigt sich nicht zuletzt auch an den Problemen, die durch eine einseitige Priorisierung von Funktionalität heraufbeschworen werden:

Gemeinwohl-freundliche Design-Gesichtspunkte drohen dann hinter der einseitigen Fokussierung auf möglichst reibungslos und bequem verfügbare Funktionen zu verschwinden. Verstärkt wird dieser Effekt gegebenenfalls durch die Abwesenheit soziotechnischer Reflexionen auf die gesellschaftlichen Aspekte der Technikentwicklung, wie sie etwa in der Technikfolgenabschätzung vermittelt werden (Grunwald 2010) – Aspekte, die in der technischen Aus- und Weiterbildung eher ein Nischendasein fristen.

4.6 Privatheit & Sicherheit als Teil des Curriculums

Um der oftmals eher mangelhaften Bildung in ethischen und rechtlichen Fragen zu begegnen, wäre eine bessere Vermittlung von Privatheits- und ähnlich gelagerten Aspekten im Rahmen der beruflichen Qualifikation wünschenswert, um solchermaßen über die Stärkung menschlicher Kompetenzen den Einsatz bereits existierender Schutzmechanismen zu fördern. Auch wenn die Aufmerksamkeit für IT-Sicherheit in den letzten Jahren gewachsen ist, bleibt Privatheit oft auf der Strecke (Kühtreiber et al. 2023; 2025). In der Praxis folgen daraus mitunter Implementierungsprobleme, die allzu oft vermeidbar wären. Ein Beispiel dafür wäre etwa, dass Entwickler:innen zuweilen mehr Zugriffe auf Daten von Smartphone-Nutzer:innen fordern, weil sie grundlegende Prinzipien nicht verstanden haben (Tahaei et al. 2023).

5. Freiheit und Selbstbestimmung aus Sicht der staatsbürgerlichen Konvention: Die informatische Perspektive der Data Governance auf Datensouveränität

Organisationen spielen sowohl für die moderne Gesellschaft (Wagner 1994) als solche wie auch für Fragen des Datenschutzes eine zentrale Rolle (Rost 2013). Organisationen strukturieren Gesellschaften und verarbeiten dabei Daten. Sofern sie dabei Einzelpersonen zumindest potenziell über verbriefte Informationsschranken hinweg berechenbar zu machen drohen (BVerfG 1983), sind Regeln des kollektiven Umgangs mit Daten gefragt – wie oben bereits angeführt: „Gesetzliche Formen" (Boltanski & Thévenot 2007: 257) bzw. Regelwerke, kollektive Vereinbarungen usw. Eben solche Regelwerke werden im Bereich der *Data Governance* entwickelt.

Entsprechend des allgemeinen Trends haben in den letzten Jahren über personenbezogene Daten hinaus Daten aus einer Vielzahl von Kontexten

zum einen für Organisationen zunehmend an Bedeutung gewonnen, während sie zum anderen für grundrechtliche Fragen der Persönlichkeit vergleichsweise neuartige Probleme aufweisen (vgl. Roßnagel 2019). Dabei kann es sich um Daten aus Produktionsprozessen handeln, oder um Daten, aus denen sich der Zustand von technischen Komponenten, von natürlichen Ressourcen oder auch von Infrastruktur-Komponenten ablesen lässt. In solchen Kontexten den Austausch von Daten und Kooperationen zu fördern, ist das Ziel des Data Governance Acts. Neben den Anforderungen des Data Governance Acts bestehen Bereitstellungspflichten für Daten aus weiteren Rechtsakten. Viele Daten sind aus Sicht von Unternehmen als unternehmenskritisch anzusehen und stellen Geschäftsgeheimnisse dar, wie beispielsweise Informationen über Innovationen, betriebswirtschaftliche Daten und Kundendaten.

Im Folgenden werden exemplarische Kontexte und Szenarien der organisationalen Kooperation mittels Daten herausgearbeitet, bei denen nicht ausschließlich personenbeziehbare Daten betrachtet werden. Sie werden auf Implikationen für Data Governance und Datensouveränität untersucht.

5.1 Exemplarische Kontexte und Szenarien für die Chancen der Kooperation mittels Daten

Als Kontexte werden im Folgenden die Land- und Forstwirtschaft und der Bereich der Mobilität betrachtet. Ein Beispiel für die fragliche Sensorik ist die Erfassung von Daten über Fernerkundung mittels Drohnen, Satellitendaten oder vernetzte Sensorik (Jamshed et al. 2022), die Messwerte liefert. Zum Einsatz gebracht werden etwa bildgebende Verfahren und Sensorik zur Messung von Umgebungsparametern, wie bspw. Temperatur, Luftfeuchtigkeit oder CO_2-Gehalt, Bodenfeuchte und -temperatur.

Um auf Basis von Daten Aussagen machen zu können, ist es hilfreich zur Kontextualisierung GPS-Informationen einsetzen zu können und diese dann mit öffentlich verfügbaren Daten wie zum Beispiel Wetterdaten zu verknüpfen. Es ist für viele Use Cases sinnvoll, Aussagen über größere Regionen zu machen und dabei Sensor-Daten zu verknüpfen, um übergreifende Aussagen zu klimatischen Bedingungen oder Erträgen in der Land- und Forstwirtschaft zu treffen und verschiedene Regionen miteinander vergleichen zu können. Hierbei können auch Aussagen zur Einhaltung rechtlicher Rahmenbedingungen wie beispielsweise der Düngemittelverordnung abgeleitet werden. Im Sinne eines Geschäftsmodells für die Land- und

Forstwirtschaft können Indikatoren des EU *Nature Restauration Law* gemessen werden (Hering et al. 2023).

Durch den Einsatz von Sensorik ist es auch möglich, für Maschinen in einer Reihe von Kontexten und im Sinne der Predictive Maintenance Wartung proaktiv zu planen oder auch Optimierungen von Konfigurationen situativ vorzunehmen. Eine Voraussetzung dafür besteht darin, Daten mit Herstellern oder Service-Dienstleistern zu teilen (Tang et al. 2022).

Ein anderer Kontext, in dem Kooperation über Daten sinnvoll sein kann, ist der Mobilitätssektor. Zur Organisation multimodaler Mobilität ist es sinnvoll, aktuelle Informationen über eine ganze Reihe von Verkehrsmitteln für Nutzende zur Verfügung zu stellen und eine Kooperation zwischen Stakeholdern ist aus Sicht der Nutzenden hilfreich, um multimodale Mobilität zu optimieren.

Bei gemeinsam genutzter Infrastruktur wie Straßen oder Schienen bieten sich weitere Chancen der Kooperation über Daten. So könnten Fahrzeuge während des Einsatzes mittels Sensorik Zustandsinformationen über Verkehrswege sammeln und so eigens durchgeführte und entsprechend aufwändige Kontrollfahrten überflüssig machen. Bei derartigen Szenarien besteht die Herausforderung darin, dass die effiziente Erhebung der Daten und die Use Cases für die Nutzung der Daten bei verschiedenen Organisationen liegen (Alten et al. 2022).

5.2 Datensouveränität und Data Governance als Voraussetzung für Kooperationen

Die skizzierten Kooperationsmöglichkeiten werfen indes kollektiv zu verhandelnde Fragen auf: Wem gehören die Artefakte, über die Aussagen getroffen werden sollen? Wem gehört die Sensorik? Und wem gehören die erfassten Daten? Dabei kann es sich innerhalb der Szenarien sowohl um personenbeziehbare Daten als auch um unternehmenskritische Daten handeln. Zusätzlich dazu stellt sich die Frage, welche Implikationen mit der Weitergabe oder gemeinsamen Nutzung von Daten verbunden sind.

Den in den oben dargestellten Szenarien enthaltenen Chancen der Kooperation stehen somit Risiken gegenüber, die im Folgenden exemplarisch dargestellt werden sollen. Dabei zeigt sich zunächst insbesondere, dass eine Aussage zu Chancen und Risiken zur Kooperation mittels Daten immer im konkreten Kontext und aus der Perspektive unterschiedlicher Stakeholder getroffen werden muss: Chancen und Risiken müssen in dem Sinne kon-

textspezifisch identifiziert und analysiert werden, um zu verstehen, warum Kooperationen über Daten in bestimmten Kontexten nicht oder nur sehr eingeschränkt umgesetzt werden.

Exemplarische Risiken aus Sicht der Stakeholder sind dabei etwa, dass Daten Informationen zu rechtlichen Rahmenbedingungen oder steuerlich relevanten Aspekten beinhalten. Das ist beispielsweise in der Land- und Forstwirtschaft der Fall, in der potenziell Aussagen zur Einhaltung von rechtlichen Rahmenbedingungen wie der Düngemittelverordnung getroffen werden könnten. In der Forstwirtschaft sind auf Basis einer Einschätzung und Prognose des Bestandes im Rahmen der Forsteinrichtung steuerlich relevante Aussagen über den Betrieb ableitbar (Pleger & Schiering 2023). Da mittels Sensorik insbesondere Aussagen über betriebswirtschaftliche Parameter von Betrieben getroffen werden können, werden von den Stakeholdern häufig dezentrale Architekturen bevorzugt (Bökle et al. 2025). Chancen durch die Kooperation ergeben sich für land- und forstwirtschaftliche Betriebe, wenn durch den Nachweis von Indikatoren, wie beispielsweise des EU Nature Restauration Law (Hering et al. 2023), neue Geschäftsmodelle ermöglicht werden.

In Use Cases aus dem Bereich des Verkehrs wie der besseren Organisation Multimodaler Mobilität ergeben sich aus der datenbasierten Kooperation Chancen für alle Stakeholder. Eine Kooperation ist beispielsweise über Ansätze wie Mobility Data Spaces möglich (Preetzsch et al. 2022). Bei Ansätzen wie der Streckenüberwachung durch Regelfahrten im Schienenverkehr (Alten et al. 2022) besteht die Herausforderung, dass die Betreiber der Schienenfahrzeuge und die Streckenbetreiber typischerweise zu verschiedenen Organisationen gehören und so zunächst Modelle der Kooperation entwickeln müssen.

Kooperation und Datenaustausch zwischen Organisationen bleibt somit eine Herausforderung, der mittels kollektiver Spielregeln zu begegnen ist – und zwar über die hier exemplarisch behandelten Felder hinaus. Die Datenethikkommission der Bundesregierung (2019, S. 146) nennt dabei insbesondere Transparenz, die gegenseitige Achtung von Geschäftsinteressen und die Minimierung der Datenabhängigkeit von Anbietern im Sinne eines Daten-Lock-In als Grundprinzipien für einen Datenaustausch zwischen Unternehmen. Interview-Studien haben zudem als Herausforderungen für die Implementierung von Datensouveränität insbesondere die Etablierung von Vertrauensmechanismen und die effektive Umsetzung von Zugriffsbeschränkungen auf die Daten, die sich über die Zeit an neue Anforderungen adaptieren lassen, herausgearbeitet (z. B. Hellmeier et al. 2023). In

einer empirischen Studie von Pampus et al. (2024) wurden zudem Anforderungen an die technische Umsetzung von Datensouveränität untersucht. Im Vordergrund stehen hier nach Aussagen der befragten Institutionen Schutzziele, die weitgehend mit den Gewährleistungszielen im Datenschutz übereinstimmen (Hansen et al. 2015). Wie hier erkennbar wird, lassen sich Methoden des Privacy by Design im Bereich der Data Governance und Datensouveränität sinnvoll einsetzen, um Anforderungen von Organisationen für datenbasierte Kooperationen effektiv zu adressieren. Die Perspektive der staatsbürgerlichen Konvention eröffnet so die Möglichkeit zur kollektiven Aushandlung von Kompromisslinien (Transparenz, Vertrauen) und des Umgangs mit Widersprüchen (Datenabhängigkeit, Lock-In).

6. Freiheit und Selbstbestimmung aus Sicht der handwerklichen Konvention: Die techniksoziologische Perspektive der Mensch-Computer-Interaktion

Bei der Beurteilung von Privatheitsrisiken und den übergeordneten Fragen nach Freiheit und Selbstbestimmung gilt es aus Sicht einer soziologisch informierten Mensch-Computer-Interaktion-Forschung zunächst grundlegend zu beachten, dass die Praktiken, Orte und Kontexte der tatsächlichen Verwendung von vernetzten Gegenständen und Webservices durchaus eigensinnig und auch widersprüchlich sind. Zwar lässt sich weltweit eine fortschreitende, und in ihren Produkten und Services in gewisser Weise auch gleichförmige Vernetzung und Verdatung im Grunde aller Lebensbereiche feststellen – dennoch sind insbesondere die Sphäre des Zuhauses und die Auswirkungen dieser Vernetzung auf Selbstbestimmung in diesem Geflecht so heterogen, wie untererforscht. Gerade weil Services wie Apps, Smart-Home-Geräte oder VR-Angebote durch den Endverbraucher-Konsum als (vermeintlich) individuelle Kaufentscheidungen in diese Lebenswelten gelangen, ergibt sich eine problematische Ausgangslage: Ein besonders sensibler Raum wird durch Verwertungslogiken und -mechanismen durchdrungen, die der dort herrschenden Beziehungslogik des Vertrauens widersprechen – Markt- und Industriekonvention drohen in Widerspruch zur handwerklichen Konvention zu geraten.

6.1 Gefährdungsquellen

Nutzungs- und Sensordaten aus dem privaten Zuhause sind zwangsläufig sozial situiert. Sie sind also einerseits von je konkreten Umständen geprägt

und unter diesen entstanden, und sie werden andererseits auch unter Hinzuziehung des Alltagswissens der Nutzer:innen – und damit der sozialen und moralischen Ordnungen vor Ort – interpretiert und bewertet (vgl. z. B. Fischer, et al. 2016; Tolmie, et al. 2016). Datenspuren zu Luftfeuchtigkeit im Kinderzimmer oder vom automatischen Schließsystem der Haustür sind per se sensibel – auch und gerade innerhalb von Haushalten (Kurze et al. 2020). Eine soziale Kontextualisierung vermeintlich objektiver Werte lässt vermeintlich harmlose Sensor- oder Nutzungsdaten kritisch werden (Richter et al. 2018). Dabei können die Implikationen für Individuen und soziale Verbände wie Familien enorm sein. Der Missbrauch vernetzter Services kann sogar häusliche Gewalt befördern, weil es durch smarte Geräte mehr Möglichkeiten gibt, Opfer „zu verfolgen, zu beobachten und zu regulieren." (Tanczer 2021) Vertrautheit gegenüber einem Endgerät, Bedienungsmuster oder Hersteller kann also gerade zur Gefahr für Freiheit und Selbstbestimmung in digital vernetzten Lebenswelten werden – Vertrauen in den verantwortungsvollen Gebrauch durch die Person im Haushalt, die das Gerät oder den Service kontrollieren kann, ebenso.

6.2 Das Privacy Paradox

Warum und wie kommen Geräte und Services mit so vielen ‚offenen Enden' dennoch so leicht und vielgestaltig in die besonders schützenswerte Sphäre des Zuhauses? In der Literatur wurde diese Frage lange Zeit mit der Erklärungsfigur des „Privacy Paradox" bezeichnet, demzufolge die diskursiv geäußerten Einstellungen der Nutzer:innen gegenüber Dingen wie Privatheit und Sicherheit in Diskrepanz zu ihren tatsächlichen diesbezüglichen Praktiken stehen würden (bspw. Rösler 2022). Erklärungen hierfür liefern Studien, die empirisch nachweisen, dass Nutzer:innen oftmals den Wunsch nach „Convenience", also nach Bequemlichkeit, gegenüber Privatsphärebedenken abwägen: Datengetriebene Produkte und Services versprechen Verbraucher:innen mehr Komfort, Sicherheit und Effizienz im Alltag, und insbesondere Nutzungsmotive, wie die allzeitige Verfügbarkeit haben sich hierbei als starker Motivator in der Abwägung gegen Privatheitsrisiken gezeigt (Gashami et al. 2016). Bei einem Smart-TV etwa lassen sich alle Unterhaltungsquellen und -inhalte mit einer Fernbedienung steuern, dem steht die von den Nutzer:innen nicht gern gehörte Tatsache gegenüber, dass das Gerät Daten über das Nutzungsverhalten aufzeichnet. Während also tief in der „Welt des Hauses" verankerte Bequemlichkeitsmotive die

Nutzung prägen, lässt sich gerade dies datenökonomisch ausbeuten – die Marktkonvention okkupiert gewissermaßen die handwerkliche.

In ähnlicher Weise kann dann auch das an der Marktkonvention orientierte Marketing normative Subjektpositionen, wie bspw. die Adressierung von Eltern, ausnutzen – etwa, wenn diesen das Wissen darum schmackhaft gemacht wird, was ihre Kinder gerade tun, um sie so vor Gefahren schützen zu können (Stark & Levy 2018). Studien zeigen darüber hinaus, dass Verbaucher:innen oft unzutreffende mentale Modelle von digitalen Daten in Produkten haben (Marky et al. 2021). Insbesondere der grundlegende Zusammenhang datafizierter Services – dass durch Tracking und Datenanalyse das Verhalten der Nutzer:innen selbst zur Ware wird – ist wenig bekannt. Dieser ökonomische Nutzen für die Anbieter:innen wird den Verbraucher:innen gegenüber teils bewusst verschleiert, womit letztere dann wiederum exklusiv oder vordringlich Gebrauchstauglichkeits-, Bequemlichkeits- oder Unterhaltsamkeitsgesichtspunkte ihren Bewertungen zugrunde legen. Für die weiter oben unter der Rubrik der Marktkonvention behandelte Forderung, Datenschutzgesichtspunkte zum Wettbewerbskriterium zu machen, sieht es damit eher schlecht aus.

6.3 Maßnahmen aus Sicht der handwerklichen Konvention

Hier tut sich nun wiederum eine Kompromisslinie zwischen Markt-, Industrie- und handwerklicher Konvention auf, sofern auch aus Sicht letzterer ein grundlegender Schritt in der Ermöglichung und Stärkung von Selbstbestimmung beim Gebrauch vernetzter Geräte und Services in der Herstellung von Transparenz besteht. Die geforderte Transparenz lässt sich dabei in verschiedenen Richtungen hin ausdifferenzieren als Transparenz dahingehend, a) dass Daten erfasst werden, b) um welche Daten genau es sich handelt, c) wohin diese übertragen werden, d) wie sie weiterverarbeitet, zusammengeführt und ausgewertet werden – und e) von wem mit welcher Absicht. Verständliche diesbezügliche Darlegungen, z. B. durch klare Auszeichnung auf Produktverpackungen o. ä. fehlen. Selbst einfache Sensorik im Zuhause wird dadurch leicht zum „versteckten Internet“ (Karaboga et al. 2015). Die Risiken und Implikationen smarter Geräte, die Video und/oder Audio erfassen können, wie etwa „intelligente Lautsprecher“, werden zwar zunehmend kritisch thematisiert, auch und vor allem hinsichtlich von Fragen zur Privatheit; im Gegensatz dazu ist jedoch insbesondere im öffentlichen Diskurs ein mangelndes Problembewusstsein und Verständnis

für Risiken und Implikationen für Privatheit durch vermeintlich einfache Sensor- und Nutzungsdaten festzustellen. Daran wird ersichtlich, dass Transparenz allein hier nicht mehr ausreicht, vielmehr bedarf es auch einer aktiven Aufklärung über mögliche privatheitsunfreundliche Implikationen durch solche Services und Geräte, die erst in der Nutzung in der Sphäre des Zuhauses entstehen (vgl. auch Karaboga et al. 2022).

Während Einstellungen, Erwartungen und Informationsdefizite durch Erhebungen wie Umfragen oder Interviews rekonstruiert werden können, sind die angesprochenen Risiken und Implikationen, die überhaupt erst in der Nutzung entstehen, schwerer zu verstehen und im Sinne eines auf Selbstbestimmtheit ausgerichteten Verbraucherschutzes zu bearbeiten. Das vom BMBF geförderte Projekt „Simplications" verfolgt deswegen einen kombinierten Ansatz aus partizipativer Forschung und der Gestaltung von Bildungsangeboten. Dem etablierten Ansatz des Privacy by Design (Schaar 2010) wird so „Privacy by Co-Design" als partizipatives Element hinzugefügt. Ausgangspunkt ist dabei der unmittelbare lebensweltliche Bezug zu den unterschiedlich situierten Formen von Privatheit im Zuhause: Verbraucher:innen erhalten über einen längeren Zeitraum ein „Sensorkit", das typische Smart-Home-Daten wie Luftfeuchtigkeit, Temperatur, Bewegung oder Lautstärke aufzeichnet; sie werden durch kleinere Aufgaben angehalten, die ihnen einsehbaren Daten mit Alltagsbegebenheiten in Beziehung zu setzen. In einer abschließenden Gruppendiskussion werden anonymisierte Datenspuren aus verschiedenen Haushalten gemeinsam betrachtet, und auf mögliche Kontexte und Implikationen zurückgeführt. Durch diese soziale Situierung anhand echter Daten wird ein Aufdecken und Adressieren der wirklich relevanten Problemstellungen aus der Praxis der Verwendung heraus möglich – was insbesondere abweichende und nicht-intendierte Nutzungen, bis hin zum potenziellen Missbrauch, sichtbar und damit im Rahmen von Verbraucherschutz und zukünftigen Designparadigmen adressierbar macht (Kurze et al. 2020). Den Schlusspunkt der handwerklichen Konventionsperspektiven bildet somit konsequenterweise die veränderte Gestaltung der „Welt des Hauses" – eine handwerkliche Antwort auf die Frage nach Freiheit und Selbstbestimmung in digitalen Infrastrukturen.

7. Schluss: „Free Expression" - Meinungsfreiheit über alles? Einige Differenzierungen zur Qualitätserhöhung der Kontroverse um Freiheit und Selbstbestimmung in soziodigitalen Infrastrukturen

Wie eingangs angemerkt, ist der vorliegende Text aus einem Diskussionspanel der Jahreskonferenz 2024 der Plattform Privatheit hervorgegangen. Im Panel, wie auch im Beitrag wurden heterogene, z. T. altbekannte Stimmen und Ansichten hörbar. Die Sortierheuristik der Konventionenökonomie hat ein relativ kohärentes Einfangen dieser Heterogenität ermöglicht, das darauf hinausläuft, nicht ein Einzelargument oder eine Einzelperspektive zur Geltung zu bringen, sondern vielmehr Pluralismus im gesellschaftlichen Zusammenhang pflegt. Was lässt sich nun aber aus der Zusammenschau der unterschiedlichen Perspektiven auf das Thema „Freiheit in digitalen Infrastrukturen" über die Kontroverse um die Gestaltung der digitalen Gegenwartsgesellschaft lernen?

- Zunächst werden mögliche *Kompromisslinien* erkennbar. Der immer wieder anzutreffende Verweis auf Transparenz legt nahe, dass es sich hierbei um ein von allen beteiligten Welten als erstrebenswert erachtetes „Gut" handelt, womit die weitere Forschung und Auseinandersetzung darum jedoch erst beginnt: Inwiefern, so wäre zu fragen, ermöglicht Transparenz wem welche Freiheit? Wie sich andeutete, halten einige die Intransparenz von technoökonomischen Plattformen für problematisch, wie wäre hierauf zu reagieren? Setzt Freiheit in soziodigitalen Infrastrukturen die Verordnung von Transparenzpflichten voraus? Nicht zufällig thematisieren Artikel 12 Absatz 7 und 8 der DS-GVO unter der Überschrift „Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person" ausdrücklich die Möglichkeit, die Wahrnehmung von Auskunftsrechten mithilfe von Bildsymbolen zu ermöglichen. Aber sind die Transparenzprobleme damit gelöst? Zwar können Bildsymbole ggf. der Überforderung (durch zu viele und zu komplex dargelegte Informationen als Entscheidungsgrundlage) von Nutzenden entgegenwirken. Aber wie nützlich ist Transparenz, wenn diese Nutzenden in quasi-monopolisierten digitalen Umgebungen agieren und folglich effektiv nicht wirklich über Handlungsalternativen verfügen? Und wie realistisch ist eine Porträtierung der Nutzenden im Sinne von individuellen Entscheidungsträger:innen überhaupt? Droht Transparenz unter den gegebenen Umständen folglich dahingehend zum „faulen Kompromiss" zu verkommen, dass sich die an der Kontroverse

Beteiligten rhetorisch darauf einigen können, ohne dass der praktische Status Quo und damit zusammenhängende Machtasymmetrien deswegen transformiert würden?[7]

- Zum zweiten macht die oben dokumentierte Zusammenschau deutlich, dass die Ermöglichung von Freiheit und Selbstbestimmung in soziodigitalen Infrastrukturen ein *Zusammenwirken unterschiedlicher Konventionen* voraussetzt. Wenn die Umsetzung der DS-GVO als Wettbewerbsvorteil genutzt werden kann, dann wirkt die Marktkonvention mit der staatsbürgerlichen zusammen, wenn in puncto Privatheitsfreundlichkeit das „race to the bottom" durch ein „race to the top" ersetzt wird, indem dieses durch den Einsatz von Standards und Metriken begünstigt wird, dann verknüpft sich die Konstellation zusätzlich mit der Industriekonvention usw. Daran wird erkennbar, dass *gesellschaftlich* produktive soziodigitale Infrastrukturen, von denen nicht bloß ein paar wenige Tech-Konzerne profitieren, ein höheres Maß an intelligenter Konventionen-Abstimmung erforderlich machen, als es das plumpe Propagieren eines einzigen Prinzips (etwa der „free expression") vorsieht.
- Drittens wird jedoch auch deutlich, dass Konventionen zuweilen gegenläufig zueinander und in unaufhebbaren *wechselseitigen Widerspruch* geraten können. Dies zeigte sich etwa an der Gefahr, dass die „Welt des Hauses" – die auf Vertrauensverhältnissen fußende, historisch ausdifferenzierte lebensweltliche Privatsphäre – von datenökonomischen Motiven durchdrungen wird. Die hier in neuem, digitalen Gewand sich artikulierende Sorge ist eine soziologisch betrachtet alte und findet sich etwa schon in Jürgen Habermas' bekannter Diagnose einer „*Kolonisierung der Lebenswelt*": „die Imperative der verselbstständigten Subsysteme dringen (…) *von außen* in die Lebenswelt – wie die Kolonialherren in eine Stammesgesellschaft – ein und erzwingen die Assimilation" (Habermas 1981: 522). Die Imperative, um die es weiter oben ging, sind offenkundig die des „Subsystems" der Marktwirtschaft, ganz grundsätzlich stellt sich aber die Frage, wo und an welchen Stellen Konventionen eben nicht in ein kompromisshaftes oder kooperatives Verhältnis zueinander gebracht werden können oder sollten, sondern sich wechselseitig ausschließen. Das heißt mitunter, dass eine Konvention nur auf Kosten der anderen zum Zuge kommen kann, weshalb die eine oder andere in ihrer Geltung

7 Für Hinweise auf die fraglichen Artikel der DS-GVO und auf die Relevanz „echter Handlungsalternativen" in Bezug auf die Transparenzthematik bedanken wir uns bei Michael Friedewald und Christian Geminn.

begrenzt werden muss.[8] Demokratische Gesellschaften könnten die gesellschaftlichen Aushandlungsspielräume an dieser Stelle normativ durch Prinzipien begrenzen, die die Wahrscheinlichkeit der Reproduktion demokratischer Spielregeln erhöhen – im Zweifel zugunsten der Demokratie.

Als generellen Befund, der sich gewissermaßen oberhalb der Frage einstellt, ob die verschiedenen Wertkonventionen in soziotechnischen Kontroversen, Konstellationen und Situationen in Kompromiss-, Kooperations- oder Widerspruchsverhältnisse treten, können wir somit wenigstens eine Gewissheit festhalten: Die Vielfalt des Wertepluralismus muss sich in den gesellschaftlichen Aushandlungen der soziotechnischen Transformation auch dann artikulieren, wenn Wertkonventionen in Widerspruch zueinander stehen – aus empirischer Sicht sind unterschiedliche Konventionen in demokratischen Gemeinwesen immer miteinander zu vermitteln. Denn die Unterordnung der Gestaltung soziotechnischer Infrastrukturen unter ein einziges Prinzip ist weder moralisch, ethisch oder politisch zu rechtfertigen noch dürfte sie mittelfristig funktionieren. Beispielsweise benötigt die Marktkonvention die staatsbürgerliche, andernfalls droht sie von ihrem eigenen Prinzip gewissermaßen „aufgefressen" zu werden, die unumschränkte Herrschaft von Markt-Prinzipien in sämtlichen Lebensbereichen würde Gesellschaften in die Dysfunktionalität treiben, so dass auch die Marktkonvention ihrer eigenen Existenzgrundlage beraubt wäre.

In diesem Sinne ziehen wir bei aller Kakophonie, die die am vorliegenden Artikel beteiligten Disziplinen bzw. Autor:innen in die Kontroverse einbringen, gemeinsam das Fazit: Die Ermöglichung von Freiheit und Selbstbestimmung in soziodigitalen Infrastrukturen benötigt weit mehr, als das einseitige Abstellen auf eine Idee der „free expression", die allzu oft weniger demokratische Diskurse hervorbringt, als eine algorithmische Privilegierung von Propaganda und extremistische Hetze, und genau des-

8 In Habermas'scher Diktion: „Der normative Sinn von Demokratie läßt sich gesellschaftstheoretisch auf die Formel bringen, daß die Erfüllung der funktionalen Notwendigkeiten systemisch integrierter Handlungsbereiche an der Integrität der Lebenswelt (…) ihre Grenze finden soll. Andererseits kann die kapitalistische Eigendynamik des Wirtschaftssystems nur in dem Maße gewahrt bleiben, wie der Akkumulationsprozeß von Gebrauchswertorientierungen abgekoppelt wird. Der Antriebsmechanismus des Wirtschaftssystems muß von lebensweltlichen Restriktionen möglichst freigehalten werden." (Habermas 1981: 507; dass Habermas das Konzept der „Lebenswelt" nicht bloß auf die „Welt des Hauses" bezieht und generell mit anders gelagerten Unterscheidungen arbeitet, klammern wir in unserer Betrachtung bewusst aus).

halb auch allzu oft als bloß strategisch in Anschlag gebrachte Rhetorik daherkommt. Demgegenüber stellen sich Freiheit und Selbstbestimmung in digitalen Infrastrukturen nur dann ein, wenn sie als Resultat der gesellschaftlichen Aushandlung unterschiedlichster Wertkonventionen Gestalt annehmen.

Literatur

Akanfe, Olulawafemi; Lawong, Diane und Rao, Raghav (2024): Blockchain technology and privacy regulation. Reviewing frictions and synthesizing opportunities. *International Journal of Information Management*, 76, doi: 10.1016/j.ijinfomgt.2024.102753.

Alten, Karoline et al. (2022). Zustandsüberwachung mit Regelfahrzeugen. *EIK-Eisenbahn Ingenieur Kompendium*, S. 111–127.

Bakos, Yannis; Marotta-Wurgler; Florencia und Trossen, David R. (2014): Does anyone read the fine print? Consumer attention to standard-form contracts. *The Journal of Legal Studies*, 43(1), S. 1-35.

Barney, Jay; Wright, Mike und Ketchen, David. J. (2001): *The resource-based view of the firm: Ten years after 1991*. Journal of Management, 27(6), S. 625-641.

Benkler, Yochai (2006): *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. New Haven, London: Yale University Press.

Benkler, Yochai; Faris, Robert und Roberts, Hal (Hrsg.) (2018): *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford: Oxford University Press.

Bier, Christoph; Kühne, Kay und Beyerer, Jürgen (2016): PrivacyInsight: The next generation privacy dashboard. In: Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K. (Hrsg.): Privacy Technologies and Policy. Cham: Springer, S. 135–152. https://doi.org/10.1007/978-3-319-44760-5_9

Bökle, Sebastian, et al. (2025). A concept of a decentral server infrastructure to connect farms, secure data, and increase the resilience of digital farming. *Smart Agricultural Technology*, 10, 100701. https://doi.org/10.1016/j.atech.2024.100701

Boltanski, Luc und Thévenot, Laurent (2007): *Über die Rechtfertigung. Eine Soziologie der kritischen Urteilskraft*. Hamburg: Hamburger Edition.

Boltanski, Luc und Thévenot, Laurent (2011): Die Soziologie der kritischen Kompetenzen. In: Diaz-Bone, Rainer (Hrsg.): *Soziologie der Konventionen. Grundlagen einer pragmatischen Anthropologie*. Frankfurt/M.: Campus, S. 43-68.

BVerfG (1983): *Bundesverfassungsgericht, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 1-215, ‚Volkszählungsurteil'*, Bundesverfassungsgericht 2022, https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/DE/1983/12/rs19831215_1bvr020983.pdf?__blob=publicationFile&v=1 (Zugriff: 13.10.2022).

Callon, Michel (1986): Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay. In: Law, John (Hrsg.): *Power, Action and Belief. A New Sociology of Knowledge?*, London: Routledge & Paul, S. 196–233.

Castells, Manuel (1996): *The Rise of the Network Society*. Cambridge, Mass. et al.: Blackwell.

Christin, Delphine; Reinhardt, Andreas; Kanhere, Salil S. und Hollick, Matthias (2011): A survey on privacy in mobile participatory sensing applications. *Journal of Systems and Software*. doi:10.1016/j.jss.2011.06.073

Crawford, Kate (2024): *Atlas der KI. Die materielle Wahrheit hinter den neuen Datenimperien*. München: C.H. Beck.

Datenethikkommission der Bundesregierung (2019): *Gutachten der Datenethikkommission*. Berlin: BMJV. https://datenethikkommission.de/wp-content/uploads/191128_DEK_Gutachten_bf_b.pdf

Diaz-Bone, Rainer (Hrsg.) (2011): *Soziologie der Konventionen. Grundlagen einer pragmatischen Anthropologie*. Frankfurt/M.: Campus.

Diaz-Bone, Rainer (2018): *Die „Economie des conventions": Grundlagen und Entwicklungen der neuen französischen Wirtschaftssoziologie*. 2. Auflage. Wiesbaden: Springer VS.

Dourish, Paul und Anderson, Ken (2006): Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human–Computer Interaction*, 21(3), S. 319–342.

Eubanks, Virginia (2018): *Automating Inequality. How High-Tech Tools Profile, Police, and Punish the Poor*. New York: Picador, St Martin's Press.

Fischer, Joel E et al. (2016): "Just whack it on until it gets hot": Working with IoT data in the home. *2016 CHI Conference*. https://doi.org/10.1145/2858036.2858518.

Fox, Grace; Lynn, Theo und Pierangelo, Rosati (2022): Enhancing consumer perceptions of privacy and trust: a GDPR label perspective. *Information Technology & People*, 35(8), S. 181-204. https://doi.org/10.1108/ITP-09-2021-0706

Gashami, Jean Pierre; Chang, Luke Y.; Rho, Jae Jeung und Park, Myeong Cheol (2016): Privacy concerns and benefits in SaaS adoption by individual users: A trade-off approach. *Information Development*, 32(4), S.837-852.

Grunwald, Armin (2010): *Technikfolgenabschätzung – eine Einführung.* 2. Auflage. Berlin: edition sigma.

Habermas, Jürgen (1981): *Theorie des kommunikativen Handelns. Band 2: Kritik der funktionalistischen Vernunft.* Frankfurt am Main: Suhrkamp.

Hamilton, R. H; Sodeman, William A. (2020): The questions we ask: Opportunities and challenges for using big data analytics to strategically manage human capital resources. *Business Horizons*, 63(1), S.85–95.

Hansen, Marit; Lo Iacono, Luigi; Reinhardt, Delphine und Zwingelberg, Harald (2025). Vergleichbare Transparenz von IoT-Privatheitseigenschaften. *Datenschutz und Datensicherheit-DuD*, 49(7), S. 425-430. https://doi.org/10.1007/s11623-025-2115-2

Hansen, Marit; Jensen, Meiko und Rost, Martin (2015): Protection Goals for Privacy Engineering. *2015 IEEE Security and Privacy Workshops* (SPW), San Jose, CA: IEEE, S. 159–166. https://doi.org/10.1109/SPW.2015.13

Hartmann, Phillip; Zaki, Mohamed; Feldmann, Niels und Neely, Andy (2016): Capturing value from big data – A taxonomy of data-driven business models used by start-up firms. *International Journal of Operations & Production Management*, 36(10), S. 1382–1406. doi:10.1108/IJOPM-02-2014-0094.

Hellmeier, Max; Pampus, Jonas; Qarawlus, Haydar und Howar, Falk (2023): Implementing Data Sovereignty: Requirements & Challenges from Practice. *Proceedings of ARES 2023*, Article 143, S. 1–9. doi:10.1145/3600160.3604995

Hering, Daniel et al. (2023): Securing success for the Nature Restoration Law. *Science*, 382(6676), S. 1248–1250. doi:10.1126/science.adk1658.

Jamshed, Muhammad A. et al. (2022): Challenges, Applications, and Future of Wireless Sensors in Internet of Things: A Review. *IEEE Sensors Journal*, 22(6), S. 5482–5494. doi:10.1109/JSEN.2022.3148128.

Kqiku, Lindrit und Reinhardt, Delphine (2024): SensitivAlert: Image Sensitivity Prediction in Online Social Networks Using Transformer-Based Deep Learning Models. *Proceedings of the International AAAI Conference on Web and Social Media*, 18(1), S. 851-864.

Karaboga, Murat et al. (2015): Das versteckte Internet: Zu Hause - Im Auto - am Körper. White Paper. Karlsruhe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. doi:10.24406/publica-fhg-297401.

Karaboga, Murat et al. (2022): Automatisierte Erkennung von Stimme, Sprache und Gesicht: Technische, rechtliche und gesellschaftliche Herausforderungen. Zürich: vdf Hochschulverlag (TA-SWISS, 79/2022). doi:10.3218/4141-5.

Kurze, Albrecht et al. (2020): Guess the Data: Data Work to Understand How People Make Sense of and Use Simple Sensor Data from Homes. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (CHI '20), S. 1–12. doi:10.1145/3313831.3376273

Kühtreiber, Patrick; Pak, Viktoriya und Reinhardt, Delphine (2023): "A method like this would be overkill": Developers' perceived issues with privacy-preserving computation methods. *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, S. 1041–1048. doi:10.1109/TrustCom58943.2023.00138.

Kühtreiber, Patrick; Heimermann, Sabrina; Schillinger, S.; Reinhardt, Delphine (2025): "We've Met Some Problems": Developers' Issues with Privacy-Preserving Computation Techniques on Stack Overflow. *IFIP International Conference on ICT Systems Security and Privacy Protection*, S. 47–60. Doi:10.1007/978-3-031-92882-6_4

Lăzăroiu, George et al. (2020): Consumers' decision-making process on social commerce platforms: Online trust, perceived risk, and purchase intentions. *Frontiers in Psychology*, 11, S. 890.

Li, He; Lu, Yu und Wu,He (2019): The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management,* 22(1), S. 1–6. https://doi.org/10.1080/1097198X.2019.1569186

Liu, Michelle (2024): Digital vulnerability: Rethinking power imbalances in the digital age. European Review of Private Law, 32(5), S. 827–48. doi:10.54648/erpl2024043.

Lovink, Geert (2017): *Im Bann der Plattformen. Die nächste Runde der Netzkritik*. Bielefeld: transcript.

Lowens, Byron et al. (2025): Misalignments and demographic differences in expected and actual privacy settings on Facebook. *Proceedings on Privacy Enhancing Technologies*, 2025(1), S. 456–471. doi:10.56553/popets-2025-0025.

Marky, Karola; Prange, Sarah; Mühlhäuser, Max und Alt, Florian (2022): Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. In: *Proceedings of the 20th International Conference on Mobile and Ubiquitous Multimedia* (MUM '21), S. 108–122. doi:10.1145/3490632.3490664.

Marres, Noortje (2007): The Issues Deserve More Credit: Pragmatist Contributions to the Study of Public Involvement in Controversy. *Social Studies of Science*, 37(5), S. 759–780.

Martin, Nicholas; Matt, Christian; Niebel, Crispin und Blind, Knut (2019): How data protection regulation affects startup innovation. *Information Systems Frontiers*, 21(5), S. 1307–1324.

Matte, Célestin; Bielova, Nataliia und Santos, Christiana (2020): Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework. *IEEE Symposium on Security and Privacy (SP)*, S. 791–809.

Obar, Jonathan A. und Oeldorf-Hirsch, Anne (2020): The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, 23(1), S. 128–147.

Ochs, Carsten (2022): *Soziologie der Privatheit. Vom Reputation Management bis zum Recht auf Unberechenbarkeit*. Weilerswist: Velbrück Wissenschaft.

Ochs, Carsten (2024): *Deep Targeting*: Zur Steigerung der Eingriffstiefe in die Erfahrungsspielräume des Sozialen. *Zeitschrift für Soziologie*, 53(1), S. 73–88.

Ochs, Carsten und Büttner, Barbara (2018): Das Internet als 'Sauerstoff' und 'Bedrohung': Privatheitspraktiken zwischen analoger und digital-vernetzter Subjektivierung. In: Friedewald, Michael (Hrsg.): *Privatheit und selbstbestimmtes Leben in der digitalen Welt. Interdisziplinäre Perspektiven auf aktuelle Herausforderungen des Datenschutzes*. Wiesbaden: Springer VS, S. 33–80.

Palen, Leysia und Dourish, Paul (2003): Unpacking "privacy" for a networked world. *CHI '03: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, S. 129-136.

Pampus, Jonas und Heisel, Matthias (2024): An Empirical Examination of the Technical Aspects of Data Sovereignty. *Proceedings of the 19th International Conference on Software Technologies - ICSOFT*, SciTePress, S. 112–122. doi:10.5220/0012760600003753.

Pfeiffer, Sabine (2021): *Digitalisierung als Distributivkraft. Über das Neue am digitalen Kapitalismus*. Bielefeld: transcript.

Pleger, Michael und Schiering, Ina (2023): Digital Transformation in Forestry - Stakeholders and Data Collection in German Forests. *INFORMATIK 2023 - Designing Futures: Zukünfte gestalten*. S. 1245-1253. doi: 10.18420/inf2023_133.

Pretzsch, Stephan; Drees, Hans und Rittershaus, Lars (2022): Mobility Data Space. In: Otto, Bernhard; ten Hompel, Michael und Wrobel, Stefan (Hrsg.): *Designing Data Spaces*. Springer, Cham. https://doi.org/10.1007/978-3-030-93975-5_21.

Puhlmann, Nico; Wiesmaier, Alex; Weber, Patrick und Heinemann, Andreas (2023): Privacy dashboards for citizens and corresponding GDPR services for small data holders: A literature review. *arXiv preprint*, https://doi.org/10.48550/arXiv.2302.00325

Quan-Haase, Anabel; Wellman, Barry; Witte, James C. und Hampton, Keith N. (2002): Capitalizing on the Net: Social Contact, Civic Engagement, and Sense of Community. In: Wellman, Barry und Haythornthwaite, Caroline (Hrsg.): *The Internet in Everyday Life*. Cambridge, Mass.: Wiley-Blackwell, S. 289–324.

Railean, Alexandr und Reinhardt, Delphine (2018): Let there be LITE: Design and evaluation of a label for IoT transparency enhancement. *MobileHCI '18: Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services Adjunct,* S. 103–110, https://doi.org/10.1145/3236112.3236126

Railean, Alexandr und Reinhardt, Delphine (2021): OnLITE: On-line label for IoT transparency enhancement. *Proceedings of the 25th Nordic Conference on Secure IT Systems*, S. 229–245, https://doi.org/10.1007/978-3-030-70852-8_14

Raschke, Philip; Küpper, Axel; Drozd, Olha und Kirrane, Sabrina (2018): Designing a GDPR-compliant and usable privacy dashboard. In: Hansen, Marit; Kosta, Eleni; Nai-Fovino, Isabella und Fischer-Hübner, Simone (Hrsg.): *Privacy and Identity Management. The Smart Revolution*. Springer, S. 221–236. doi:10.1007/978-3-319-92925-5_14.

Rheingold, Howard (1993): *The Virtual Community. Homesteading on the Electronic Frontie*r. Reading, Massachusetts: Addison-Wesley.

Richter, Julia et al. (2018): Machtförmige Praktiken durch Sensordaten in Wohnungen. *Mensch und Computer 2018*. doi: 10.18420/muc2018-mci-0253.

Rössler, Beate (2022): Der Überwachung entgegenkommen: Paradoxien der Privatheit im Internet. In: Honneth, Axel; Maiwald, Klaus-Otto; Speck, Svenja und Trautmann, Frank (Hrsg.): *Normative Paradoxien: Verkehrungen des gesellschaftlichen Fortschritts*. Frankfurt am Main: Campus, S. 239–252.

Roßnagel, Alexander (2019): Quantifizierung der Persönlichkeit – aus grundrechtlicher und datenschutzrechtlicher Sicht. In: Baule, Bernward; Hohnsträter, Dirk; Krankenhagen, Stefan und Lamla, Jörn (Hrsg.): *Transformationen des Konsums. Vom industriellen Massenkonsum zum individualisierten Digitalkonsum*. Baden-Baden: Nomos, S. 33–53.

Rost, Martin (2013: Zur Soziologie des Datenschutzes. *DuD – Datenschutz und Datensicherheit* (2/2013), S. 85–91.

Schaar, Peter (2010): Privacy by design. Identity in the Information Society, 3, S. 267–274. doi:10.1007/s12394-010-0055-x.

Schuler, Doug (1994): Community Networks: Building a New Participatory Medium. *Communications of the ACM*, 37(1), S. 38–51.

Schumpeter, Joseph A. (1942): *Capitalism, Socialism, and Democracy*. New York: Harper & Brothers.

Sorescu, Alina (2017): Data-driven business model innovation. *Journal of Product Innovation Management,* 34(5), S. 691–696.

Staab, Philipp (2019): *Digitaler Kapitalismus. Markt und Herrschaft in der Ökonomie der Unknappheit*. Berlin: Suhrkamp.

Stark, Luke und Levy, Karen (2018): The surveillant consumer. *Media, Culture & Society*, 40(8), S. 1202–1220.

Steinbrink, Enno und Reuter, Christian (2024): The impact of transparency and trust on user acceptance of contact tracing apps. *International Journal of Disaster Risk Reduction*, 112, doi: 104661.

Steinfeld, Nili (2016): "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in Human Behavior*, 55, S. 992–1000. doi:10.1016/j.chb.2015.09.038

Tahaei, Mohammad; Abu-Salma, Ruba und Rashid, Awais (2023): Stuck in the Permissions With You: Developer & End-User Perspectives on App Permissions & Their Privacy Ramifications. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI '23)*. Article 168, S. 1–24. doi:10.1145/3544548.3581060.

Tanczer, Leonie Maria (2021): Das Internet der Dinge: Die Auswirkungen ‚smarter' Geräte auf häusliche Gewalt. In: Prasad, Nivedita (Hrsg.): *Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung: Formen und Interventionsstrategien*. Bielefeld: transcript Verlag, S. 205–226. doi:10.1515/9783839452813-011.

Tang, Ruifan; et al. (2022): A literature review of Artificial Intelligence applications in railway systems. *Transportation Research Part C: Emerging Technologies*. doi:10.1016/j.trc.2022.103679.

Tolmie, Peter et al. (2016): "This has to be the cats": Personal data legibility in networked sensing systems. *ACM CSCW,* S. 491–502. doi:10.1145/2818048.2819992.

Tillmann, Arne; et al. (2023): Privacy estimation on Twitter: Modelling the effect of latent topics on privacy by integrating XGBoost, topic and generalized additive models. *IEEE International Conference on Privacy Computing*. S.2325-2332. doi:.1109/SmartWorld-UIC-ATC-ScalCom-DigitalTwin-PriComp-Metaverse56740.2022.00365.

Turkle, Sherry (1995): *Life on the screen: identity in the age of the Internet*. New York: Simon & Schuster.

van Dijck, José (2013*): The Culture of Connectivity. A Critical History of Social Media*. Oxford, New York: Oxford University Press.

Wellman, Barry (2001): Physical Place and Cyberplace: The Rise of Personalized Networking. *International Journal of Urban and Regional* Research, 25(2), S. 227-252.

Wagner, Isabel; Eckhoff, David (2018). Technical Privacy Metrics: A Systematic Survey. *ACM Comput. Surv.* 51, 3, Article 57, https://doi.org/10.1145/3168389

Wagner, Peter (1994): *A Sociology of Modernity. Liberty and Discipline.* London: Routledge.

Zhang, Julia; Koivumäki, Timo und Chalmers, Dominic (2024): Privacy vs Convenience: Understanding intention-behavior divergence post-GDPR. *Computers in Human Behavior,* 160(6221). doi:10.1016/j.chb.2024.108382.

Zuboff, Shoshana (2018): *Das Zeitalter des Überwachungskapitalismus.* Frankfurt a.M./New York.

Diversitätsgerechter Privatheitsschutz in digitalen Umgebungen

Heiner Koch, Clara Strathmann, Martin Hennig, Luisa Schmied, Christian L. Geminn, Jessica Heesen, Nicole Krämer und Karoline Reinhardt

Zusammenfassung
Im digitalen Zeitalter ist der Schutz der Privatheit besonders wichtig, doch bestehende Datenschutzmechanismen sind oft unzureichend. Menschen sind unterschiedlich vulnerabel, wenn es um Eingriffe in ihre Privatsphäre geht. Dies hat nicht nur strukturelle Ursachen, sondern ist auch durch individuelle Faktoren bedingt. Die Einwilligung und die damit verbundene informationelle Selbstbestimmung ist ein zentraler Aspekt des Datenschutzes. Ansätze, die sich hier auf „Privacy Literacy" und die Fähigkeiten des „Durchschnittsnutzenden" beziehen, sind für vulnerable Personen oft unzureichend. Weder schützt „Privacy Literacy" immer ausreichend, noch ist diese für vulnerable Personen immer erreichbar. Um ein angemessenes Schutzniveau zu gewährleisten, ist es notwendig, die Vulnerabilität verschiedener Gruppen diversitätsgerecht zu berücksichtigen. Ein neuer Ansatz, der im Rahmen eines BMFTR-Projekts untersucht wird, ist der Einsatz viszeraler Reize, um das Bewusstsein für Privatheitsrisiken zu schärfen.
Empirische Studien und theoretische Überlegungen zeigen, dass der Schutzbedarf und die Vulnerabilität individualisiert betrachtet werden müssen. Anstelle von festen Kategorien wie Geschlecht oder Klasse ist es sinnvoller, mit dem offeneren Begriff der Diversität zu arbeiten. Die Entwicklung diversitätsgerechter Privatheitsunterstützung und die Kommunikation von Wissen über Privatheit an diverse Gruppen sind von großer Bedeutung. Der Schutz besonders vulnerabler Personen in digitalen Umgebungen ist dabei gleichzeitig oft auch ein Schutz aller.

1. Einleitung - Privatheit in digitalen Umgebungen

Deutschland feierte 2024 75 Jahre Grundgesetz; es gilt als Garant für Grund- und Menschenrechte, Demokratie und Rechtsstaatlichkeit und verspricht allen Bürgerinnen und Bürgern gleiche Teilhabe am politischen und gesellschaftlichen Leben. Betrachtet man Privatheitsschutz unter Gerechtigkeits- und Demokratieaspekten, wird insbesondere der Einbezug von marginalisierten und vulnerablen Bevölkerungsgruppen, die oft weniger Einfluss auf öffentliche Debatten und gesellschaftliche Gestaltungsprozesse haben, als notwendig bewertet (Castro Varela/Heinemann 2016). In Bezug auf den Privatheitsschutz besteht für die Gesellschaft insgesamt ein demokratietheoretisch begründetes Interesse an der Wahrung der informationellen Selbstbestimmung, selbst dann, wenn einzelne Personen Daten zu ihrer Person und ihrem Verhalten nicht schützen wollen oder können. Auch das Bundesverfassungsgericht hat die Bedeutung der informationellen Selbst-

bestimmung für die Demokratie von Anfang an betont (BVerfGE 65, 1, Rn. 148).

Gerade im digitalen Zeitalter stellt der Schutz der Privatheit eine komplexe Herausforderung dar, die häufig über die bisher bestehenden datenschutzrechtlichen Schutzmechanismen hinausgeht. Unterschiedliche Personen sind unterschiedlich vulnerabel gegenüber Verletzungen ihrer Privatsphäre. Diese Ungleichheit kann durch größere strukturelle Bedingungen zustande kommen (etwa Diskriminierungen oder ungleicher Ressourcenzugang) aber auch durch sehr individuelle Gründe, die insbesondere auf situations- und kontextabhängiges Nutzungsverhalten zurückzuführen sind (etwa Häufigkeit und Art der Internetnutzung) (Kroschwald 2023, S. 5; Strauß/Bettin 2023, S. 54).

Bestehende Instrumente zum Schutz vulnerabler Gruppen, wie z. B. in Form von Art. 8 DSGVO bezogen auf Kinder, erfassen diesen Schutzbedarf nicht ausreichend differenziert (Roßnagel 2020, S. 88; Roßnagel/Geminn 2020, S. 55 ff.; Geminn 2023, S. 193 ff.). Es bleibt die Notwendigkeit einer adäquaten Adressierung von Vulnerabilität auch von z. B. älteren Menschen oder Personen mit kognitiven Beeinträchtigungen (Geminn 2023, S. 203 ff.). Der klassische Diskriminierungsschutz auf Grundlage von abschließenden Merkmallisten muss um eine Diversitätsperspektive ergänzt werden, die anhand der Vulnerabilitäten im Kontext des konkreten Gegenstandsbereichs entwickelt wird. Ein zentrales Anliegen muss es sein, diversitätsgerecht der Vulnerabilität der Privatheit verschiedener Gruppen Rechnung zu tragen. Ein besserer Schutz vulnerabler Personen kommt dabei letztlich allen zugute.

2. Problemaufriss: Einwilligung als datenschutzrechtliche Legitimationsgrundlage der Verarbeitung personenbezogener Daten

Die Erfassung personenbezogener Daten hat zur Entstehung neuer Geschäftsmodelle geführt, die auf der Erstellung umfassender Identitätsprofile durch Tracking und Profiling der Nutzenden basieren. Neben den Zielen, damit die Kundenbindung zu erhöhen oder personalisierte Werbung zu schalten, entstehen Informations- und Machtasymmetrien (Strauß/Bettin 2023, S. 33, 48). Die digitalisierten Infrastrukturen wirken dabei intrusiv in die Privatsphäre der Menschen hinein und vergrößern damit die Angriffsfläche für Grundrechtseingriffe sowie die Exposition in Hinblick auf Vulnerabilitätsfaktoren (Geminn 2023, S. 172). Als gesetzlich legitime Rechts-

grundlage zur Verarbeitung personenbezogener Daten zu diesen Zwecken kommt in der Regel die Einwilligung zum Tragen. Im Rahmen des Privatheitsschutzes vulnerabler Personen (und nicht nur dort) muss die gängige Praxis der Einwilligung als datenschutzrechtliche Legitimationsgrundlage der Verarbeitung personenbezogener Daten jedoch kritisch hinterfragt werden.

Die Einwilligung gilt als „genuiner Ausdruck der informationellen Selbstbestimmung" (Roßnagel u. a 2001, S. 15, 72; Schulz, in: Gola/Heckmann 2022). Die Betonung der Selbstbestimmung als zentraler Aspekt des Datenschutzes findet sich bereits im Volkszählungsurteil des BVerfG aus dem Jahr 1983, das durch die Konzipierung des Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG dem Einzelnen die Befugnis einräumt, „selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" (BVerfGE 65, 1, Rn. 74). Auch aus dem europäischen Grundrecht auf Datenschutz aus Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union (GRCh) lässt sich ein Recht des Einzelnen auf Selbstbestimmung im Hinblick auf den Umgang mit den ihn betreffenden personenbezogenen Daten ableiten (Kühling/Buchner, in: Kühling/Buchner 2024; Liedke-Deutscher 2024, S. 8; Nebel 2015, S. 517-521). Art. 8 Abs. 2 Satz 1 GRCh nennt die Einwilligung als eigenständigen Rechtfertigungsgrund zur Verarbeitung von Daten. Eine auf Grundlage einer selbstbestimmten, autonomen Entscheidung getroffene Erteilung der Einwilligung kann folglich als Grundrechtsausübung im Sinne der GRCh gesehen werden (Klement, in: Simitis/Hornung/Spiecker gen. Döhmann 2025; Liedke-Deutscher 2024, S. 8).

Zur Umsetzung der grundrechtlichen Vorgaben zum Datenschutz wird die Einwilligung als Rechtsgrundlage zur Verarbeitung personenbezogener Daten in der Datenschutz-Grundverordnung (DSGVO) konkretisiert. Die Wirksamkeitsvoraussetzungen der Einwilligung ergeben sich aus Art. 4 Nr. 11 DSGVO. Für Menschen, die aufgrund struktureller oder individueller Faktoren eine erhöhte Vulnerabilität aufweisen, stellt sich die Frage nach den Voraussetzungen für eine wirksame Einwilligung, insbesondere hinsichtlich der Freiwilligkeit und der Informiertheit, mit besonderer Dringlichkeit. Eine informierte Einwilligung setzt voraus, dass die betroffene Person versteht, dass und in welchem Umfang sie ihre Einwilligung erteilt hat und damit auch z. B. von ihrem Recht auf Widerspruch Gebrauch machen kann. Dies hat der Verantwortliche durch entsprechende Vorkehrungen sicherzustellen (vgl. ErwG 42 Satz 2 DSGVO).

Transparenz kann dabei als zentrale Voraussetzung der Ausübung der informationellen Selbstbestimmung verstanden werden (Albers/Veit, in: BeckOK Datenschutzrecht 2024). Dem Grundsatz der Transparenz aus Art. 5 Abs. 1 lit. a DSGVO folgend, müssen personenbezogene Daten „in einer für die betroffene Person nachvollziehbaren Weise" verarbeitet werden. Gemäß Art. 12 Abs. 1, S. 1 DSGVO haben „Verantwortliche geeignete Maßnahmen zu treffen, um der betroffenen Person alle Informationen […], die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln". Das Transparenzgebot verlangt dabei nicht nur formale Verständlichkeit im Sinne von Lesbarkeit, sondern auch Sinnverständlichkeit (Heberlein, in: Ehmann/Selmayr 2024).

Die Einwilligung prägt das Datenschutzrecht durch einen stark individualistischen Ansatz. Dem liegt die Annahme zugrunde, dass Transparenz und Eigenverantwortung ausreichen, um eine wirksame Einwilligung und damit die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu gewährleisten (Friedewald u. a 2020, S. 7). Als Bezugspunkt für Verantwortliche wird dazu auf den „Durchschnittsnutzer" (Artikel-29-Datenschutzgruppe 2018, S. 16) und dessen Privacy Literacy abgestellt. Privacy Literacy bezeichnet das Wissen und die Fähigkeiten, die erforderlich sind, um Datenschutzentscheidungen informiert zu treffen. Sie umfasst verschiedene Dimensionen, darunter prozedurales Wissen (z. B. über Schutzstrategien), Erfahrungswissen (z. B. eigene Erlebnisse mit Datenschutzverletzungen) und Faktenwissen über gesetzliche Grundlagen, technische Datenschutzmaßnahmen sowie Unternehmenspraktiken (Brough/Martin 2020; Trepte u. a 2015). Ein angemessenes Schutzniveau kann auf diesem Wege jedoch zumindest nicht durchgehend gewährleistet werden. Besonders vulnerable Personen, wie z. B. Menschen mit kognitiven Beeinträchtigungen, haben oft nicht die gleichen Voraussetzungen, um informierte Entscheidungen über ihre Daten zu treffen. Das Konzept der Privacy Literacy greift hier zu kurz, da es voraussetzt, dass alle Nutzenden über die notwendigen Ressourcen verfügen können, um sich entsprechend zu informieren. Selbstbestimmung im Datenschutz muss jedoch allen Menschen möglich sein, unabhängig von ihren individuellen Fähigkeiten, sozioökonomischem Hintergrund oder der jeweiligen digitalen Umgebung. Sie darf nicht nur Personen zu Teil werden, die über die notwendigen Mittel verfügen, um sie auszuüben, wie z. B. die Fähigkeit, Datenschutzeinstellungen vorzunehmen oder Datenschutzhinweise zu lesen und zu verstehen (BVerfGE 65, 1, Rn. 148).

Die Gründe für das Fehlen der Informiertheit bei Datenschutzentscheidungen sind so divers wie die Vulnerabilität, die den betroffenen Personen eigen ist. Oftmals wird das Problem in einem Mangel an Privacy Literacy gesehen. Doch Privacy Literacy und das damit verbundene Wissen ist nur eine von vielen notwendigen Ressourcen. Zeit, Geld, digitale Erfahrung und kognitive Kapazitäten spielen eine entscheidende Rolle dabei, ob jemand in der Lage ist, die komplexen Dynamiken der digitalen Marktwirtschaft zu begreifen und entsprechend zu handeln. Während Bildungsangebote zwar einen sicheren Umgang mit dem Internet unterstützen können, stößt das Konzept für einige Bevölkerungsgruppen an seine Grenzen. Nicht alle Menschen können etwa gleichermaßen erreicht werden; andere haben spezielle Bedürfnisse, denen man nicht universell gerecht werden kann. Auch in Bezug auf Einwilligungsfragen muss demnach aus Diversitätsperspektive kritisch untersucht werden, wo Schutzlücken entstehen und wie diese geschlossen werden können. Herkömmliche Ansätze, die auf Privacy Literacy setzen, berücksichtigen dabei oft nicht, dass hierdurch kein angemessenes Schutzniveau für alle Gruppen hergestellt werden kann.

Darüber hinaus wird im Rahmen von Privacy Literacy durch die starke Betonung individueller Verantwortung (Responsibilisierung) die strukturelle Dimension des Privatheitsschutzes ausgeblendet. Viele digitale Dienste und Plattformen sind aber so gestaltet, dass die standardmäßige Datenweitergabe erleichtert und datenschutzfreundliche Alternativen erschwert werden. Solche systematischen Probleme können nicht allein durch individuelle Kompetenzbildung gelöst werden. Vielmehr bedarf es ergänzender Maßnahmen, wie regulatorischer Vorgaben und weniger kognitionsbasierter Ansätze, um ein umfassendes und gerechtes Schutzniveau für alle zu erreichen.

3. Viszerale Reize als mögliche Lösung

Vor dem Hintergrund der oben geführten Diskussion möchten wir den Ansatz der Privacy Literacy zur Unterstützung des Privatheitsmanagements um weniger kognitionsbasierte Möglichkeiten ergänzen. Neue Ansätze wie der Einsatz viszeraler (also körperlich-wahrnehmbarer) Reize könnten das Bewusstsein für Privatheitsrisiken schärfen und Menschen dabei unterstützen, informierte Entscheidungen über ihre Privatsphäre zu treffen (Acquisti u. a. 2022). Dabei geht es z. B. darum, Erfahrungen aus dem Kontext analoger Privatheitsverletzungen auf die Online-Welt zu übertragen, wie

etwa, sich bei einem vertraulichen Gespräch beobachtet zu fühlen, weil eine fremde Person zu nah kommt. Dafür wurde im Kontext von digitaler Privatheit das Konzept der *viszeralen Hinweise* (visceral notice) vorgestellt (Calo 2011). Dabei geht es, im Gegensatz zum traditionellen symbol- und textgeprägten Hinweis, um eine Informationsvermittlung durch Erfahrung bei Gefahr. Ein anschauliches Beispiel dafür findet sich in Baustellensituationen: Um die Verkehrsteilnehmer:innen dort zur Vorsicht aufzurufen, werden Verkehrsschilder aufgestellt, die bildlich oder per Text auf die Notwendigkeit besonderer Aufmerksamkeit hinweisen sollen. Als Alternative bietet sich der Einsatz von Rüttelschwellen an, die unmittelbar „aufrütteln", ohne kognitiv verarbeitet werden zu müssen und somit einen intuitiveren Charakter innehaben. Calo (2011) unterscheidet dabei zwischen drei Kategorien: Vertrautheit als Warnung, psychologische Reaktion als Warnung, und Zeigen als Warnung. Bei Vertrautheit geht es darum, dass die Nutzenden das Verhalten von bestimmten Technologien kennen und deshalb dasselbe Verhalten in anderen, ähnlichen Interaktionen erwarten. Ein Beispiel dafür sind digitale Kameras, die mit einem Auslösegeräusch ausgestattet sind, das ertönt, wenn ein Foto gemacht wird. Dieses sollte an die analoge Kamera erinnern und so eine Warnung vor potenziellem Eindringen in die Privatsphäre geben. Die Kategorie der psychologischen Reaktion umfasst biologisch bzw. evolutionär bedingte Reaktionen auf bestimmte Designelemente (z. B. die Rüttelschwelle, wobei ein besonderes Aufmerken die Reaktion darstellt). Solche Reaktionen können auch durch die anthropomorphe (also menschenähnliche) Gestaltung von Technologien ausgelöst werden. Dadurch könnten z. B. soziale Skripte getriggert werden, wie dass man sich beobachtet fühlt (Rodriguez-Priego u. a. 2021). Die dritte Kategorie, Zeigen als Warnung, kann gestaltet werden durch konkretes Sichtbarmachen von Konsequenzen, z. B., wie bestimmte Daten genutzt werden. Dadurch sollen die Gefahren, die mit einer bestimmten Entscheidung einhergehen (könnten), transparenter und anschaulicher gestaltet werden.

Drei Probleme bestehen nun bei dem möglichen Einsatz viszeraler Reize: (i) viszerale Reize können ein paternalistisches „Nudging" von Privatheitsentscheidungen darstellen, (ii) viszerale Reize sind Teil eines individuellen Selbstschutzes und lösen damit keine strukturellen Probleme und (iii) ob der Einsatz viszeraler Reize wirksam ist, wird sich erst noch zeigen müssen, was jedoch kein konzeptionelles Problem des Ansatzes darstellt.

Grundsätzlich gilt, dass Paternalismus nicht immer falsch sein muss (Birnbacher 2012, S. 564). Paternalismus hat jedoch einen deutlich erhöhten Rechtfertigungsbedarf und muss kontinuierlich auf seine Notwendig-

keit hin untersucht werden. Paternalismusprobleme können auftreten, weil viszerale Reize gerade dazu da sein sollen, eine Schutzlücke durch fehlende Privacy Literacy zu schließen. Privacy Literacy soll jedoch dazu dienen, selbstbestimmte Entscheidung über Privatheitsfragen zu treffen. Viszerale Reize können damit Personen zu Entscheidungen zu drängen, die in ihrem Interesse sind, die sie aber ohne diese Reize anders treffen würden. Damit entsteht eine Offenheit dafür, dass viszerale Reize festlegen, was im Interesse der jeweiligen Personen ist. Zwei Lösungsstrategien sind sinnvoll: erstens sollte den Nutzenden die Möglichkeit gegeben werden einzustellen, welche Privatheitspräferenzen durch viszerale Reize unterstützt werden. Damit wären die Präferenzen zweiter Ordnung berücksichtigt und eine damit verbundene Selbstbestimmung gewährleistet. Zweitens können viszerale Reize auch so gestaltet werden, dass sie einen Beitrag zur Privacy Literacy und damit zum Selbstschutz leisten, beispielsweise, indem sie einen konkreten Bezug zur Gefahrensituation herstellen oder indem man diese um einen Hinweis ergänzt, welcher mehr Informationen anbietet. In diesem Sinne würde es sich dann nicht einfach um Paternalismus handeln, sondern um eine Form des „Mothering" (Wartenberg 1990, S. 192-193), das die Personen befähigen soll, selbstbestimmte Entscheidungen treffen zu können. Auch Damm (2013, S. 213) weist allgemeiner darauf hin, dass es beim Konflikt zwischen Schutz und Freiheit oder Selbstbestimmung sinnvoll ist, „Fürsorge gerade auch ihrerseits als Instrument der Förderung und „Ermöglichung der Selbstbestimmung" zu begreifen".

Neben Paternalismus besteht das Problem, dass unter den realen Nutzungsbedingungen keine selbstbestimmten Entscheidungen über Privatheit getroffen werden können. Entweder wird gar nicht erst eine Entscheidungsmöglichkeit angeboten oder die Entscheidung ist zu komplex und zeitaufwendig, als dass diese wirklich getroffen werden könnte. Dort, wo schon Privacy Literacy keine Lösung ist (Hagendorff 2018), kann auch ein viszeraler Reiz, der die individuellen Entscheidungen unterstützen soll, keine Lösung sein. Regulierungen und gesetzliche Vorgaben bleiben damit ein unverzichtbares Instrument des Schutzes vulnerabler Personen. Viszerale Reize sollten damit in diesen Kontexten nicht zu einer Rechtfertigung individueller und eigenverantwortlicher Lösungen werden (Responsibilisierung). Gleichzeitig wäre es jedoch auch ein fragwürdiger Paternalismus, wenn durch Regulierungen vulnerablen Personen grundsätzlich die Entscheidungsmöglichkeiten genommen würden. Vulnerablen Personen gesellschaftliche Teilhabe zu nehmen, indem ihnen etwa der Zugang zu sozialen Medien untersagt wird (etwa das Verbot für unter 16-Jährige, soziale

Medien zu nutzen), ist ethisch problematisch. Gesellschaftliche Teilhabe bedeutet immer auch ein gewisses Maß an Vulnerabilität, bei dem ein paternalistischer Schutz, der mit dieser Vulnerabilität auch die gesellschaftliche Teilhabemöglichkeit beseitigt, Freiheit zu sehr beschränken kann.

Zuletzt muss sich empirisch zeigen, ob viszerale Reize tatsächlich eine geeignete Lösung für Schutzlücken durch eine fehlende Privacy Literacy sein können. Es besteht hier die Gefahr, dass technische Innovationen Lösungen für soziale Probleme sein sollen. Bei der Evaluation viszeraler Reize sind damit Fragen des Paternalismus, der Responsibilisierung und der Eignung technischer Lösungsansätze zu berücksichtigen.

4. Notwendigkeit einer kontextbezogenen Diversitätsperspektive

4.1 Empirische Evidenzen

Um zunächst zu verstehen, welchen Schutzbedarf unterschiedliche vulnerable Gruppen im Umgang mit ihrer Privatsphäre im Internet haben, wurden insgesamt neun Fokusgruppen durchgeführt. Dabei wurden drei besonders vulnerable Kohorten miteinbezogen: Grundschulkinder, Senior:innen sowie Personen mit kognitiven Beeinträchtigungen. Zwei Gruppen mit Personen zwischen 18 und 65 dienten darüber hinaus als Vergleichsgruppe. Innerhalb der Fokusgruppen wurde eruiert, inwiefern bei den Teilnehmenden ein Bewusstsein für systematische Datensammlungspraktiken von Unternehmensseite vorliegt. Darüber hinaus sollte ein Eindruck darüber gewonnen werden, welcher Risiken und Schutzmaßnahmen sich die Teilnehmenden bewusst sind, wobei der Einsatz von Cookie-Bannern als Mechanismus zum Schutz der eigenen Daten diskutiert wurde. Zuletzt wurden die Teilnehmenden dazu ermuntert, eigene Ideen für den Schutz vor Privatheitsrisiken zu generieren.

Die Analyse des Bewusstseins für und Wissens der Teilnehmenden über Datenschutz ergab ein diverses Bild. Kinder beispielsweise attribuierten Datensammlungspraktiken eher auf einer horizontalen Ebene (z. B. in Bezug auf Influencer:innen, die mit erhöhten Zuschauer:innenzahlen mehr Geld verdienen könnten). Unter den Personen mit kognitiven Einschränkungen zeigte sich das diverseste Spektrum an Wissen: von Einzelnen, die schon mal von der Sammlung persönlicher Daten gehört hatten, bis hin zu jenen, die sich nicht vorstellen konnten, dass YouTube auf irgendwelche Informationen über sie zugreifen kann oder diese gar sammelt (oft begründet

im mangelnden Verständnis des Werts von Daten). Bei den Senior:innen beobachteten wir, dass Teile ihres Verständnisses auf populären Gerüchten basierten, so etwa, dass das eigene Handy einen ständig belausche und auf Basis des Gehörten entsprechende Werbung geschaltet würde. Andererseits hatte diese Gruppe von den drei untersuchten vulnerablen Gruppen das höchste Bewusstsein dafür, dass große Firmen wie Google Zugang zu verschiedenen Datenquellen haben und, dass Werbeunternehmen auf Basis verschiedener Nutzer:innendaten personalisierte Empfehlungen ausgeben können. Das Wissen der Senior:innen stieß dann an seine Grenzen, wenn es um komplexere Prozesse wie Big Data oder Algorithmen ging, was üblicherweise bereits weit über das Verständnis der Kinder und Personen mit kognitiven Einschränkungen hinausging. Bei diesen ließ sich beobachten, welchen Wert physische Greifbarkeit in Privatheitsvorstellungen hat: So äußerten einige Kinder, man könne Datensammlungen durch das Zerstören eines entsprechenden Geräts verhindern. Auch bei den Personen mit kognitiven Einschränkungen zeigte sich allenfalls ein grundlegendes Verständnis. So beobachteten manche beispielsweise, dass die Google-Suche nach einem Produkt oft zu Werbung für diesen oder ähnliche Konsumartikel führt. Andere erkannten, dass ein Zusammenhang zwischen dem aktuellen Video auf YouTube und den personalisierten Empfehlungen am Rand der Seite besteht.

Darüber hinaus fiel die Attribution der Verantwortung im Hinblick auf Privatheitsschutz im Internet unterschiedlich aus. Sowohl bei den Kindern als auch bei den Personen mit kognitiven Beeinträchtigungen standen Hilfestellungen bei der Navigation der eigenen Privatheit durch Vertrauenspersonen im Vordergrund. Das Verständnis für die Verletzung der Privatheit durch Institutionen oder Unternehmen unterschied sich stark interindividuell, war aber gerade in diesen Gruppen durchschnittlich gering und spiegelte teils wider, was von Vertrauenspersonen übernommen worden war. So war einigen Personen bekannt, dass Cookies abgelehnt werden sollten, worum es sich dabei allerdings handele und warum sie abgelehnt werden sollten, entzog sich oft dem allgemeinen Verständnis. Senior:innen auf der anderen Seite lokalisierten die Verantwortung tendenziell bei sich und dem eigenen Wissen. Im Vergleich zu den beiden vorgenannten Gruppen wurde zwar gelegentlich der Wunsch nach einer externen Schutzinstanz geäußert, die das Individuum um die eigene Verantwortung erleichtern solle (ähnlich wie bei den Vergleichsgruppen), diese Möglichkeit wurde aber tendenziell als nicht umsetzbar wahrgenommen. Bildungsangebote wurden insbesondere von den Senior:innen als wertvoll betrachtet und am ehesten

als realistische externe Schutzmöglichkeit angesehen. Grundsätzlich fand sich in dieser Gruppe jedoch auch ein starker Bezug auf die eigene Lebenserfahrung, der ein großer Stellenwert im Hinblick auf das Erkennen von und den Umgang mit Gefahren zugeschrieben wurde.

Im Zusammenhang mit den Fokusgruppen hat sich empirisch gezeigt, dass es sinnvoll sein kann, Schutzbedarf und Vulnerabilität individualisierter zu denken. Diese Position soll im Folgenden - insbesondere für den Privatheitsbereich - auch theoretisch begründet werden.

4.2 Vulnerabilität und Privatheit

Oft wird angenommen, dass Menschen einerseits universell vulnerabel sind, aber andererseits auch partikulare Personengruppen oder einzelne Personen eine besondere Vulnerabilität aufweisen (Albertson Fineman 2017). Vulnerabilität bedeutet, dass Personen sich nicht allein schützen können und damit einen Schutzbedarf haben. Zunehmend wird hierbei Vulnerabilität auch im Privatheitsbereich diskutiert (Geminn 2023; Behrendt/Loh 2022). Insofern Personen ein Interesse an informationeller Selbstbestimmung haben und sich nicht allein und mit absoluter Sicherheit schützen können, sind sie in dieser Hinsicht vulnerabel. Damit ist auch klar, dass Personen immer nur in bestimmten Hinsichten besonders vulnerabel sind. Vulnerabel im Bereich der Privatheit zu sein bedeutet etwa nicht, auch im Gesundheitsbereich vulnerabel zu sein.

Privacy Literacy beispielsweise kann die Vulnerabilität im Privatheitsbereich abschwächen, aber nicht beseitigen. Während wir eine gewisse Vulnerabilität im Privatheitsbereich universell teilen, bestehen jedoch auch wichtige Unterschiede darin, wie ausgeprägt vulnerabel die einzelnen Personen sind. Eine ungleiche Verteilung von Privacy Literacy kann zu einer solchen ungleichen Vulnerabilität führen. Auch kann die gleiche Verletzung der informationellen Selbstbestimmung sehr unterschiedliche Konsequenzen nach sich ziehen. So ist es ungleich problematischer, wenn die Gesundheitsdaten einer kranken Person ungewollt zugänglich werden, als wenn dies bei einer gesunden Person passiert. Weiterhin kann das Ausmaß, in dem Personen Gefahren ausgesetzt sind, sehr unterschiedlich verteilt sein. Personen des öffentlichen Lebens etwa sind oft dauerhaft intensiven Angriffen auf ihre Privatsphäre ausgesetzt.

Zumindest zwei Probleme treten hierbei jedoch auf: erstens kann Privacy Literacy unzureichend sein, um sich zu schützen. Zweitens ist es

verschiedenen Personengruppen erschwert, eine hinreichende Privacy Literacy zu erwerben.

Schon auf der Ebene von Privacy Literacy liegt nicht nur ein einziger Mechanismus vor, der dazu führt, dass diese nicht ausreicht, um sich angemessen schützen zu können. Dass Probleme und die betroffenen Personengruppen vielfältig sind, bedeutet jedoch nicht automatisch, dass die Lösungsansätze genauso vielfältig sein müssen. Wird etwa durch Regulation die Erhebung von Daten durch Unternehmen in einem bestimmten Bereich effektiv untersagt, so wird durch diesen Schutz eine bestimmte Form der Vulnerabilität mindestens deutlich abgeschwächt. Auch Verfahren zum Schutz von partikularen Vulnerabilitätsgruppen können dazu geeignet sein, auch andere Gruppen zu schützen. Während die viszeralen Reize, die wir in diesem Kontext diskutieren, dazu entwickelt werden, Privacy Literacy-Probleme bei Personen mit eingeschränkten kognitiven Fähigkeiten zu bewältigen, können diese viszeralen Reize auch für andere Personen geeignet sein, sie bei dem Schutz ihrer Privatsphäre zu unterstützen.

Für den Privatheitsbereich stellen außerdem die Einwilligung und die damit verbundenen Aspekte der Informiertheit und Freiwilligkeit einen wesentlichen Bereich der Vulnerabilität dar. In Bezug auf Freiwilligkeit lässt sich im Anschluss an Kiener (2023) argumentieren, dass sich diese nur in konkreten Interaktionen zwischen der Person, die die Einwilligung erteilt und der einwilligungserhaltenden Stelle feststellen lässt. Dies bedeutet auch, dass Vulnerabilitäten auf den ganz konkreten Interaktionskontext bezogen sein müssen. Erst wenn diesen Vulnerabilitäten angemessen von der einwilligungserhaltenden Stelle begegnet worden ist, kann überhaupt von Freiwilligkeit in diesem Interaktionskontext ausgegangen werden. Dies lässt sich analog auch auf die Informiertheit übertragen. Auch hier gibt es Anforderungen des konkreten Interaktionskontextes, denen begegnet werden muss, damit Vulnerabilitäten in Bezug auf Informiertheit die Einwilligung nicht ungültig werden lassen. Insofern die Verschiedenheit der einzelnen Interaktionen bei Einwilligungen in Datennutzung relevant sind, stützt dies die Anforderung, Vulnerabilität anhand kontextspezifischer Kriterien zu entwickeln.

4.3 Kategorienbildung und Vulnerabilität

Verbreitet ist die Annahme, dass Vulnerabilitäten sich nicht anhand von festen vorgegebenen Kategorien feststellen lassen, sondern individuelle

Eigenschaften sind (Birnbacher 2012, S. 561). Damit soll über Vulnerabilität eine moralisch richtige Einschätzung von Einzelfällen stattfinden und eine Einzelfallgerechtigkeit erreicht werden können (Damm 2013, S. 212). Gruppenkategorien können jedoch auch im Bereich der Vulnerabilität aus später noch diskutierten Gründen unverzichtbar sein. Dabei bleibt jedoch festzuhalten, dass Personen, die zu einer dieser Gruppen gehören, nur mit einer höheren Wahrscheinlichkeit eine größere Vulnerabilität aufweisen (Birnbacher 2012, S. 561). Einzelne Gruppenmitglieder können durch eine geringere Vulnerabilität gekennzeichnet sein und genauso können auch Personen, die nicht in eine dieser Gruppenkategorien fallen, eine höhere Vulnerabilität aufweisen.

Wie können wir nun über die partikularen Vulnerabilitäten sprechen? In der Vergangenheit wurde dies oft anhand von Kategorien getan (klassisch etwa Geschlecht, Klasse und „Rasse"), die wir auch aus dem Diskriminierungskontext kennen (kritisch hierzu: Luna 2009, S. 124-125). Albertson Fineman (2017) argumentiert, dass Diskriminierungsansätze davon ausgehen würden, dass Menschen gleichbehandelt werden müssten und nur bestimmte diskriminierte Gruppen einen Schutzbedarf hätten. Damit werde ignoriert, dass einerseits alle vulnerabel seien und andererseits eine Gleichbehandlung nicht genüge, um spezifischen Vulnerabilitäten zu begegnen. Anstelle individueller Gleichbehandlung zur Vermeidung von Diskriminierung benötige es aktive staatliche Schutzmaßnahmen, die die Vulnerabilität aller und gleichzeitig auch die je spezifischen und kontextabhängigen besonderen Vulnerabilitäten bestimmter Gruppierungen vermindere. Insofern auf partikulare Vulnerabilität abgezielt werde, würde jedoch nur das Paradigma der Diskriminierung aufgerufen, ohne die universelle Vulnerabilität und die damit erforderlichen systemisch-strukturellen Aspekte zu thematisieren (Albertson Fineman 2017, S. 133). Solange die universelle Vulnerabilität berücksichtigt wird und nicht einfach auf Gleichbehandlung abgezielt wird, ist trotz Albertson Finemans Kritik die Thematisierung partikularer Vulnerabilitäten in bestimmten Fällen notwendig und angemessen.

Insofern jedoch Diskriminierungskategorien zur Thematisierung der Vulnerabilitäten herangezogen werden, bleiben weitere Probleme bestehen. Diese Diskriminierungskategorien sind sehr grob und werden den tatsächlichen partikularen Vulnerabilitäten nicht gerecht. Es entsteht die Gefahr, dass die Vulnerabilität von Personen, die nicht in diese Kategorien fallen, übersehen wird und die Vulnerabilität von Personen in einer solchen Kategorie essentialisiert wird (Martin 2023, S. 23; Luna 2009, S. 123). Personen, die sich – insbesondere in autoritären Regimen – politisch engagieren,

sind beispielsweise besonders vulnerabel in Bezug auf ihre informationelle Selbstbestimmung, ohne dass diese Personen von klassischen Diskriminierungskategorien erfasst werden. Gleichzeitig kann es sein, dass Menschen mit Lernschwierigkeiten zwar durchschnittlich eine höhere Vulnerabilität im Privatheitsbereich aufweisen, dies aber nicht auf jede Einzelperson dieser Gruppe zutreffen muss und sich dies auch bei einzelnen Personen dieser Gruppe im Laufe der Zeit ändern kann. Daher lehnen etwa Albertson Fineman (2017) und Luna (2009) solche Vulnerabilitätskategorien ab. Damit stellt sich jedoch die Herausforderung, diejenigen Personen zu benennen, die besonders vulnerabel sind und eines besonderen Schutzes bedürfen (Wrigley 2014, S. 6).

Intersektionale Ansätze sehen das Problem und thematisieren daher Überschneidungen dieser Kategorien, die zu eigenständigen Formen der Vulnerabilität führen. Linabary und Corple (2019) zeigen dies etwa anhand unterschiedlicher Erfahrungen, die Frauen in Bezug auf Online-Belästigungen im Kontext von Wikipedia machen, je nachdem, welche Überschneidungen mit weiteren Merkmalen vorliegen. Damit gelingt es, ein komplexeres Bild der Wirklichkeit zu erhalten. Es bleibt jedoch das Problem, dass auch intersektionale Ansätze oft bei typischen Diskriminierungskategorien und deren Überschneidungen stehen bleiben. Damit bleibt auch die Abbildung von Wirklichkeit in diesen Kategorien verhaftet. Die Kategorien werden nicht anhand von Vulnerabilitäten im Bereich der Privatheit entwickelt, sondern entlang großer gesamtgesellschaftlicher Benachteiligungen. Auch intersektionale Ansätze können damit die Vielfältigkeit der Vulnerabilitäten im Privatheitsbereich nicht unbedingt abbilden.

Hier bietet es sich an, stattdessen mit dem offeneren Begriff der Diversität zu arbeiten. Diversitätskategorien können zwar auch über endliche Listen gegeben sein (siehe etwa die „4 Layers of Diversity" von Gardenswartz/Rowe 2003), doch Diversität kann auch als grundsätzlich offen verstanden werden. Dies würde die Entwicklung von Diversitätskategorien in Auseinandersetzung mit Vulnerabilitäten im Privatheitsbereich erlauben. Diversität hat jedoch den Nachteil, dass, anders als bei Diskriminierung und Intersektionalität, die moralische Problemdimension ausgeblendet wird. Diversität begründet schließlich noch keinen Schutzbedarf. Daher ist die Kombination von Diversität mit Vulnerabilität besonders geeignet, wenn man ohne Vorannahmen über Kategorien ethische Probleme im Privatheitsbereich thematisieren will. Die Diversitätskategorien, mit denen sich Vulnerabilitäten im Privatheitsbereich beschreiben lassen, müssen

dementsprechend in Auseinandersetzung mit dem konkreten Gegenstandsbereich entwickelt werden.

4.4 Gleichheit und Schutzbedarf

Ethisch gesehen ist es von besonderer Relevanz, um welche Vulnerabilitäten es gehen soll. Oft wird eine besondere Vulnerabilität thematisiert, sei es durch eine erhöhte Schadenswahrscheinlichkeit oder einen erhöhten Schaden (Racine/Bracken-Roche 2019), welche einen Schutzbedarf oder eine Schutzpflicht nach sich ziehen. Als Vergleichsgröße können „normale Situationen" oder „normale Personen" herangezogen werden. Dies ist jedoch problematisch, da es eine solche „Normalität" für gewöhnlich nicht gibt und diese außerdem als eine Art normativer Standard gelesen werden könnte (Koch 2014). Ein weiteres Problem ist, dass schon „normale" Risiken nicht akzeptabel sein müssen und deshalb auch bei „normalen" Risiken schon ein Schutzbedarf bestehen kann. Dies ist im Privatheitsbereich offensichtlich: insofern etwa große Technologiekonzerne systematisch einen defizitären Datenschutz realisieren, ist die überwältigende Mehrheit bei der alltäglichen Nutzung von sozialen Medien im Bereich der informationellen Selbstbestimmung vulnerabel. Insofern Vulnerabilitätstheorien im Privatheitsbereich Anwendung finden sollen, muss dieses verbreitete und alltägliche Risiko miterfasst werden können.

Wenn es ethisch also darum geht, einen Schutzbedarf festzustellen, dann kann es hierbei weder allein um einfache Gleichheit (etwa ein gleiches, aber zu geringes Schutzniveau), noch um irgendeine Form der „Normalität" gehen. Stattdessen muss es um ein ethisch begründetes maximales Risiko gehen, dem Menschen bei ihrer gesellschaftlichen Teilhabe ausgesetzt sein dürfen. Wird dieses maximale Risiko überschritten und damit die gesellschaftliche Teilhabe gefährdet, so besteht ein Schutzbedarf. Darüber hinaus müssen selbstverständlich auch Ungleichheiten thematisiert werden. Vulnerabilität erlaubt es einerseits, Mindeststandards einzufordern, und andererseits Ungleichheiten zu problematisieren. Der Schutzbedarf kann hierbei unabhängig von vorgegebenen Kategorien in der konkreten Auseinandersetzung mit dem Gegenstandsbereich ergründet werden.

4.5 Grenzen individualisierter Ansätze

Während Vulnerabilität durch die Vermeidung klassischer Kategorienbildung eine Einzelfallgerechtigkeit gewährleisten soll, gehen mit diesem Ansatz auch Nachteile einher, die eine solche Kategorienbildung dennoch notwendig machen kann. Hierzu gehört die Aggregation von Benachteiligungen, eine erschwerte politische Organisierung entlang von Kategorien, eine fehlende Komplexitätsreduktion und eine individualisierte Verantwortung, Vulnerabilitäten zu begegnen, die auch zu einer geringeren Rechtssicherheit führen kann. Darüber hinaus weisen Davis and Aldieri (2021) auch darauf hin, dass Vulnerabilität zu unspezifisch sei, eine positive Deutung offenlasse und zumindest in Albertson Finemans Lesart zu sehr auf staatliche Schutzmaßnahmen hinauslaufe. Dabei sei es gerade der Staat, der mit seinen Schutzmaßnahmen oft vulnerable Gruppen schädigt oder deren Vulnerabilität erzeuge oder verstärke.

Vulnerabilität und Diversität erlauben es zwar, sachgerechtere und kontextspezifische Analysen eines Schutzbedarfes im Privatheitsbereich durchzuführen, doch dies darf nicht bedeuten, die größeren gesellschaftlichen Diskriminierungsstrukturen zu vernachlässigen. Dies liegt daran, dass aggregierte Benachteiligungen aus verschiedenen Bereichen eine besondere Last darstellen können, die es zu berücksichtigen gilt. Eine queere Person, die über eine besonders hohe Privacy Literacy verfügt, mag keine besondere Vulnerabilität aufweisen, wenn man allein den Privatheitsbereich betrachtet. Ist jedoch klar, dass diese Person in anderen Lebensbereichen diskriminiert wird und Vulnerabilitäten aufweist, kann selbst eine vergleichsweise geringe Vulnerabilität im Privatheitsbereich eine unzumutbare zusätzliche Belastung darstellen, die einen Schutzbedarf nach sich zieht.

Diskriminierungskategorien anstelle von kontextspezifischen Vulnerabilitätskategorien zu verwenden kann auch dann notwendig sein, wenn die Einzelfälle zu komplex sind, um diesen jeweils Rechnung tragen zu können. (Intersektionale) Diskriminierungskategorien zu verwenden, kann damit auch im Privatheitsbereich eine pragmatisch gerechtfertigte Entscheidung sein. So ist etwa kaum möglich, bei der Nutzung jeder Internetseite eine umfassende Einzelfallprüfung von kontextspezifischen Vulnerabilitäten vorzunehmen.

Ein weiteres Problem bei dem Bezug auf Vulnerabilität besteht darin, dass politische Organisierungen entlang von Vulnerabilität schlechter funktionieren könnten, als wenn sich entlang großer gesellschaftlicher Diskri-

minierungsachsen organisiert wird. Dies ist bereits im Zusammenhang mit intersektionalen Analysen ein bekanntes Problem (Koch 2013).

Die Abhebung auf individuelle Vulnerabilitäten kann außerdem dazu führen, dass keine allgemeinen Schutzvorkehrungen getroffen werden können, sondern individualisierte Lösungen angestrebt werden. Dies könnte jedoch bedeuten, dass es etwa bei Einwilligungen in Datennutzung die einwilligungserhaltende Stelle ist, die die individuelle Vulnerabilität feststellen und für den Einzelfall angemessenen Schutzmaßnahmen treffen muss. Dies lässt jedoch viel Willkürspielraum zu, der letztendlich zu einem geringeren Schutzniveau führen könnte. So weist Damm (2013, S. 213) zurecht darauf hin, dass es bei Einzelfallgerechtigkeit und Kategorienbildung zentral darauf ankommt, welcher Ansatz ein höheres Schutzniveau gewährleisten kann.

5. Fazit

Insgesamt verdeutlichen unsere ersten Befunde, dass ein effektiver Privatheitsschutz eine interdisziplinäre Herangehensweise erfordert. Nur so kann sowohl ethisch fundiert als auch rechtlich gestützt ein Ansatz gefunden werden, welcher empirisch geprüft den Weg zu einem diversitätsgerechten Privatheitsschutz ebnen kann.[1]

Um einen effektiven Privatheitsschutz zu gewährleisten, sind zielgruppengerechte und auf die individuellen Nutzenden zugeschnittene Ansätze erforderlich. Hier hat sich gezeigt, dass rechtliche und ethische Debatten, die an allgemein bestehende Benachteiligungskategorien anknüpfen, oft zu kurz greifen. Stattdessen ist es zielführender, mit den Ansätzen von Diversität und Vulnerabilität zu arbeiten, da diese erlauben, die Vielfältigkeit

1 Zusätzlich kann der Bereich der Kommunikation von Wissensbeständen über Privatheit an diverse Gruppen von einem integrativen Ansatz profitieren, der vulnerable Gruppen stets im Wissenschaftsdialog mitdenkt. In der Empirie und Theorie (vgl. Schrögel et al. 2018) wird deutlich, dass Bedarf besteht, grundlegende Zusammenhänge stärker auch für Personen mit wenig Vorwissen oder kognitiven Beeinträchtigungen zugänglich zu machen. Eine inklusive Wissenschaftskommunikation fördert dabei nicht nur die Demokratisierung des Wissens, sondern verbessert im besten Fall auch die Qualität und Relevanz von Forschung. Statt einer Konzeption von Wissenschaft als objektiv und universell, als Vermittlung von ‚reinen' Fakten, geht es bei einem solchen Verständnis um die Berücksichtigung von Perspektivität, Praxiswissen und dezentraler Wissensbestände. Das Projekt *DiversPrivat* arbeitet auch in dieser Hinsicht an entsprechenden Vorschlägen und Maßnahmen.

des Schutzbedarfs abzubilden. Hierbei sind Kategorien erst anhand der Gefahren und Schutzbedarfe in den konkreten Situationen zu entwickeln. Gerade Privacy Literacy und das Abstellen auf „Durchschnittsnutzende" wird den konkret vorliegenden Vulnerabilitäten und Schutzbedarfen nicht gerecht. Viszerale Reize könnten hierbei ein Ansatz sein, um Grenzen der Privacy Literacy zu begegnen. Doch auch viszerale Reize sind dort keine Lösungen, wo strukturelle oder regulatorische Ansätze anstelle individualisierter Lösungen notwendig sind. Viszerale Reize könnten jedoch nicht nur bestimmte vulnerable Personen mit geringer Privacy Literacy bei der Wahrung ihrer Privatheit unterstützen, sondern grundsätzlich alle. Der Schutz besonders vulnerabler Personen ist schließlich oft auch ein Schutz aller.

Danksagung

Diese Arbeit wurde im Rahmen des vom BMFTR geförderten Projekts *DiversPrivat* (Förderkennzeichen: 16KIS1879) durchgeführt.

Literatur

Acquisti, Alessandro; Brandimarte, Laura und Hancock, Jeff (2022)*:* How privacy's past may shape its future. *Science***,** 375, S. 270-272. https://doi.org/10.1126/science.abj0826

Albertson Fineman, Martha (2017): Vulnerability and inevitable inequality. *Oslo Law Review*, 4(3), S. 133-149. https://doi.org/10.18261/issn.2387-3299-2017-03-02

Artikel-29-Datenschutzgruppe (2018): Leitlinien in Bezug auf die Einwilligung gemäß Verordnung 2016/679. Working Paper 259 rev. 01. Brüssel. URL: https://www.datenschutz-bayern.de/datenschutzreform2018/wp259rev01_de.pdf.

Behrendt, Hauke und Loh, Wulf (2022): Informed consent and algorithmic discrimination – is giving away your data the new vulnerable? *Review of Social Economy,* 80(1), S. 58–84. https://doi.org/10.1080/00346764.2022.2027506.

Birnbacher, Dieter (2012): Vulnerabilität und Patientenautonomie – Anmerkungen aus medizinethischer Sicht. *MedR,* 30(9), S. 560–565. https://doi.org/10.1007/s00350-012-3223-1.

Brough, Aaron R. und Martin, Kelly D. (2020): Critical roles of knowledge and motivation in privacy research. *Current opinion in psychology*, 31, S. 11-15. https://doi.org/10.1016/j.copsyc.2019.06.02

Calo, Ryan (2011): Against notice skepticism in privacy (and elsewhere). *Notre Dame L. Rev.*, 87, S. 1027.

Castro Varela, María do Mar und Heinemann, Alina (2016): Globale Bildungsbewegungen – Wissensproduktionen verändern. *ZEP: Zeitschrift für internationale Bildungsforschung und Entwicklungspädagogik*, 39(2), S. 17–22. https://doi.org/10.25656/01:15447.

Damm, Reinhard (2013): Vulnerabilität als Rechtskonzept? *Medizinrecht*, 31(4), S. 201-214. https://doi.org/10.1007/s00350-013-3389-1.

Davis, Benjamin P. und Aldieri, Eric (2021): Precarity and Resistance: A Critique of Martha Fineman's Vulnerability Theory. *Hypatia,* 36(2), S. 321–337. https://doi.org/10.1017/hyp.2021.25.

Gardenswartz, Lee und Rowe, Anita (2003): *Diverse teams at work. Capitalizing on the power of diversity.* Alexandria, Virginia, USA.: Society for Human Resource Management.

Geminn, Christian L. (2023): *Deus ex machina? Grundrechte und Digitalisierung*. Tübingen: Mohr Siebeck.

Hagendorff, Thilo (2018): Privacy Literacy and Its Problems. *Journal of Information Ethics,* 27(2), S. 127–145.

Kiener, Maximilian (2023): *Voluntary consent. Theory and practice*. New York: Routledge Taylor & Francis.

Koch, Heiner (2013): Gemeinsame antipatriarchale Kämpfe und die Ontologie von Gender und Herrschaft. *Kollektivität nach der Subjektkritik. Geschlechtertheoretische Positionierungen*, 153-176.

Koch, Heiner (2014): Probleme der Normalisierung. In: Regina Ammicht Quinn (Hg.): *Sicherheitsethik*. Wiesbaden: Springer VS (Studien zur Inneren Sicherheit, Band 16), S. 167–181.

Kroschwald, Steffen (2023): Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften Schutz, Selbstbestimmung und Teilhabe „by Design" vor dem Hintergrund des Art. 25 DSGVO und dem KI-Verordnungsentwurf. *Zeitschrift für Digitalisierung und Recht*, 1/2023, S. 1-22.

Liedke-Deutscher, Bernd (Hrsg.): (2024): *Die datenschutzrechtliche Einwilligung nach der DSGVO*. Oldenburg: OlWIR.

Linabary, Jasmine R. und Corple, Danielle J. (2019): Privacy for whom?: A feminist intervention in online research practice. *Information, Communication & Society,* 22(10), S. 1447–1463. https://doi.org/10.1080/1369118X.2018.1438492.

Luna, Florencia (2009): Elucidating the concept of vulnerability: Layers not labels. *IJFAB: International Journal of Feminist Approaches to Bioethics,* 2(1), S. 121–139. https://doi.org/10.3138/ijfab.2.1.121

Martin, Angela K. (2023): *The Moral Implications of Human and Animal Vulnerability.* Cham: Springer International Publishing.

Nebel, Maxi (2015): Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung? Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht. *Zeitschrift für Datenschutz,* 11/2015, S. 517-521.

Racine, Eric und Bracken-Roche, Dearbhail (2019): Enriching the concept of vulnerability in research ethics: An integrative and functional account. *Bioethics*, 33(1), S. 19–34. https://doi.org/10.1111/bioe.12471.

Rodriguez-Priego, Nuria; van Bavel, René, und Monteleone, Shara (2021): Nudging online privacy behaviour with anthropomorphic cues. *Journal of Behavioral Economics for Policy*, 5(1), 45-52.

Roßnagel, Alexander; Pfitzmann, Andreas und Garstka, Hansjürgen (2001): Gutachten im Auftrag des Bundesministeriums des Innern. Modernisierung des Datenschutzrechts. Berlin. URL: http://www.datenschutzgeschichte.de/pub/dphistory/2001_GarskaPfitzmannRossnagel_Modernisierung_des_Datenschutzrechts.pdf (besucht am 27.02.2025).

Roßnagel, Alexander; Bile, Tamer; Nebel, Maxi; Geminn, Christian; Karaboga, Murat; Ebbers, Frank; Bremert, Benjamin; Stapf, Ingrid; Teebken, Mena; Thürmel, Verena; Ochs, Carsten; Uhlmann, Markus; Krämer, Nicole; Meier, Yannic; Kreutzer, Michael; Schreiber, Linda und Simo, Hervais (2020): White Paper Einwilligung. Möglichkeiten und Fallstricke aus der Konsumentenperspektive. Karlsruhe: Fraunhofer ISI. URL: https://doi.org/10.24406/publica-fhg-300317.

Roßnagel, Alexander und Geminn, Christian (2020): *Datenschutz-Grundverordnung verbessern: Änderungsvorschläge aus Verbrauchersicht.* Baden-Baden: Nomos.

Roßnagel, Alexander (2020): Der Datenschutz von Kindern in der Datenschutz-Grundverordnung: Vorschläge für die Evaluierung und Fortentwicklung. *Zeitschrift für Datenschutz (ZD)*, S. 88.

Schrögel, Philipp; Humm, Christian; Leßmöllmann, Annette; Kremer, Bastian; Adler, Jona und Weißkopf, Markus (2018): Nicht erreichte Zielgruppen in der Wissenschaftskommunikation: Literatur-Review zu Exklusionsfaktoren und Analyse von Fallbeispielen. Berlin: Wissenschaft im Dialog gGmbH; Karlsruher Institut für Technologie (KIT), Institut für Technikzukünfte (ITZ), Teilinstitut Wissenschaftskommunikation. URL: https://doi.org/10.5445/IR/1000094529.

Strauß, Stefan und Bettin, Steffen (2023): Digitalisierung, Vulnerabilität und (kritische) gesellschaftliche Infrastrukturen. Wien: Institut für Technikfolgen-Abschätzung der Österreichischen Akademie der Wissenschaften. https://doi.org/10.1553/ITA-pb-2023-01.

Trepte, Sabine; Teutsch, Doris; Masur, Philipp K.; Eicher, Christopher; Fischer, Mona; Hennhöfer, Alisa und Lind, Fabienne (2015): Do people know about privacy and data protection strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). *Reforming European data protection law*, S. 333-365. https://doi.org/10.1007/978-94-017-9385-8.

Wartenberg, Thomas E. (1990): *The forms of power: From domination to transformation.* Philadelphia, USA: Temple University Press, U.S.

Wrigley, Anthony (2014): An Eliminativist Approach to Vulnerability. *Bioethics*, 29(7), S. 478-487. https://doi.org/10.1111/bioe.12144

Personalisierung von Werbung – wer, was, warum und wie? Eine soziologische Perspektive darauf, wie Betroffene datenverarbeitende Organisationen personifizieren

Maximilian Lukat und Volkan Sayman

Zusammenfassung
Internetnutzerinnen stehen täglich vor der Herausforderung, zu entscheiden, welche Risiken sie mit der Einwilligung zur Verarbeitung personenbezogener Daten zur Personalisierung von Werbung in Kauf nehmen und welche Vorteile sie erwarten. Dies stellt normativ eine Herausforderung für die informationelle Selbstbestimmung der Betroffenen dar. Für Nutzer: innen sind viele der aktuellen Methoden und Formate zur Informierung über die Datenverarbeitung bei personalisierter Werbung und Personalisierung im Internet unzureichend, überkomplex und unwirksam. Zudem mangelt es an verständlichen Grundlagen, die für Verarbeitungszwecke und Interventionsmöglichkeiten Transparenz herstellen könnten. Das Forschungsprojekt „Sicher im Datenverkehr" (SiD)[1] untersucht in einem nutzer:innenorientieren Ansatz, wie Menschen die Verarbeitung ihrer Daten, insbesondere der Risiken und Chancen wahrnehmen. Dazu wurde eine qualitative empirische Studie zur Rekonstruktion von Deutungsmustern von Laien in Bezug auf die Verarbeitung ihrer personenbezogenen Daten mit dem Zweck der Personalisierung von Werbung durchgeführt. Eine zentrale Erkenntnis dabei ist, dass Betroffene *datenverarbeitende Organisationen häufig personifizieren*, indem sie ihnen individuelle Absichten und Handlungsmacht zuschreiben. Dieses und weitere Deutungsmuster wie die *Analogien der Nutzer:innen zu anderen alltäglichen Situationen*, *die Verantwortlichkeit für Interventionen und Alternativen bei der Datenverarbeitung* und *die Manipulierbarkeit der Nutzer:innen* aus dem aktuellen Forschungsprojekt SiD, sowie praktische Anknüpfungspunkte, werden in diesem Beitrag besprochen. Aus den Erkenntnissen ziehen wir Schlüsse für verbesserte, d.h. an die Deutungsmuster und lebensweltlichen Wissensbestände der befragten Laien anschließende Informations- und Einwilligungsdialoge.

1. Einleitung

Die Umsetzung des Rechts auf informationelle Selbstbestimmung bei der Verarbeitung personenbezogener Daten zur Personalisierung von Inhalten und Werbung ist bisher unbefriedigend. Es gibt viele Unklarheiten für Nutzer:innen, die daraus resultieren, dass die bisherigen Lösungen, die informationelle Selbstbestimmung ermöglichen sollen, nicht wirksam funktionieren. Dies wiederum ist eine Folge dessen, dass Datenverarbeiter die Nutzung personenbezogener Daten für passgenaue Personalisierung und in der Regel auch zur Vermarktung von Inhalten als Selbstverständlichkeit

1 Gefördert vom Bundesministerium für Bildung und Forschung, Förderkennzeichen 16KIS1968

betrachten. Für viele Betroffene erscheinen die gesetzlichen Grundlagen, Zwecke der Datenverarbeitung, technische Verfahren und Interventionsmöglichkeiten jedoch intransparent.

Im Projekt SiD forschen wir zu neuen Wegen, informationelle Selbstbestimmung herzustellen und über Risiken, Vorteile und Interventionsmöglichkeiten aufzuklären. Teil des Problems ist, dass der Diskurs sehr juristisch und technisch geprägt ist und Informations- und Einwilligungsdialoge stark von den Perspektiven dieser Fachcommunities ausgehend gestaltet sind. Die so geprägte Aufklärung ist aber nicht unbedingt besonders zugänglich für Nutzer:innen. Insbesondere stehen Nutzer:innen vor der Herausforderung, die Informationen zur Verarbeitung personenbezogenen Daten auf ihnen vertraute lebensweltliche und gesellschaftliche Kontexte zu beziehen und daraus Schlüsse für ihren persönlichen Umgang mit den (positiven wie negativen) Konsequenzen der Verarbeitung ihrer personenbezogenen Daten zu ziehen. Der von uns verfolgte nutzer:innenzentrierte Ansatz wird dabei helfen, methodisch kontrolliert nachzuvollziehen, wie Betroffene zentrale Elemente der in der EU-Datenschutzgrundverordnung (DSGVO) zum Teil verpflichtenden Informierung deuten. Zu diesen Elementen zählen zum Beispiel gesetzliche Grundlagen, Zwecke der Datenverarbeitung, technisch-organisatorische Infrastruktur und Risiken. Weiter lassen sich mit dem Ansatz die Deutungen zu Deutungsmustern systematisieren. Theoretisch gehen wir davon aus, dass Nutzer:innen eine Vorstellung davon haben, was passiert, wenn Inhalte personalisiert werden, da sie ihre Alltagswelt in einer gesellschaftlich vorstrukturierten Weise deuten (Berger/Luckmann 1980). Im Sinne des Sozialkonstruktivismus nehmen wir eine analytische Perspektive auf die Wirklichkeitskonstruktionen gesellschaftlicher Akteur:innen ein und enthalten uns einer Bewertung der Korrektheit oder Angemessenheit der Deutungsmuster von Betroffenen.

Relevant ist vielmehr, dass diese Vorstellungen in Form von Deutungsmustern vorliegen. Auf Grundlage der im Folgenden vorgestellten Ergebnisse der empirischen Analyse werden wir im weiteren Projektverlauf Informations- und Einwilligungsdialoge entwickeln, die gezielt die Deutungsmuster von Betroffenen in der Gestaltung der Kommunikationsschnittstelle berücksichtigen.

In diesem Beitrag legen wir den Schwerpunkt auf die Konzeption, Erhebung und zentralen Erkenntnisse aus der qualitativen Analyse der Deutungsmuster von betroffenen Laien in Bezug auf Personalisierung und personalisierte Werbung. Zunächst wird auf die theoretische Rahmung eingegangen und die Herleitung der Fragestellung erörtert. Anschließend wird

kurz das empirische Design unserer Studie erklärt und darauffolgend ein Deutungsmuster ausführlich dargelegt. Abschließend diskutieren wir die Ergebnisse mit Hinblick auf den avisierten Anwendungsbezug im weiteren Projektverlauf und leiten einige Empfehlungen ab.

2. Einordnung in den Forschungsstand

Die Verarbeitung personenbezogener Daten ist trotz ihrer Alltäglichkeit für Nutzer:innen weitgehend unsichtbar (Christl 2017). Die Verarbeitung personenbezogener Daten dient im Fall der Personalisierung von Werbung der Analyse der Interessen und Präferenzen der Betroffenen (Roßnagel 2007), wovon sich die Werbetreibende und Unternehmen Ad-Tech-Industrie unter anderem versprechen, die Relevanz der Werbeinhalte für potenzielle Kund:innen zu steigern und dadurch deren Kaufverhalten zu beeinflussen. Zur Kontrolle der daraus resultierenden Grundrechtsrisiken definiert die DSGVO-Regeln für Verarbeiter personenbezogener Daten. Das gesetzliche Erfordernis verständlicher und zugleich umfassender Informationen als Grundlage für Einwilligungen erscheint dabei nahezu als Widerspruch in sich. Die DSGVO erkennt in diesen Umständen – der Komplexität, Alltäglichkeit sowie der relativen Unsichtbarkeit der Datenverarbeitung – signifikante Risiken für die Grundrechte und deren Ausübung. Sie reagiert darauf mit zahlreichen Vorschriften, die Verarbeiter:innen personenbezogener Daten anzuwenden haben, allen voran zur Zweckbindung, Transparenz und Intervenierbarkeit (insb. zur Einwilligung).

Für die wirksame Informierung im Kontext Einwilligung braucht es also eine einfach zugängliche Benutzer:innenschnittstelle, über die Verarbeiter:innen personenbezogener Daten nicht nur formal-rechtlich ihren allgemeinen Informationspflichten nachkommen, wie die gängigen Cookie-Banner. Die Betroffenen müssen auch die Möglichkeit haben, ihr Auskunftsrecht über die konkret vorhandenen Daten sowie die weiteren Betroffenenrechte, insbesondere das Recht auf Berichtigung und Löschung, nutzerfreundlich wahrnehmen zu können. So kann eine wirksame Risikokontrolle gewährleistet werden. Voraussetzung ist jedoch die Entwicklung von Metriken, Methoden und Verfahren, anhand derer die aus Nutzer:innensicht wirksame Ausgestaltung sichergestellt und nachgewiesen werden kann.

Die weiter unten vorgestellte Analyse der Deutungsmuster von Betroffenen soll ein mit empirischen Methoden abgesichertes Verständnis der men-

talen Risikomodelle der Nutzer:innen schaffen. Sie ist insbesondere für die verständliche Gestaltung der Visualisierung von Grundrechtsrisiken unerlässlich, um die Informierung von Betroffenen so zu gestalten, dass sie an juristische Diskurse über Grundrechte und Grundrechtsrisiken anschließt und zugleich alltagstauglich über entstehende Risiken angemessen aufklärt, d.h. wirksam ist. Mit anderen Worten: Datenschutz durch Technikgestaltung erfordert eine Wissensbasis, die keine übermäßigen Anforderungen an „digital literacy" stellt und trotzdem praktisch handhabbar bleibt. Dieses Verständnis der mentalen Risikomodelle der Nutzer:innen ist schon deshalb notwendig, um nicht die Datenschutz- und Privatsphärevorstellungen der Forscher:innen und Gestalter:innen selbst zu reproduzieren. Denn die Nutzer:innenvorstellungen, ebenso wie die von Expert:innen (Friedewald et al. 2022), sind erheblich geprägt von den Privatsphäre- und Datenschutznarrativen, die in der öffentlichen wie der fachlichen Debatte dominieren und die eine Mischung aus drei Charakteristika darstellen: Erstens lässt sich eine Verengung der Diskurse in den Bereichen Datenschutz, Privacy und Surveillance auf Probleme der individuellen Privatheit beobachten (Pohle 2022). Zweitens ist die Debatte stark von negativ besetzten Begriffen wie „Missbrauch", „Überwachung" oder „Angriff" geprägt. Und drittens sind exzeptionalistische, also gerade nicht alltagstaugliche Risikobilder weit verbreitet, etwa die Beobachtung durch Geheimdienste oder „Hacker" als Akteure oder das chinesische Sozialkreditsystem als Dystopie.

Cookie-Banner klären die Nutzer:innen weder wirksam darüber auf, was mit ihren Daten geschieht, noch geben sie ihnen eine wirksame Kontrolle über die mit der Datenverarbeitung verbundenen Risiken (Utz et al. 2019). Der Grund für dieses Umsetzungsversagen ist dabei dreierlei: Erstens fehlen Nutzer:innen alltagstaugliche Narrative für die gedankliche Durchdringung der Risiken für ihre Grundrechte (vgl. Gaycken 2011). Zweitens fehlen Metriken, Methoden und Verfahren, anhand derer die Umsetzung entsprechender Transparenz- und Kontrollmaßnahmen an den jeweiligen Benutzer:innenschnittstellen auf ihre Wirksamkeit hin entwickelt, evaluiert, getestet und bestenfalls zertifiziert werden kann (Jakobi et al. 2022). Und drittens fehlen entsprechend entwickelte Benutzer:innenschnittstellen, die im Hinblick auf Risikoverständnis und -kontrolle aus Nutzer:innensicht wirksam sind.

Methoden zur Messung und Ansätze zur Verbesserung von Lesbarkeit und Verständlichkeit zielen dabei vor allem auf die Beschreibung der Datenverarbeitungspraktiken der Verantwortlichen (z.B. Bui et al. 2021) und der verwendeten personenbezogenen Daten ab (z.B. Bhatia, Breaux

2015), nicht aber auf die dabei betroffenen Grundrechte und -freiheiten oder auf die damit einhergehenden Risiken. Aus diesem Mangel an Transparenz folgt, dass den Nutzer:innen abverlangt wird, aus der Auflistung der verarbeiteten Daten und der Beschreibung der Datenverarbeitungszwecke und -praktiken auf die Grundrechtsrisiken zu schließen. Die Nutzer:innen ziehen diese Schlüsse je nach ihrer lebensweltlichen Erfahrung – etwa mit digitalen Technologien, medial verbreiteten Schadensereignissen oder der eigenen Verletzlichkeit – und bringen ihre Vorstellungen über die zu erwartenden Risiken ein. Es gibt auch eine große Zahl an empirischen Arbeiten zu Privatheitsrisiken und Privatheitsrisikovorstellungen (Kang et al. 2015), jedoch finden sich keine empirischen Untersuchungen der spezifisch grundrechtsbezogenen Risikovorstellungen von Nutzer:innen, vor allem nicht in Bezug auf personalisierte Werbung, geschweige denn sonstigen personalisierten Inhalten. Diesem Mangel will das Projekt SiD abhelfen, indem es die empirisch ermittelten Risikovorstellungen der Nutzer:innen mit den juristisch abgesicherten Aussagen über Grundrechtsrisiken abgleicht und damit zugleich eine wichtige Forschungslücke schließt.

Während in der Literatur häufig von „Dark Patterns" und „Nudging" die Rede ist (Grafenstein et al. 2018), stellt sich hier aus soziologischer Betrachtung zunächst die Frage der generellen Handlungsbeeinflussung über die Bereitstellung von Information und erst darauffolgend die Frage nach Sanktionierung bestimmter Verhaltensweisen oder ihrer Verunmöglichung (Gläser et al. 2018). Es gibt bereits Vorarbeiten zu den Auswirkungen von Zweckspezifizierungen auf Einwilligungshandlungen und die Wahrnehmung von Betroffenenrechten (Grafenstein et al. in review) sowie zu den Effekten von Android-Berechtigungsdialogen auf die Gewährung derselben (Smith & Muszynska 2019). Dringend erforderlich ist jedoch weitergehende Forschung zu den Auswirkungen des jeweiligen Designs auf die Verständlichkeit von Datenschutzrisiken sowie zu geeigneten Wirksamkeitsmetriken und Nachweismethoden, wie sie im Projekt SID erarbeitet werden.

3. Theoretische Rahmung

Mit der wissenssoziologischen Diskursanalyse gehen wir davon aus, dass soziale Deutungsmuster individuelle und kollektive Erfahrungen Bedeutung verleihen und dadurch intersubjektiv geteilten Sinn stiften

„Als allgemeine, typisierbare Bestandteile gesellschaftlicher Wissensvorräte stehen sie [Deutungsmuster; V.S.] für individuelle und kollektive Deutungsarbeit zur Verfügung und werden in ereignisbezogenen Deutungsprozessen aktualisiert. Eine Deutung ist die Verknüpfung eines allgemeinen, typisierten Deutungsmusters mit einem konkreten referentiellen Anlass. [...] Diskurse bauen auf mehreren, spezifisch gebündelten und mehr oder weniger ausgreifenden Grundmustern der Deutung, und den konkreten Elementen ihrer Manifestation (Beispiele, Symbole, Statistiken, Bilder, u.a.m.) auf." (Keller 2011, S. 131f).

Das Zitat verdeutlicht die zentrale Rolle des gesellschaftlichen Wissensvorrats in der Konstitution gesellschaftlicher Wirklichkeit. Zudem verweist das Zitat darauf, dass Wissen nicht in unstrukturierter Form in Diskursen vorliegt, sondern eine bestimmte Gestalt hat, eine „Wissensgestalt" (Keller 2007, S. 21). Diskurse wie der um Datenschutz oder über Grundrechte sind keine abstrakt-überindividuellen Strukturen. Es handelt sich dabei nicht um Strukturen, die den Subjekten bestimmte Weltwahrnehmungen und Sprechweisen kraft ihres Abstraktionsgrades oder ihrer normativen Richtigkeit aufzwingen. Vielmehr werden, wie Keller argumentiert, Diskurse inhaltlich durch sozio-kulturelle Deutungsmuster, Klassifikationen, Phänomstrukturen und Narrative Strukturen inhaltlich strukturiert und dadurch im Handeln wirksam. Deutungsmuster als eine Form der inhaltlichen Strukturierung sind dabei „[...] ein historisch-interaktiv entstandenes, mehr oder weniger komplexes Interpretationsmuster für weltliche Phänomene, in dem Interpretamente mit Handlungsorientierungen, Regeln u.a. verbunden werden." (Keller 2007, S. 21). Umgekehrt inkorporieren Akteur:innen in Sozialisationsprozessen Deutungsmuster und richten ihr Denken, Handeln, Deuten und Wirken in der Welt danach aus. Wichtig ist festzuhalten, dass die Inkorporierung und Beherrschung von Deutungsmustern durch Individuen nicht damit gleichzusetzen ist, dass diese die ihnen zur Verfügung stehenden Deutungsmuster unhinterfragt reproduzieren. Deutungsmuster entfalten bereits ihre handlungsorientierende Wirkung insofern auf sie Bezug genommen wird: „Das kann sowohl bewusste wie unbewusste, affirmative, kritische, ablehnende und kreative Bezugnahmen einschließen." (Keller 2007, S. 21).

Ein klassisches Beispiel für ein Deutungsmuster ist das des „Risikos". Als kollektives, sozial typisiertes und historisch eingebettetes Deutungsmuster fungiert es als Schema, um aktuelle Ereignisse, Handlungen und diskursive wie nicht-diskursive Praktiken zu deuten. „'Risk' is a good example for one such modern frame which structures the perception of and action towards

certain socio-technical complexes (e.g. nuclear energy, waste incineration, genetically modified plants)" (Keller 2005, S. 27).

Der Datenschutzdiskurs wird, wie potentiell jeder Diskurs, von mehreren Deutungsmustern inhaltlich strukturiert. Das Deutungsmuster des „Risikos" ist eines, das neben dem der „digitalen Souveränität" (Pohle et al. 2023), der „Selbstbestimmung" und „Sicherheit" (Petri 2010) relevant gemacht wird.

Abschließend möchten wir darauf verweisen, dass sich die Analyse von Deutungsmustern eines Diskurses sehr gut mit der inhaltlich strukturierenden qualitativen Inhaltsanalyse als einem Instrument zur Auswertung (Kodierung) und Methodenreflexion verbinden lässt (Keller 2007, S. 31f).

4. Empirie und Methode: Erhebung, Auswertung und Interpretation

Da es bisher wenig Forschung zu der Perspektive von alltäglichen Internetnutzer:innen auf personalisierte Werbung im Internet gibt, wurde für das Forschungsdesign ein qualitativer explorativer Ansatz gewählt. Es sollen Akteure, Handlungen und Datenverarbeitungsweisen aus Sicht von alltäglichen Internetnutzer:innen rekonstruiert werden. Da die bisherige Forschung zu dem Thema vor allem juristisch und technisch geprägt ist, sind diese Perspektiven besonders wertvoll, um alltagsnahe Erkenntnisse für Verbesserungen der informationellen Selbstbestimmung zu finden.

Zur Bearbeitung der Forschungsfrage wurden 18 problemzentrierte Interviews und zwei Gruppendiskussionen durchgeführt. Das problemzentrierte Interview eignet sich nach Andreas Witzel (2000) besonders dafür, die Sicht von Akteuren auf ein Problem festzuhalten und durch induktives Vorgehen Erkenntnisse zu erlangen. Durch die Struktur der problemzentrierten Interviews wird den Teilnehmenden zunächst größtmögliche Freiheit bei der Erzählung ihrer Erfahrungen gegeben. Durch den Fokus auf die persönlichen Erfahrungen der Teilnehmenden wird sichergestellt, dass Befragte Framings und Wörter von den Interviewern übernehmen.

Für die Befragung wurden Personen gesucht, die das Internet auf einem einfachen, alltäglichen Level nutzen und sich nicht professionell oder extensiv mit Datenschutz, Personalisierung oder dahinterstehenden Technologien auseinandersetzen. Die Stichprobe der Einzelinterviews ist eine convenience sample, wurde also pragmatisch ausgewählt, und umfasst 18 Personen, von sich keine als divers, neun als weiblich und neun als männlich identifiziert haben. Es wurde eine gleichmäßige Altersverteilung

angestrebt, die erreicht werden konnte. Es war jedoch schwierig, jüngere Teilnehmende für die Befragung zu finden. Außerdem handelte es sich bei den Teilnehmenden hauptsächlich um Akademiker:innen. Es stellte sich des weiteren heraus, dass einige der Teilnehmer:innen mehr Vorwissen hatten, als ursprünglich erwartet. Diese beiden Probleme wurden zwar zu umgehen versucht, indem bei der Rekrutierung das Internetnutzungsverhalten und der Beruf abgefragt wurden, ließen sich aber nicht ganz vermeiden. Die Stichprobe der zwei Gruppendiskussionen umfasste zusammen 15 Teilnehmer:innen (acht Männer, sieben Frauen, null Divers), vorwiegend im Alter von 40 Jahren und aufwärts. Die Rekrutierung der Teilnehmenden fand über eine Social Media Kampagne, sowie über direkte Ansprache auf der Straße und das Verteilen von Infozetteln in Nachbarschaftszentren in Berlin statt.

Da in der Gruppendiskussion hauptsächlich Aspekte zur Sprache kamen, die bereits in den Einzelinterviews identifiziert wurden, gingen wir davon aus, dass keine weiteren unbekannten Punkte auftauchen würden. Daher haben wir keine Einzelinterviews nacherhoben.

Die offene Interviewmatrix wurde in vier Themenfelder aufgeteilt. Diese Themenfelder orientieren sich an der Untersuchung aus dem Text „Technological frames: making sense of information technology in organizations“ (Orlikowski & Gash 1994). Darin wird versucht, eine Übersicht zu entwickeln, wie Technologien von Mitgliedern einer Organisation wahrgenommen werden. Orlikowski und Gash halten fest, dass Beobachtungen von Nutzer:innen über Technologien in drei Kategorien einsortiert werden können: 1. „Nature of Technology“, was sich auf das Verständnis von Personen über Möglichkeiten und Funktion von Technologie bezieht; 2. Gründe, warum eine Technologie zum Einsatz kommt und 3. wie Technologie eingesetzt wird und welche Konsequenzen dies hat (ebd. S. 183f). Zwar sind die bei uns untersuchen Personen nicht Mitglied einer datenverarbeitenden Organisation, aber sie verwenden alle personalisierte Angebote, also das Produkt einer datenverarbeitenden Organisation. Aus dem Framework leiten sich die ersten drei Themenfelder „Was ist Personalisierung? Wie findet Personalisierung statt? Und warum findet Personalisierung statt?“ ab. Das vierte Themenfeld „Interventionen/Datenschutz“ ergab sich aus unserem Interesse herauszufinden welche Handlungsmöglichkeiten aus Sicht der Laien bisher zum Umsetzen der informationellen Selbstbestimmung bestehen und wo aus ihrer Sicht konkrete Anknüpfungspunkte für Verbesserungen sind.

Die Themenfelder klopfen die Erfahrungen ab, die die Laien im Umgang mit Personalisierung und personalisierter Werbung im Internet gesammelt haben und wie ihr Bild über diese Technologie konstituiert ist. Witzels Methode entsprechend, wurde zunächst ein offener Erzählimpuls gesetzt, anschließend weiter gefasste und spezifische Nachfragen dazu gestellt. Nachfragen wurden ad hoc aus dem Gesprächsverlauf entwickelt sowie den vorbereiteten Aufrechterhaltungs- und Präzisierungsfragen der Matrix entnommen. Die Fragematrix der Gruppendiskussionen orientierte sich an den gleichen Themenfeldern und Fragen.

Die Erhebung fand von März bis August 2024 statt. Die Einzelinterviews haben hauptsächlich online oder telefonisch stattgefunden. Die Gruppendiskussionen fanden vor Ort in den Räumlichkeiten des Humboldt Instituts für Internet und Gesellschaft in Berlin statt. Die Gespräche wurden aufgezeichnet und mit der Software „Trint" transkribiert. Es wurde keine Glättung vorgenommen. Pausen und Betonungen wurden nicht verschriftlicht, da sie bei der qualitativen Inhaltsanalyse nicht mit ausgewertet werden. Satz- oder Wortabbrüche wurden zur besseren Lesbarkeit mit einem „ / " gekennzeichnet. Die Interviews haben eine durchschnittliche Länge von 30 bis 45 Minuten. Die Kürzel der Gesprächspartner:innen setzen sich wie folgt zusammen: Die erste Zahl ist fortlaufend, der Buchstabe M oder W kennzeichnet die Geschlechtsidentität der Teilnehmer:innen und das letzte Zahlenpaar das Alter. 11W55-64 bezeichnet also die elfte Teilnehmerin und diese befindet sich in der Altersspanne zwischen 55 und 64.

Tabelle 1: Zusammensetzung der Stichprobe

Altersgruppe	Männlich	Weiblich
18-24	1	1
25-34	2	2
35-44	0	2
45-54	2	1
55-65	1	3
65+	3	0

Das so generierte Interviewsample (Tabelle 1) wurde in einer qualitativ strukturierenden Inhaltsanalyse nach Kuckartz und Rädiker (2022) computergestützt in MAXQDA2022 ausgewertet. Diese Methode eignet sich laut den Autoren, um alle Formen menschlicher Kommunikation zu strukturieren und kann deshalb sowohl für Interviews als auch für Videos, Chats oder sonstige Aufzeichnungen der Kommunikation verwendet werden

(ebd., S. 40ff.). Als deduktive Kategorien wurden zunächst Akteure, Folgen positiv und Folgen negativ eingeführt, da ein zentrales Erkenntnisinteresse die Auswirkungen bzw. Grundrechtsrisiken sind, die Laien bei Personalisierung und personalisierter Werbung im Internet sehen. Anschließend wurde das Kategoriensystem im ersten Codiergang induktiv erweitert, anschließend ähnliche Kategorien zusammengeführt und ein weiteres Mal codiert.

Das Kategoriensystem (Tabelle 2) strukturiert das Material anhand der Kernaspekte, die für Personalisierung von Werbung ausschlaggebend sind. Aus diesen lassen sich die Sichtweisen der Laien in Form von Deutungsmustern rekonstruieren.

Diese Deutungsmuster lassen sich wiederum zu Karten bzw. Maps der Sozialen Welten der alltäglichen Internetnutzer:innen verbinden. Dies ist für diesen Beitrag aber nicht vorgesehen.

5. Deutungsmuster

In unserer Untersuchung haben wir mehrere Deutungsmuster aus den Interviews mit den Internetnutzer:innen rekonstruiert. Bisher haben wir vier Deutungsmuster ausführlicher anhand des empirischen Materials rekonstruiert. Diese vier Deutungsmuster sind die Analogien der Nutzer:innen zu anderen alltäglichen Situationen, die Verantwortlichkeit für Interventionen und Alternativen bei der Datenverarbeitung, die Manipulierbarkeit der Nutzer:innen und die Personifizierung von datenverarbeitenden Organisationen. Bevor wir das für diesen Beitrag zentrale Deutungsmuster der Personifizierung von Organisationen vorstellen, sollen die weiteren Erkenntnisse aufgeführt werden, da sie beispielsweise für eine Neugestaltung von Informations- und Einwilligungsdialogen relevant sein können und einen weiteren Einblick in unseren aktuellen Forschungsstand geben.

Zunächst war im Material besonders auffällig, dass die befragten Internetnutzer:innen ihre Erfahrungen mit personalisierter Werbung und Personalisierung häufig auf *Situationen übertragen, die sie aus der analogen Welt* kennen. Damit ist gemeint, dass sie sich in Bezug auf potenzielle Risiken und Auswirkungen, positiv oder negativ, auf bekannte Situationen beispielsweise mit Zeitungen oder dem Fernsehen beziehen und dies zur Abschätzung vergleichen. Ein Beispiel dafür wäre, dass den Befragten bewusst ist, dass auch im Fernsehen oder der Zeitung die Werbung an eine Zielgruppe angepasst ist.

Tabelle 2: Kategoriensystem der Auswertung

Kategorie	Definition	Beispiel aus dem Material
Akteure	Erzählungen zu beteiligten Akteuren	Also vielleicht die Plattform oder Unternehmen, die ihre Sachen verkaufen wollen oder ihre Inhalte verbreiten wollen. (7W18, Pos. 27)
Datenverarbeitung	Erzählungen zu Abläufen der Datenverarbeitung	für mich persönlich, […] interessieren sich nicht so viele Leute, aber ich als quasi Zielgruppe oder Gruppe an jungen Frauen, dass da ganz viele Daten gesammelt werden, um so ein Durchschnitts Profil anlegen zu können, um besser herauszufinden, was die Zielgruppe dann interessiert. (12W27, Pos. 33)
Folgen	Auswirkungen der Personalisierung	ich vertraue dann ja quasi einem Unternehmen darauf, dass die mich so gut kennen, dass sie quasi meinen Geschmack bestimmen. (12W27, Pos. 39)
Positiv	Positiv empfundene und erwünschte Auswirkungen	„[…] das sind Effekte, um meine Werbung schlagkräftiger und effektiver zu machen. Ich meine, das sehe ich als durchaus zulässig an, unterhalb eines gewissen Niveaus, das wieder nervt" (3M65, Pos. 51)
Negativ	Negativ empfundene und unerwünschte Auswirkungen	Aber dieses, dass es so eine direkte Reaktion auf meine Recherche ist, das ist, glaube ich, wirklich der kritische Punkt (4M25, Pos. 26)
Interventionen	Nutzer:innen bekannte Interventionsmöglichkeiten auf Personalisierung	„[…] versuche ich immer, dass ich sämtliche Cookies soweit es geht ablehne und auch ansonsten, dass ich halt über Browser Add on, äh die ganzen Tracking und Werbe Sachen grundsätzlich gar nicht erst zulasse, so wie No-Skript oder You-Block (5M18, Pos. 6)
Beispiele aus der analogen Welt	Beispiele der Teilnehmenden die sich nicht auf das Internet beziehen	[…] ganz ohne Personalisierung klappt ja nie […] natürlich gibt es ein Prinzip oder Konzept dahinter, wie Schaufenster dekoriert sind 12W27 Pos. 55

In Bezug auf Alternativen und Interventionen wurde eine Differenzierung zwischen der *Verantwortlichkeit* der Nutzer:innen und der Datenverarbeiter festgestellt. So sahen einige Befragte eher sich selbst in der Verantwortung, durch ihr Handeln zu bestimmen, welche und wie viele ihrer Daten für personalisierte Werbung und Personalisierung verwendet werden. Andere Befragte wiesen den datenverarbeitenden Organisationen die Verantwortung zu, für eine gesetzmäßige und datensparsame Verarbeitung zu sorgen.

Ein weiterer Punkt, der oft genannt wurde, ist die *Manipulierbarkeit* der Nutzer: innen. Hier wurden vor allem zwei Sichtweisen genannt. Zum einen, dass die Nutzer:innen vermuten, dass sie manipuliert werden, beispielsweise durch Nudging zum ungewollten Kauf von Produkten. Zum

anderen wurde vor allem von älteren Befragten häufig die Sichtweise geäußert, dass sie sich nicht manipulieren lassen, da sie nach eigenen Angaben die eingeblendete Werbung ignorieren.

Das Deutungsmuster der *Personifizierung* von Organisationen wollen wir nun ausführlich vorstellen.

5.1. Personifizierung

Eine zentrale Beobachtung unserer Analyse ist, dass die befragten Laien in ihren Erzählungen die datenverarbeitenden Organisationen personifizieren. Sie thematisieren datenverarbeitende Organisationen so, als ob es einzelne, reale Personen wären, die die erhobenen Daten verarbeiten und einsehen können. Gleichzeitig äußern sie ihr Unbehagen darüber, dass reale Personen die erhobenen Daten und Informationen einsehen können. Aus den Aussagen lässt sich außerdem schließen, dass dies eine unerwünschte Folge ist.

> „Also [...] eines meiner größten No-Gos [ist], dass halt irgendwer aufgrund meines Nutzerverhalten im Internet Sachen darüber ablesen kann, wie ich die Welt, in der ich in Zukunft lebe, gestalten möchte. Weil sowas möchte ich über Wahlen und sonst wie zu Kenntnis geben." (5M18, Pos. 44)

In dieser Aussage ist die Personifizierung besonders durch die Ansprache „irgendwer" zu erkennen. Weiter stellt der Teilnehmer eine Verbindung zu einer Vorhersagenutzung und einer potentiell politischen Nutzung der erhobenen Daten her. Dies wird ganz explizit als unerwünscht formuliert.

In der nächsten Aussage beschreibt eine Betroffene, wie sie die Datenverarbeitung wahrnimmt und welche Aspekte sie als unerwünscht ansieht. Konkret beschreibt sie, was bei ihr ein Unwohlsein auslöst.

> „Ich weiß nicht, was konkret passieren könnte, aber ich hätte ein sehr ungutes Gefühl davon, meine sämtlichen Gewohnheiten jemandem anzuvertrauen, von dem ich nichts weiß. Einer Maschine sozusagen zu, Mein komplettes, meinen kompletten Tagesablauf [...], meine Gewohnheiten öffentlich zu machen sozusagen. Hätte ich ein Problem." (11W55-64, Pos. 35)

Einerseits kann diese Aussage so interpretiert werden, dass aus Sicht der Interviewteilnehmerin eine Informationsasymmetrie besteht, bei der die

datenverarbeitende Organisation mehr Informationen über die Nutzerin hat. Andererseits hat die Nutzerin keine Informationen über die datenverarbeitende Organisation, was zu einem Unbehagen führt. Zudem wird hier die datenverarbeitende Organisation als „jemand" adressiert, also als würde eine Person die erfassten Daten verarbeiten und einsehen können.

In der Regel ist es jedoch nicht so, dass eine Person diese Information einsieht oder einfach einsehen kann, da große Mengen an Daten automatisch in kurzer Zeit verarbeitet werden. Laut Art. 22 der Datenschutz-Grundverordnung haben Nutzer:innen aber das Recht darauf, nicht nur automatisierten Entscheidungen ausgesetzt zu sein, wenn diese rechtliche Auswirkungen für sie haben oder sie dadurch beeinträchtigt werden. Ohne den expliziten Wunsch der Nutzer:innen, dass reale Personen die Daten einsehen und einschätzen, passiert dies also nicht (siehe Art. 22 Abs. 2 lit. c. DSGVO). Die Einsicht und Entscheidung durch reale Personen in Ergebnisse der Datenverarbeitung ist also eher die Ausnahme als die Regel.

Trotz alledem wird diese Personifizierung vorgenommen. Ein Erklärungsansatz könnte sein, dass Betroffene dies als eine legitime Komplexitätsreduktion gesehen werden. So eine Heuristik ist in der Organisationsforschung nicht unbekannt. Meist wird das Konzept aber dazu eingesetzt, sich als Organisation von anderen Organisationen durch verinnerlichte kognitive Strukturen abzugrenzen (Albert, Ashforth & Dutton 2000, S. 13).

Das Konzept der organisationalen Identität nach Albert & Whetten (1985) versucht die Identität einer Organisation aus Sicht von Organisationen und ihren Mitgliedern anhand von zentralen, permanenten und distinktiven Merkmalen, sowie durch Erfahrungen, die von Personen mit der Organisation gesammelt wurden, zu beschreiben (Whetten 2006, S. 220). Nach dem Konzept von Albert und Whetten wird die Identität eines kollektiven Akteurs geformt durch zentrale und permanente Merkmale. Dies sind beispielsweise interne Regeln, Normen und Prozeduren einer Organisation. Weiter wird die Identität durch distinktive Merkmale geprägt, also Merkmale, die die Organisation einzigartig macht. Das können Werte und Positionen sein, für die die Organisation steht (Whetten 2006, S. 221f).

Ähnliche Zuschreibungen nehmen die Befragten in unserer Untersuchung auch vor. Dabei lassen sich aber keine dezidierten Identitäten für einzelne datenverarbeitende Organisation finden, sondern es tritt eine Identität – „die datenverarbeitende Organisation" – durch die Ansprache von Person(en) hervor.

Das äußert sich wie folgt. Unter den zentralen und permanenten Merkmalen können im Interviewmaterial zum einen alle Aspekte gefasst werden,

die mit dem Sammeln von Daten zusammenhängen, da dies die Punkte waren, die am häufigsten von den Interviewteilnehmenden in Bezug auf Ihre Erfahrungen mit personalisierter Werbung und Personalisierung im Internet genannt wurden, beispielsweise die beteiligten Akteure, und was gesammelt wird. Als beteiligte Akteure sehen die Befragten unter anderem die Websitebetreiber, so wie die Werbetreibenden. Die Werbenetzwerke, die die Verbreitung technisch realisieren, sind für die Betroffenen meistens keine bekannten Akteure. Weiter denken sie, dass eine automatische Auswertung ihres Nutzungsverhaltens und ihrer Interessen passiert. Gleichzeitig besteht die Vermutung, dass die Ergebnisse dieser Auswertung durch Menschen begutachtet werden kann oder wird. Daraus resultierend berichten sie von einem Unwohlsein, weshalb sich diese Auswertung aus Perspektive der befragten Nutzer:innen als eine unerwünschte Auswirkung interpretieren lässt.

Als zentrales distinktives Merkmal lässt sich in der Untersuchung vor allem die Vertrauenswürdigkeit der Organisationen ausmachen. So haben sie einigen Organisationen gegenüber mehr Vertrauen, wie beispielsweise Behörden oder dem öffentlich-rechtlichen Rundfunk. Dem Großteil der datenverarbeitenden Organisationen, wie Werbetreibenden wird dieses Vertrauen jedoch nicht ausgesprochen. Besonders relevant ist dabei für die Nutzer:innen eine Angst vor der potenziellen Weitergabe von Informationen über sie.

Die datenverarbeitende Organisation zeichnet sich aus Sicht unserer Befragten also dadurch aus, dass sie alle möglichen Daten zu ihrem Nutzungsverhalten und Interessen erfasst. Dazu gehören auch potenziell reale Personen, die Ergebnisse dieser Auswertung sehen können und dass die Nutzenden in den meisten Fällen kein Vertrauen gegenüber datenverarbeitenden Organisationen haben.

5.2. Zusammenfassung

Wie bereits erwähnt, ist das hier dargestellte Deutungsmuster der Personifizierung von datenverarbeitenden Organisationen ist nur eines von mehreren Deutungsmustern, die wir in unserem Projekt rekonstruiert haben. Sie hier weiter zu skizzieren wäre zu umfassend, erwähnenswert sind sie für die weitere Forschung aber definitiv.

Wie sich die Ergebnisse unserer Analyse in weitere Veröffentlichungen einbinden lassen, entweder in die Gestaltung von Bildungsmaterialien oder

Informations- und Einwilligungsdialogen, wird in den nächsten Schritten noch ausgearbeitet. Einen Ausblick darauf geben wir nun.

6. Ausblick

Die aus unserem Interviewmaterial rekonstruierten Deutungsmuster lassen sich zu Karten oder Maps der sozialen Welten der alltäglichen Internetnutzer:innen zusammenfügen. Diese können übersichtlich darstellen, wie die Sicht von Betroffenen auf personalisierte Werbung und Personalisierung im Internet konstituiert ist. Im Abgleich mit der Sicht von Expert:innen lassen sich Schnittpunkte und Leerstellen identifizieren, an denen angesetzt werden kann, um besser über Risiken und Vorteile von Personalisierung aufklären zu können. Im Moment arbeiten wir an der Ausarbeitung der Betroffenen- und Expert:innenrisikomodelle, also eines dokumentierten Abgleichs der einzelnen Inhalte der Risikomodelle. Drei Anknüpfungspunkte unserer bisherigen Forschungsergebnisse werden wir nun besprechen.

6.1. Identität der Datenverarbeitenden Organisationen schärfen

Unsere Analyse hat gezeigt, dass die Beziehung der Betroffenen zu den datenverarbeitenden Organisationen eine wichtige Rolle spielt. Denn das Vertrauen, das die Betroffenen den datenverarbeitenden Organisationen entgegenbringen, entscheidet darüber, ob sie in die Datenverarbeitung einwilligen. Einerseits konnten wir häufig feststellen, dass die Teilnehmenden vor allem bekannten Akteuren, wie z.B. staatlichen Institutionen, mehr Vertrauen entgegenbringen. Andererseits trauen sie bestimmten Akteuren einen verantwortungsvollen Umgang mit Daten gar nicht zu, etwa wenn es sich um große Technologiekonzerne handelt. Gerade dort herrscht aus Sicht der Betroffenen auch eine große Intransparenz, die paradoxerweise eigentlich auch gegenüber staatlichen Institutionen vorherrschen müsste, da auch dort nicht ad hoc überprüft werden kann, wie die Datenverarbeitung abläuft. Für das von vielen Befragten geäußerte Unbehagen gegenüber der Personalisierung im Internet dürfte diese Intransparenz mitverantwortlich sein.

Um dieses Problem zu lösen, sollte in weiteren Arbeiten darüber nachgedacht werden, wie die Identität(en) von datenverarbeitenden Organisatio-

nen geschärft werden können, um mehr Transparenz und Vertrauen zu schaffen.

Dabei sollte es jedoch nicht nur darum gehen, dass sich die Organisationen anders oder besser darstellen, sondern es müsste ebenfalls überlegt werden, ob die Einflussfaktoren auf die Identität, also die Datenverarbeitungspraktiken, ebenfalls geändert werden müssen. Denn letztendlich sind es diese Praktiken, die unerwünschte Folgen für Betroffene hervorrufen und das Bild der Organisationen prägen.

6.2. Deklaration der Datenverarbeitungszwecke

Ein Punkt, der eine solche Transparenz schaffen soll, existiert bereits in Form der Angabe der Zwecke für die Erhebung verschiedener Daten in den Cookie-Bannern. Unsere Ergebnisse deuten darauf hin, dass die bisher deklarierten Zwecke nicht klar genug sind. Mehr Komplexität und mehr Informationen sind aber auch nicht unbedingt die richtige Lösung, da genau dies im Vorfeld als Problem gesehen wurde. Eine Lösung für das Problem der Zweckspezifizierung könnte beispielsweise darin bestehen, in Cookie-Bannern zu deklarieren, welche Datenverarbeitungen mit den erhobenen Daten explizit nicht durchgeführt werden. Dies ist darauf zurückzuführen, dass die Betroffenen in unseren Interviews häufig auch darüber gesprochen haben, was sie explizit nicht wollen bzw. wofür ihre Daten explizit nicht verarbeitet werden sollen. Darüber hinaus könnte auch explizit auf die Vorteile der Personalisierung bzw. der jeweiligen Datenverarbeitung eingegangen werden. Dies entspräche eher der Sichtweise der Betroffenen.

6.3. Neue Interventionsmöglichkeiten

Um ganz konkrete Verbesserungen der informationellen Selbstbestimmung herzustellen, wären Privacy Dashboards oder Transparenz Dashboards, in denen die Nutzer:innen dezidiert und übergreifend Einstellungen zu personalisierter Werbung und Personalisierung vornehmen können eine Lösung. Einige Unternehmen wie Google bieten solche Möglichkeiten bereits an.

Seitenübergreifende Lösungen fallen unter den Begriff Personal Information Management System (PIMS). Ein Projektpartner aus unserem Konsortium arbeitet an einem Demonstrator für ein solches System. Die Erkennt-

nisse aus unserer Forschung mit Betroffenen und Expert:innen sollen in die Entwicklung und Gestaltung dieses Demonstrators einfließen.

Ein Ansatz zur Verwendung unserer Forschungsergebnisse in dem Demonstrator ist die Entwicklung von Personas, also knappen Beschreibungen von in bestimmten Hinsichten markanten Persönlichkeitstypen. Diese Personas dienen als Bezugspunkt, um Anforderungen an die Gestaltung des Demonstrators im Anschluss an die Bedürfnisse typischer Betroffener abzuleiten.

In einem PIMS könnten solche Personas weiterverwendet werden, um über bestimmte Voreinstellungen zu entscheiden. Wenn das PIMS erstmals konfiguriert wird, könnten die Nutzer:innen eine Persona auswählen, mit der sie sich identifizieren und davon ausgehend weitere Einstellungen vornehmen. Ein Problem bei der Implementierung einer solchen Gestaltung als Entscheidungsgrundlage wird sein, dass die Datenschutzaufsichtsbehörden durch ihre Rechtsauslegung eine informierte Einwilligung mit ausführlicher Aufklärung als Goldstandard ansehen. Andere Designs von Informations- und Einwilligungsdialogen, die einen grundlegend anderen Ansatz verfolgen, werden es daher in der realen Umsetzung schwer haben. Doch ist es gerade diese komplexe Art der Aufklärung, die die Nutzer:innen kontraintuitiv und intransparent finden und die weitgehend unwirksam ist.

Literatur

Albert, S., & Whetten, D. A. (1985). Organizational identity. *Research in Organizational Behavior, 7*, 263–295.

Albert, S., Ashforth, B. E., & Dutton, J. E. (2000). Organizational identity and identification: Charting new waters and building new bridges. *Academy of Management Review, 25*(1), 13–17.

Bhatia, J., & Breaux, T. D. (2015). Towards an information type lexicon for privacy policies. In *2015 IEEE Eighth International Workshop on Requirements Engineering and Law (RELAW*) (pp. 19–24).

Bui, D., Shin, K. G., Choi, J. M., & Shin, J. (2021). Automated extraction and presentation of data practices in privacy policies. *Proceedings on Privacy Enhancing Technologies, 2021*(2), 88–110. https://doi.org/10.2478/popets-2021-0019

Christl, W. (2017). *Corporate surveillance in everyday life – How companies collect, combine, analyze, trade, and use personal data on billions*. Cracked Labs.

Friedewald, M., Schiering, I., Martin, N., & Hallinan, D. (2022). Data protection impact assessments in practice – Experiences from case studies. In S. Katsikas et al. (Eds.), *Computer Security. ESORICS 2021. Lecture Notes in Computer Science* (Vol. 13106, pp. 424–443).

Gaycken, S. (2011). Informationelle Selbstbestimmung und narrativistische Rezeption – Zur Konstruktion informationellen Vertrauens. *DuD – Datenschutz und Datensicherheit, 35*(5), 346–350.

Gläser, J., Guagnin, D., Laudel, G., Meister, M., Schäufele, F., Schubert, C., & Tschida, U. (2018). *Technik vergleichen: ein Analyserahmen für die Beeinflussung von Arbeit durch Technik. AIS-Studien, 11*(2), 124–142. https://doi.org/10.21241/ssoar.64869

Grafenstein, M. v., Jakobi, T., & Stevens, G. (in review, minor changes). *Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-centered UX-design methods. Computer Law & Security Review.*

Jakobi, T., Grafenstein, M. v., Smieskol, P., & Stevens, G. (2022). A taxonomy of user-perceived privacy risks to foster accountability of data-based services. *Journal of Responsible Technology*. https://doi.org/10.1016/j.jrt.2022.100029

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "My data just goes everywhere": User mental models of the internet and implications for privacy and security. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security (SOUPS '15)* (pp. 39–52). USENIX Association.

Keller, R. (2005). Wissenssoziologische Diskursanalyse als interpretative Analytik. In R. Keller (Ed.), *Die diskursive Konstruktion von Wirklichkeit: Zum Verhältnis von Wissenssoziologie und Diskursforschung* (pp. 251–277). UVK.

Keller, R. (2007). Diskurse und Dispositive analysieren. Die Wissenssoziologische Diskursanalyse als Beitrag zu einer wissensanalytischen Profilierung der Diskursforschung. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 8*(2). https://doi.org/10.17169/FQS-8.2.243

Keller, R. (2011). *Diskursforschung: Eine Einführung für SozialwissenschaftlerInnen* (4. Aufl.). VS Verlag.

Kuckartz, U., & Rädiker, S. (2022). *Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung: Grundlagentexte Methoden, Grundlagentexte Methoden.* Beltz Juventa.

Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: Making sense of information technology in organizations. *ACM Transactions on Information Systems, 12*(2), 174–207. https://doi.org/10.1145/196734.196745

Petri, T. (2010). Sicherheit und Selbstbestimmung: Deutsche und europäische Diskurse zum Datenschutz. *Datenschutz und Datensicherheit - DuD, 34*(8), 539–543. https://doi.org/10.1007/s11623-010-0186-0

Pohle, J. (2022). Datenschutz: Rechtsstaatsmodell oder neoliberale Responsibilisierung? Warum Datentreuhänder kein Mittel zum Schutz der Grundrechte sind. In Verbraucherzentrale NRW e. V. (Ed.), *Zu treuen Händen? Verbraucherdatenschutz und digitale Selbstbestimmung*. https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-05-pohle-datenschutz-rechtsstaatsmodell-oder-neoliberale-responsibilisierung_0.pdf

Pohle, J., Thüer, L., Dammann, F., & Winkler, J. (2023). Das Subjekt im politischen Diskurs zu „digitaler Souveränität". In N. Kersting, J. Radtke, & S. Baringhorst (Eds.), *Handbuch Digitalisierung und politische Beteiligung* (pp. 1–23). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-31480-4_12-1

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

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19)* (pp. 973–990). ACM. https://doi.org/10.1145/3319535.3354212

Whetten, D. A. (2006). Albert and Whetten revisited: Strengthening the concept of organizational identity. *Journal of Management Inquiry, 15*(3), 219–234.

Witzel, A. (2000). The problem-centered interview. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, 1*(1). https://doi.org/10.17169/fqs-1.1.1132

Erkenntnisse zur Verbesserung von Datenschutz in Plattformökonomien: Transparenz, Intervenierbarkeit und User Experience im Fokus

Lennart Kiss, Rachelle Sellung, Björn Hanneke und Lorenz Baum

Zusammenfassung
Transparenz und Intervenierbarkeit sind zentrale Prinzipien der DSGVO, doch ihre praktische Umsetzung bleibt herausfordernd. In diesem Beitrag wird untersucht, wie Datenschutz durch gezielte Gestaltung von technischen Hilfssystemen in Plattformökonomien effektiver gestaltet werden kann, um Nutzerrechte verständlich und anwendbar zu machen. Dieses Ziel wird fortlaufend als Datenschutzinitiative bezeichnet. Im Rahmen des PERISCOPE-Projekts wurden interdisziplinäre Methoden aus User Experience, Recht und Ökonomie kombiniert, um Datenschutzmaßnahmen aus verschiedenen Perspektiven zu bewerten. Empirische Studien mit Endnutzern und Plattformbetreibern zeigen, dass bestehende Datenschutzlösungen oft schwer verständlich sind und Nutzerrechte durch komplexe Prozesse eingeschränkt werden. Die Forschung hebt hervor, dass eine transparente Kommunikation, nutzerfreundliche Gestaltung und gezielte Interaktivität entscheidend für die Akzeptanz und Wirksamkeit von Datenschutzinitiativen sind. Zudem werden wirtschaftliche Faktoren analysiert, die Unternehmen zur Implementierung datenschutzfreundlicher Modelle motivieren können. Dieser Beitrag leitet konkrete Handlungsempfehlungen für die Weiterentwicklung nutzerzentrierter Datenschutzstrategien ab und betont die Notwendigkeit einer ganzheitlichen Integration von Regulierung, Technologie und Nutzererwartungen.

1. Einleitung: User Experience und Datenschutz

Datenschutz ist zu einem zentralen Anliegen von Nutzenden, Unternehmen und Gesetzgebern geworden. Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union setzt mit ihren Anforderungen an Transparenz und Intervenierbarkeit wesentliche Standards für einen nutzerfreundlichen Datenschutz. Trotz der formalen Vorteile dieser Grundsätze bleibt ihre praktische Umsetzung eine Herausforderung. Dieser Beitrag stammt aus der Forschung des vom Bundesministerium für Bildung und Forschung, Technologie und Raumfahrt geförderten PERISCOPE-Projekts[1], das datenschutzfreundliche Lösungen für kleine und mittelständische Unternehmen (KMUs) entwickelte.

1 Die Forschung des PERISCOPE-Projekts wurde vom Bundesministerium für Bildung und Forschung, Technologie und Raumfahrt gefördert. https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/periscope.

Zwei der wichtigsten Ergebnisse des PERISCOPE-Projekts sind ein Privacy Friendly Business Model Recommender Tool[2] und ein Personal Rights Management System.

Das Privacy Friendly Business Model Recommender Tool von PERISCOPE wurde entwickelt, durch Forschung validiert und im PERISCOPE-Projekt implementiert. Ziel dieses Demonstrators ist es, Geschäftsmodelle von Plattformanbietern mit einem Privacy-Score zu bewerten und Verbesserungsvorschläge zu liefern. Dieses Tool hilft, die Privatssphärenfreundlichkeit von Geschäftsmodellen zu messen und zu vergleichen und quantifiziert das Engagement für Privatsphäre in Geschäftsmodellen. Die Methodik dieser Anwendung ist durch verschiedene Studien des Projekts validiert[3]. Darüber hinaus entwickelte PERISCOPE ein Personal Rights Management System als Demonstrator, das sowohl für den Plattformanbieter als auch für den Verbraucher konzipiert wurde. Das Tool kann genutzt werden, um den Nutzern mehr Transparenz über ihre Datennutzung und Möglichkeiten zur Intervenierbarkeit zu bieten, sowie um die Bearbeitung der ausgeübten Betroffenenrechte für die Plattformbetreiber zu erleichtern. Die Ergebnisse des PERISCOPE-Projekts sind auf der Projektwebsite veröffentlicht[4]. Die Entwicklung des Demonstrators basiert auf den verschiedenen Zwischenergebnissen und der Forschung des Projekts[5].

Durch einen interdisziplinären Forschungsansatz untersucht die Studie, wie Datenschutzinitiativen aus der Sicht von User Experience, dem Recht und der Ökonomie verbessert werden können. Die Ergebnisse dieser Untersuchung liefern Erkenntnisse für die Gestaltung effektiver Datenschutzmaßnahmen und präsentieren konkrete Implikationen zur Weiterentwicklung datenschutzfreundlicher Technologien.

---

2 https://privacy.wiim-research.de

3 *Hanneke/Baum/Schnuck/Hinz*, DuD 2024; Tool siehe https://aisel.aisnet.org/icis2024/security/security/3/.

4 Für die Ergebnisse des PERISCOPE Projekts siehe: https://websites.fraunhofer.de/periscope-projekt/?page_id=490 (zuletzt abgerufen am 23.05.2025).

5 Näher *Hanneke/Baum/Schlereth/Hinz*, ICIS 2023.; *Hanneke/Baum/Hinz*, ECIS 2023.; *Astfalk/Schunck*, LNI, Open Identity Summit 2023.; *Pfeiffer/Astfalk/Baum/Haneke/Schunck/Winterstetter*, in: Friedewald u.a. (Hrsg.), Daten-Fairness in einer globalisierten Welt, Nomos, 2023, S. 117–144.; *Pfeiffer*, Datenzugang in der Plattformökonomie: *Regulierungsinstrumente in P2B-VO, DMA und DSA*, in: Buchheim u.a. (Hrsg.), Plattformen. Grundlagen und Neuordnung des Rechts digitaler Plattformen, 2024, S. 53–76.; *Schmitt/Schunck/Lo Iacono*, Ökosysteme – Neue Herausforderungen für den Datenschutz, 2024.; *Pfeiffer*, in: Augsberg u.a. (Hrsg.), Datenzugangsregeln. Zwischen Freigabe und Kontrolle, 2024, S. 101–136.

Diese Forschungsarbeit umfasste mehrere Studien mit einer diversifizierten Nutzergruppe, darunter Tiefeninterviews, Usability-Tests und quantitative Online-Umfragen mit realen Anwendern. Die Teilnehmer repräsentierten verschiedene demografische Gruppen, um unterschiedliche Perspektiven zu gewährleisten. Das Projekt konzentrierte sich auf mehrere Schlüsselaspekte, die durch die Studien untersucht werden sollten. Als erstes wurde die (1) Wahrnehmung von Betroffenenrechten untersucht, also wie Endnutzer, die ihnen durch die DSGVO gewährten Rechte wahrnehmen und verstehen. Ein weiteres zentrales Thema war (2) die Transparenz der Plattformen und Intervenierbarkeit durch Endnutzer. Es wurde die Rolle von Transparenz bei der Vermittlung von Datenschutzinformationen und dessen Einfluss auf die Nutzererfahrung untersucht. Darüber hinaus wollten wir herausfinden, wie einfach es für Nutzer ist, ihre Rechte durchzusetzen und in Datenschutzprozesse einzugreifen. Schließlich betrachteten wir auch (3) die Perspektive weiterer Stakeholder, insbesondere die Sichtweisen der Plattformbetreiber auf Datenschutz und ihre Bereitschaft, Lösungen zu adaptieren, bei denen Transparenz und Intervenierbarkeit im Vordergrund stehen.

Im Folgenden werden die Erkenntnisse aus den verschiedenen Studien, Anforderungsdefinitionen und Bewertungen sowie die Erkenntnisse aus den Demonstrationsumsetzungen des PERISCOPE-Projekts dargelegt und reflektiert. Die nachfolgenden Abschnitt stellen die zentralen Ergebnisse dieser Untersuchungen dar: Abschnitt 2 eröffnet mit einem theoretischen Hintergrund zu den Aspekten der Transparenz und Intervenierbarkeit, Abschnitt 3 erläutert das Forschungsdesign und die durchgeführten Studien, Abschnitt 4 präsentiert interdisziplinäre Erkenntnisse aus der Perspektive der User Experience (UX), des Rechts und der Ökonomie, Abschnitt 5 leitet konkrete Implikationen für die Gestaltung künftiger Datenschutzinitiativen ab, Abschnitt 6 diskutiert die Limitationen der Forschung sowie potenzielle zukünftige Forschungsansätze, und Abschnitt 7 fasst die zentralen Erkenntnisse zusammen und zieht ein abschließendes Fazit.

2. Theoretischer Hintergrund: Transparenz und Intervenierbarkeit als Schlüssel für nutzerfreundlichen Datenschutz

Transparenz und Intervenierbarkeit werden allgemein als wesentliche Bestandteile eines nutzerzentrierten Datenschutzes anerkannt, doch ihre

praktische Umsetzung ist nach wie vor mit Herausforderungen verbunden. Zwar sind Transparenz (Art. 5 Abs. 1 lit. a DSGVO) und Intervenierbarkeit (Art. 15–21 DSGVO) in der Datenschutz-Grundverordnung formell verankert, doch ist es alles andere als einfach, sicherzustellen, dass diese Rechte zu einer wirkungsvollen Kontrolle für die Betroffenen führen. Verantwortliche sind verpflichtet, Informationen in „präziser, transparenter, verständlicher und leicht zugänglicher Form" bereitzustellen (Art. 12 Abs. 1 DSGVO), aber in der Praxis bleiben Datenschutzhinweise schwer verständlich,[6] Einwilligungsmechanismen beruhen oft auf sogenannten „Dark Patterns"[7] und das Volumen der Datentransaktionen erschwert die Übersicht für die Betroffenen.

Die Möglichkeit der Intervention ist nicht nur eine Frage der gesetzlichen Rechte, sondern auch der technischen Machbarkeit. Während die DSGVO das Recht auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO) und Datenübertragung (Art. 20 DSGVO) vorschreibt, haben viele Organisationen mit fragmentierten Datenarchitekturen und Altsystemen zu kämpfen, die eine rasche Umsetzung dieser Rechte erschweren.[8] Plattformen verarbeiten große Mengen an Benutzerdaten in Echtzeit, und die Beantwortung von Anfragen innerhalb der vorgeschriebenen einmonatigen Frist (Art. 12 Abs. 3 DSGVO) kann logistisch anspruchsvoll sein. Darüber hinaus ist die Wirksamkeit der Intervenierbarkeit begrenzt, wenn datengesteuerte Geschäftsmodelle auf personenbezogene Daten als Kernbestandteil angewiesen sind. Einige Verantwortliche schrecken auf subtile Weise Nutzer von Löschanfragen ab, indem sie bewusst Reibungspunkte einführen – mehrstufige Prozesse, Verzögerungen oder unvollständige Datenlöschungen –, was Bedenken aufwirft, ob die Datenschutz-Grundverordnung immer wirksam ausgeübt wird.

Über die Einhaltung von Vorschriften hinaus erschwert die sich entwickelnde technologische und rechtliche Landschaft diese Grundsätze zusätzlich. Automatisierte Personalisierung, algorithmische Entscheidungsfindung und Echtzeit-Datenhandel stellen traditionelle Vorstellungen von Transparenz und Benutzerkontrolle in Frage. Regulierungsbehörden und

6 *Tesfay* u.a., Privacy Guide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation, 2018, S. 15-21.

7 *Nouwens* u.a., in ACM (Hrsg.), Proceedings of the CHI Conference on Human Factors in Computing Systems, 2020, 1–13.

8 *Shah* u.a., in USENIX (Hrsg.), Proceedings des 11th Workshop on Hot Topics in Storage and File Systems (HotStorage), 2019.

Wissenschaftler setzen sich zunehmend für Technologien zur Verbesserung der Transparenz (*Transparency enhancing Technologies*, TETs) und automatisierte Datenschutz-Tools ein, aber die Akzeptanz dieser Lösungen ist uneinheitlich, insbesondere bei KMU, denen die Ressourcen für robuste Compliance-Infrastrukturen fehlen.[9]

Daher geht es nicht mehr primär darum, ob Transparenz und Intervenierbarkeit gesetzlich verankert sind, sondern vielmehr darum, wie sichergestellt werden kann, dass sie in einer zunehmend komplexen, datengesteuerten Ökonomie wirkungsvoll umgesetzt werden. Die Diskrepanz zwischen rechtlichen Vorgaben und praktischer Umsetzung wirft zentrale Fragen auf: Sind Nutzer tatsächlich in der Lage, informierte Entscheidungen zu treffen, oder führen Transparenzpflichten lediglich zu einer Flut juristischer Offenlegungen? Lässt sich Intervenierbarkeit in einem Umfeld effektiv skalieren, in dem personenbezogene Daten kontinuierlich verarbeitet, analysiert und weitergegeben werden? Um diesen Herausforderungen zu begegnen, bedarf es nicht nur einer konsequenten Durchsetzung regulatorischer Anforderungen, sondern auch technologischer Innovationen und bewährter branchenweiter Ansätze, die nicht nur dem Wortlaut, sondern auch dem Geist der DSGVO gerecht werden.

3. Forschungsdesign: Nutzererfahrungen mit Datenschutz-Tools

Dieser Beitrag untersucht, wie verschiedene Stakeholdergruppen das PERISCOPE-System wahrnehmen und nutzen. Um ein umfassendes Verständnis über die Nutzererfahrungen mit Datenschutz-Tools zu gewinnen, wurden verschiedene empirische Untersuchungen durchgeführt. Dabei lag der Fokus insbesondere auf den Aspekten Transparenz, Intervenierbarkeit und User Experience. Ziel war es, herauszufinden, wie unterschiedliche Stakeholder das Tool wahrnehmen, welche Herausforderungen sie bei der Ausübung von Betroffenenrechten erleben und inwiefern entworfene Lösungen ihre Erwartungen erfüllen. Die erhobenen Daten liefern Erkenntnisse über multidisziplinäre Aspekte solcher Initiativen, insbesondere im Hinblick auf die User Experience, rechtliche Rahmenbedingungen und ökonomische Einflussfaktoren.

Um verschiedene Perspektiven auf Datenschutzinitiativen zu erfassen, wurde ein Methodenmix eingesetzt, der qualitative und quantitative An-

9 *Kergroach*, SMEs Going Digital, 2021.

sätze kombiniert. Die Endnutzerperspektive wurde durch Usability-Tests und eine Online-Umfrage untersucht, während die Sichtweise der Stakeholdergruppe der Plattformbetreiber anhand qualitativer Tiefeninterviews erfasst wurde. Durch diese methodische Herangehensweise konnten sowohl praktische Nutzungshürden als auch strategische Herausforderungen bei der Implementierung und Anwendung des PERISCOPE-Tools identifiziert werden.

Die Usability-Tests wurden mit Endnutzern des PERISCOPE-Tools durchgeführt, um deren Interaktion mit dem System systematisch zu analysieren. Im Rahmen dieser Tests wurden Fragen zur Wahrnehmung von Datenschutzpräferenzen, zu auftretenden Hürden sowie zur empfundenen Schwierigkeit einzelner Testaufgaben gestellt. Zusätzlich kamen standardisierte Messinstrumente wie die System Usability Scale und das User Experience Questionnaire zum Einsatz, um die Benutzerfreundlichkeit und Nutzererfahrung des Systems in einem vergleichbaren Rahmen zu bewerten. Zusätzlich wurde die allgemeine Zufriedenheit der Teilnehmenden untersucht, insbesondere im Hinblick auf die Erfüllung ihrer Erwartungen an die Funktionen des Tools, mögliche Verbesserungsvorschläge sowie potenzielle Anwendungsgebiete.

Die Perspektive der Plattformbetreiber wurde durch leitfadengestützte Tiefeninterviews erfasst, die sich an dem Design-Science-Ansatz orientierten. In diesem Zusammenhang diente das PERISCOPE-System als Artefakt, um spezifische Herausforderungen und Anforderungen an Datenschutzinitiativen aus Sicht der Betreiber zu identifizieren. Der Fokus lag auf Erfahrungen mit der Umsetzung von Transparenz- und Intervenierbarkeitsfunktionen, auf strategischen Überlegungen zur Einführung solcher Maßnahmen sowie auf Hürden bei der praktischen Umsetzung. Die Interviews wurden inhaltsanalytisch nach den Prinzipien von Mayring[10] ausgewertet, um wiederkehrende Themen, Herausforderungen und Potenziale systematisch zu erfassen.

Ergänzend wurde eine Online-Umfrage mit realen Nutzern des PERISCOPE-Projektpartners Gohobi, ein Onlineplattformbetreiber, durchgeführt. Diese Untersuchung zielte darauf ab, allgemeine Wahrnehmungen und Nutzungsgewohnheiten im Umgang mit Datenschutzinitiativen zu erfassen. Die Teilnehmenden bewerteten ihre ersten Eindrücke in Bezug auf die Benutzerfreundlichkeit des Tools und gaben Auskunft über ihre persönlichen Datenschutzpräferenzen und ihr generelles Verhalten im Umgang

10 *Mayring*, Qualitative Content Analysis, 2021.

mit Datenschutzoptionen. Darüber hinaus wurde untersucht, inwiefern sie mit Betroffenenrechten vertraut sind und in welchem Maße sie diese in Anspruch nehmen. Zusätzlich wurde erfasst, ob die Teilnehmer bereit wären, eine datenschutzfreundliche Plattform aktiv weiterzuempfehlen und inwiefern das Vertrauen in die Plattform durch Transparenz- und Intervenierbarkeitsfunktionen beeinflusst wird. Abschließend wurde ein allgemeines Feedback zur Nutzung des Systems eingeholt, um weiterführende Erkenntnisse zur praktischen Anwendbarkeit zu gewinnen.

Durch die Kombination dieser methodischen Ansätze konnte eine fundierte Grundlage für die Analyse der Nutzererfahrungen mehrerer Stakeholdergruppen mit Datenschutzinitiativen geschaffen werden. Während die Usability-Tests praxisnahe Nutzungshürden offenlegten, ermöglichten die Tiefeninterviews eine differenzierte Betrachtung der Herausforderungen und Strategien der Plattformbetreiber. Die Online-Umfrage diente dazu, diese hauptsächlich qualitativen Erkenntnisse durch eine größere empirische Basis zu ergänzen.

4. Erkenntnisse aus der Nutzerforschung

Die empirischen Untersuchungen im Rahmen des PERISCOPE-Projekts liefern praktische Erkenntnisse darüber, wie verschiedene Nutzergruppen Datenschutzinitiativen wahrnehmen und welche Faktoren deren Akzeptanz und Nutzung beeinflussen. Dabei zeigte sich, dass Datenschutz nicht nur aus technischer oder regulatorischer Sicht betrachtet werden kann, sondern entscheidend davon abhängt, wie verständlich, zugänglich und anwendungsfreundlich entsprechende Maßnahmen gestaltet sind. Die Forschungsergebnisse verdeutlichen, dass insbesondere die User Experience, die rechtlichen Rahmenbedingungen, sowie die wirtschaftlichen Implikationen eine wesentliche Rolle für die erfolgreiche Umsetzung datenschutzfreundlicher Technologien spielen. Die folgenden Abschnitte beleuchten die zentralen Erkenntnisse aus diesen drei Perspektiven.

4.1 User Experience Erkenntnisse

Die Studien zur Nutzung des PERISCOPE-Systems verdeutlichen zentrale Herausforderungen und Gestaltungsmöglichkeiten für eine verbesserte User Experience im Kontext von Datenschutzinitiativen. Die Studien in

diesem Abschnitt basieren auf den Erkenntnissen aus mehreren Runden von User Experience-Tests, die mit einem Mix aus Methoden durchgeführt wurden, sowie auf Interviews mit Plattformanbietern und einer Umfrage unter Endnutzern. Insbesondere wurden vier Schlüsselfaktoren identifiziert, die maßgeblich zur Benutzerfreundlichkeit und Nutzererfahrung von Datenschutztools beitragen: unmittelbares Feedback und Unterstützung, Reduktion von Komplexität, visuelle Hilfsmittel und interaktive Elemente zur Förderung der Nutzerkontrolle.

4.1.1 Unmittelbares Feedback und Unterstützung

Die Analyse der Nutzerinteraktion mit dem PERISCOPE-System zeigte, dass eine fehlende Rückmeldung während der Nutzung erhebliche Unsicherheiten hervorrufen kann, insbesondere wenn es um die Wahrnehmung und Ausübung von Betroffenenrechten geht. Nutzer benötigen eine unmittelbare Bestätigung darüber, ob ihre Anfragen oder Teilschritte der Prozesse erfolgreich waren oder welche weiteren Schritte erforderlich sind, um ihre Datenschutzanliegen effektiv zu verfolgen. Unklare oder ausbleibende Rückmeldungen können zu Frustration und im schlimmsten Fall zu einem Vertrauensverlust gegenüber dem Tool führen.

Ein Ansatz zur Verbesserung der Nutzererfahrung ist die Bereitstellung von Echtzeit-Feedback, welches den Nutzern signalisiert, ob ihre Datenschutzanfragen – beispielsweise eine Datenlöschung – erfolgreich bearbeitet wurden oder ob noch weitere Aktionen erforderlich sind. Darüber hinaus können kontextbezogene Anleitungen und Tutorials integriert werden, die Nutzern schrittweise erklären, wie sie ihre Betroffenenrechte durchsetzen können. Diese Art der Unterstützung erweist sich insbesondere für weniger rechtsaffine Nutzer als essenziell, da sie eine strukturierte und verständliche Hilfestellung für komplexe Datenschutzprozesse bietet.

Neben automatisierten Hilfestellungen zeigte sich in den Untersuchungen auch, dass Nutzer in bestimmten Fällen auf direkte menschliche Unterstützung angewiesen sind. Wenn Echtzeit-Feedback und Tutorials nicht ausreichen, können persönliche Support-Optionen dabei helfen, individuelle oder komplexe Probleme effizient zu lösen. Die Möglichkeit, eine direkte Ansprechperson zu konsultieren, beeinflusst die Ausübbarkeit von Betroffenenrechten positiv.

4.1.2 Reduktion von Komplexität

Ein zentrales Ergebnis der Nutzerforschung ist, dass die Verständlichkeit von Datenschutztools maßgeblich darüber entscheidet, ob und in welchem Umfang Nutzer ihre Betroffenenrechte wahrnehmen. Die Komplexität rechtlicher und technischer Sachverhalte stellt eine signifikante Barriere dar, die dazu führt, dass Nutzer Datenschutzoptionen nur eingeschränkt oder gar nicht nutzen. Besonders problematisch ist der häufige Einsatz juristischer Fachterminologie, die für viele Nutzer schwer zugänglich ist.

Die Reduktion von Komplexität erfordert jedoch mehr als nur eine Vereinfachung von Begrifflichkeiten. Vielmehr sollte die gesamte Sprach- und Interaktionsgestaltung eines Datenschutztools darauf ausgerichtet sein, eine intuitive Nutzung zu ermöglichen. Dies umfasst die Verwendung eines verständlichen Vokabulars sowie einer klaren und strukturierten Informationsaufbereitung, die es auch weniger datenschutzaffinen Nutzern erleichtert, ihre Rechte durchzusetzen. Die Herausforderung besteht darin, eine Balance zu finden: Während die Inhalte zugänglich und verständlich sein müssen, dürfen essenzielle rechtliche und technische Details nicht verloren gehen.

Die Ergebnisse zeigen, dass eine gezielte sprachliche Vereinfachung nicht nur zu einer erhöhten Nutzerfreundlichkeit führt, sondern auch die allgemeine Akzeptanz von Datenschutzinitiativen steigert. Eine benutzerzentrierte Gestaltung der Informationsvermittlung trägt dazu bei, dass Datenschutztools als verständlich, zugänglich und somit als verlässlich wahrgenommen werden. Besteht diese Hürde weiterhin, kann nicht von informierten Entscheidungen der Nutzer ausgegangen werden.

4.1.3 Visuelle Unterstützung als Vermittlungsstrategie

Visuelle Darstellungen spielen eine wesentliche Rolle bei der Vermittlung komplexer Datenschutzinhalte. Die Studien zeigten, dass Nutzer von Infografiken, Schritt-für-Schritt-Anleitungen und weiteren visuellen Hilfsmitteln profitieren, da diese abstrakte Datenschutzkonzepte in einer leicht verständlichen Weise präsentieren. Besonders bei der Entscheidungsfindung, beispielsweise zur Ausübung eines Betroffenenrechts, erweisen sich visuelle Elemente als hilfreich, da sie strukturierte Orientierung bieten und so die kognitive Belastung der Nutzer reduzieren.

Der Einsatz von Diagrammen, Icons und interaktiven Visualisierungen kann dazu beitragen, dass Nutzer schneller erfassen, welche Datenschutz-

optionen ihnen zur Verfügung stehen und welche Konsequenzen ihre Entscheidungen haben. Durch die Reduktion textlastiger Erklärungen und die gezielte Einbindung visueller Unterstützung wird das System insgesamt benutzerfreundlicher und zugänglicher.

4.1.4 Interaktive Elemente zur Förderung der Nutzerkontrolle

Interaktivität stellt einen weiteren zentralen Faktor für eine positive Nutzererfahrung im Bereich datenschutzfreundlicher Technologien dar. Nutzer müssen das Gefühl haben, aktiv in die Verwaltung ihrer Daten eingebunden zu sein, um Vertrauen in die Funktionsweise des Systems zu entwickeln. Die Untersuchungsergebnisse zeigen, dass interaktive Funktionen wie eine dynamische Einwilligungsmanagementkomponente oder ein dialogbasierter Assistent maßgeblich dazu beitragen, dass Nutzer sich als souveräne Akteure im Datenschutzprozess wahrnehmen.

Im konkreten Fall des PERISCOPE-Systems wurde eine Chatbot-ähnliche Struktur implementiert, die Nutzern eine schrittweise Unterstützung bei der Durchsetzung ihrer Betroffenenrechte bietet. Durch diesen interaktiven Ansatz erhalten Nutzer eine gezielte Anleitung und können ihre Entscheidungen zur Datennutzung in Echtzeit anpassen. Die Möglichkeit, direkt Einfluss auf die eigenen Daten zu nehmen, förderte das Gefühl der Eigenverantwortung und zu Teilen die Motivation sich der Datenschutzthematik anzunehmen. Nutzer, die aktiv in den Datenschutzprozess eingebunden sind, zeigen eine höhere Bereitschaft, Datenschutzinitiativen nachhaltig zu nutzen und weiterzuempfehlen.

4.1.5 Zusammenfassung der User Experience Erkenntnisse

Zusammenfassend ist zu sagen, dass die Gestaltung der User Experience maßgeblich über die Akzeptanz und Wirksamkeit von Datenschutzinitiativen entscheidet. Vier zentrale Faktoren wurden als besonders relevant identifiziert: Die Bereitstellung von unmittelbarem Feedback in Form von Echtzeit-Rückmeldungen, Tutorials oder direktem Support steigert die Nutzerzufriedenheit und reduziert Unsicherheiten. Die Reduktion von Komplexität durch eine verständliche Sprache und eine intuitive Struktur senkt Nutzungshürden und fördert eine breitere Akzeptanz. Visuelle Unterstützung erleichtert die Informationsaufnahme und steigert die Effizienz bei der Entscheidungsfindung. Schließlich fördern interaktive Elemente das

Gefühl der Kontrolle und Eigenverantwortung der Nutzer, wodurch Datenschutzinitiativen als transparenter und vertrauenswürdiger wahrgenommen werden.

4.2 Rechtliche Erkenntnisse

Die rechtlichen Analysen im Rahmen des PERISCOPE-Projekts haben zentrale Herausforderungen bei der Umsetzung datenschutzrechtlicher Anforderungen innerhalb einer technischen Datenschutzinitiative offenbart. Besonders deutlich wurde, dass die späte Integration rechtlicher Vorgaben in technische Systeme zu unnötigen Anpassungskosten und ineffizienten Implementierungsprozessen führen kann. Im Fall des PERISCOPE-Projekts wurde hingegen ein Ansatz verfolgt, bei dem von Beginn an eine rechtskonforme Gestaltung im Fokus stand. Ziel war es, Plattformbetreibern, insbesondere kleinen und mittelständischen Unternehmen, ein System bereitzustellen, das sie bei der Einhaltung relevanter datenschutzrechtlicher Verpflichtungen unterstützt.

4.2.1 Fokus auf relevante rechtliche Anforderungen

Ein zentraler Aspekt bei der Entwicklung von Datenschutzinitiativen ist die frühzeitige und präzise Definition rechtlicher Anforderungen, um sicherzustellen, dass diese nicht nur theoretisch, sondern auch praktisch relevant sind. Erfahrungen aus dem PERISCOPE-Projekt zeigen, dass viele anfänglich formulierte rechtliche Vorgaben im späteren Verlauf keine unmittelbare Umsetzung erforderten oder sich als überflüssig erwiesen. Um ineffizienten Mehraufwand zu vermeiden, ist es daher essenziell, bereits zu Beginn eines Projekts einen gezielten Fokus auf diejenigen rechtlichen Anforderungen zu legen, die für die praktische Implementierung tatsächlich von Bedeutung sind. Dies betraf beispielsweise spezifische Vorgaben zur Einwilligung von Minderjährigen gemäß Art. 8 DSGVO oder regulatorische Anforderungen aus der Platform-to-Business-Verordnung und dem Digital Services Act. Eine selektive Priorisierung relevanter rechtlicher Fragestellungen kann somit nicht nur den Entwicklungsaufwand reduzieren, sondern auch die Integration rechtlicher Mechanismen in digitale Anwendungen effizienter gestalten.

4.2.2 Bedeutung der frühzeitigen Klärung der datenschutzrechtlichen Verantwortlichkeit

Eine weitere zentrale Herausforderung bestand darin, dass die datenschutzrechtliche Einordnung des späteren Bereitstellers des PERISCOPE-Systems zu Beginn des Projekts nicht eindeutig geklärt war. Unklar blieb, ob dieser als Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter oder als Softwarehersteller agieren würde. Diese Unsicherheit führte dazu, dass bestimmte datenschutzrechtliche Anforderungen in einer hohen Detailtiefe analysiert wurden, die sich im Rückblick als teilweise ineffizient herausstellte. Eine frühzeitige Festlegung der datenschutzrechtlichen Rolle des Systemanbieters hätte diesen Mehraufwand verringert und die Implementierung rechtlicher Anforderungen zielgerichteter gestaltet.

Die Ergebnisse des Projekts zeigen, dass es für die Entwicklung datenschutzkonformer Systeme essenziell ist, rechtliche Zuständigkeiten so früh wie möglich zu definieren. Insbesondere die Rolle des Anbieters eines Datenschutztools bestimmt maßgeblich, welche rechtlichen Anforderungen erfüllt werden müssen. Eine unklare Verantwortlichkeitsverteilung kann dazu führen, dass unnötige Ressourcen in rechtliche Detailanalysen investiert werden, die letztlich nicht relevant für die praktische Umsetzung sind.

4.2.3 Zusammenfassung der rechtlichen Erkenntnisse

Die im PERISCOPE-Projekt gewonnenen rechtlichen Erkenntnisse verdeutlichen, dass eine selektive Priorisierung zentraler datenschutzrechtlicher Anforderungen essenziell ist, um eine effiziente und praxisnahe Umsetzung zu ermöglichen. Anstatt von Beginn an einen umfassenden Anforderungskatalog zu entwickeln, der später in Teilen nicht relevant ist, sollte der Fokus auf wenige, aber praxisrelevante juristische Kernaspekte gelegt werden. Darüber hinaus zeigt sich, dass eine frühzeitige Klärung der datenschutzrechtlichen Verantwortlichkeit die Effizienz der Systementwicklung erheblich steigern kann. Diese Erkenntnisse tragen dazu bei, zukünftige datenschutzrechtliche Implementierungsstrategien zielgerichteter zu gestalten und unnötigen Mehraufwand in der rechtlichen Analyse zu vermeiden.

4.3 Ökonomische Erkenntnisse

Die zunehmende Bedeutung von Datenschutzinitiativen in digitalen Geschäftsmodellen offenbart nicht nur regulatorische und ethische Anforde-

rungen, sondern auch substanzielle ökonomische Potenziale. Insbesondere Transparenz über Datennutzung und Intervenierbarkeit, verstanden als die Möglichkeit der Nutzenden, aktiv Kontrolle über ihre Daten auszuüben, entwickeln sich zu zentralen Differenzierungsmerkmalen im Wettbewerb. Basierend auf drei empirischen Studien wird im Folgenden herausgearbeitet, welche ökonomischen Implikationen sich aus Transparenz- und Intervenierbarkeitsmechanismen für Konsumierende, Plattformbetreibende und Anbietende von Privacy Management Systems (PMS) ergeben.

4.3.1 Privatsphärenfreundliche Plattformgeschäftsmodelle

In einer ersten Studie wurden die Präferenzen der Nutzenden hinsichtlich der Ausgestaltung von Plattform-Geschäftsmodellen analysiert.[11] Hierzu wurde ein Recommender-System entwickelt, das auf einer adaptiven Choice-Based Conjoint Analyse (ACBC) basiert. Ziel war es, jene Tradeoffs zu identifizieren, die Konsumentinnen und Konsumenten zwischen unterschiedlichen Datenschutzmerkmalen von Geschäftsmodellen vornehmen, insbesondere im Hinblick auf Transparenz und Kontrolle.

Die Untersuchung erfolgte mit einer Stichprobe von 84 Teilnehmenden aus den Vereinigten Staaten. Bewertet wurden hypothetische Plattformkonfigurationen, die sich hinsichtlich der Datennutzung (personenbezogen, anonymisiert, keine Nutzung), der Transparenzmechanismen (etwa digitaler Datenzugriff über Dashboards) und der Möglichkeiten zur Nutzungssteuerung unterschieden.

Die Ergebnisse zeigen, dass Plattformen, die auf anonyme Datennutzung und digitalen, jederzeit verfügbaren Zugang zu persönlichen Daten setzen, von den Nutzenden signifikant bevorzugt werden. Transparenzmechanismen wie Dashboards, die einen einfachen und kontinuierlichen Datenzugriff ermöglichen, steigern den wahrgenommenen Wert einer Plattform erheblich. Somit kann eine datenschutzfreundliche Ausgestaltung von Plattformmodellen durch transparente Informationsangebote und verbesserte Intervenierbarkeit nicht nur regulatorische Vorgaben erfüllen, sondern auch als strategisches Differenzierungsmerkmal mit direktem Einfluss auf die Marktattraktivität dienen.

11 *Baum* u.a., A Recommender System for Privacy Friendly Platform Business Models. 2024

4.3.2 Nutzungspräferenzen und Zahlungsbereitschaft für Privacy Management Systemen

Eine zweite Studie[12] untersuchte die Präferenzen der Konsumentinnen und Konsumenten für Privacy Management Systems (PMS), die darauf abzielen, Transparenz über Datenverarbeitungspraktiken zu schaffen und Intervenierbarkeit durch flexible Kontrollmöglichkeiten zu gewährleisten. Hierzu wurde eine klassische Choice-Based Conjoint Analyse (CBC) mit einer repräsentativen Stichprobe von 589 Teilnehmenden aus der deutschen Internetbevölkerung durchgeführt. Im Fokus standen zentrale Attribute wie der Modus des Datenzugriffs (postalische Information, digitaler Einmalzugriff, kontinuierliches Dashboard), die Verwaltung von Einwilligungen (individuell, vorgefertigte Profile, vollständige Zustimmung) sowie verschiedene Arten der Datennutzung für Marketingzwecke.

Die Ergebnisse zeigen, dass Nutzende einen kontinuierlichen, digitalen Zugriff über Dashboards und die Möglichkeit zur granularen Steuerung von Einwilligungen deutlich bevorzugen. Anonymisierte Datennutzung wird signifikant positiver bewertet als personenbezogene oder umfassende Nutzung. Zudem zeigen die Analysen, dass Rabatte zwar einen Einfluss auf die Nutzung von PMS haben, jedoch Transparenz und Intervenierbarkeit als primäre Treiber der Akzeptanz zu betrachten sind.

Daraus ergibt sich ein klares wirtschaftliches Potenzial: Systeme, die Transparenz schaffen und Intervenierbarkeit ermöglichen, erhöhen nicht nur die Bereitschaft zur Nutzung, sondern stärken auch das Vertrauen in digitale Dienste. Anbieter, die in solche PMS investieren, können sowohl ihre regulatorische Konformität absichern als auch die Nutzerloyalität und Zahlungsbereitschaft steigern.

Auch monetäre Anreize wie Rabatte beeinflussen die Bereitschaft zur Nutzung von datengetriebenen Diensten: Ein Rabatt von 12 % kann die Nutzungswahrscheinlichkeit selbst für weniger datenschutzfreundliche Konfigurationen erhöhen – z. B. bei der schlechtesten Konfiguration von 16,8 % auf 43,3 %. Dennoch bleibt Transparenz über Datennutzungspraktiken und die Möglichkeit, individuelle Datenfreigaben einfach zu verwalten, der entscheidende Treiber für Akzeptanz und Zahlungsbereitschaft. Nutzer bevorzugen digitalen Zugriff auf ihre Daten (CBC-Nutzenbeitrag +0,39) gegenüber postalischer Zustellung (−0,41); Privacy-Dashboards wurden

12 *Hanneke* u.a., Consumer Preferences for Privacy Management Systems, 2023.

hingegen neutral bewertet (+0,02), was auf weiteres Optimierungspotenzial in der User Experience hinweist.

4.3.3 Nutzersegmentierung

Abschließend wurde in einer dritten Studie eine Clusteranalyse durchgeführt, um unterschiedliche Nutzersegmente hinsichtlich ihrer Datenschutzpräferenzen zu identifizieren.[13]

Grundlage der Segmentierung bildeten zwei latente Konstrukte: die subjektive Bedeutung von Datenschutz (Privacy Importance) und das Wissen über Datenschutzrechte (GDPR Knowledge), die eine Differenzierung der Nutzenden nach Datenschutzbewusstsein und Handlungskompetenz ermöglichen. Anhand der repräsentativen Stichprobe von 589 Teilnehmenden aus der deutschen Internetbevölkerung wurden vier Cluster bzw. Segmente identifiziert:

- *Fundamentalists* (34 %) zeichnen sich durch ein hohes Maß an Datenschutzbewusstsein und Schutzmotivation aus
- *Amateurs* (27 %) haben ein moderates Bewusstsein, aber geringes Wissen und handeln häufig situativ.
- *Pragmatists* (24 %) wägen Datenschutzbedenken gegen Nutzenüberlegungen ab und verhalten sich kontextabhängig.
- Die *Unconcerned* (15 %) messen Datenschutz nur eine geringe Bedeutung bei und priorisieren Bequemlichkeit und finanzielle Anreize.

Diese Segmentierung orientiert sich an bestehenden Einteilungen,[14] wird jedoch um die Gruppe der *Amateurs* erweitert, um aktuelle Entwicklungen wie Sensibilisierung bei gleichzeitig begrenztem Wissen über Datenschutzrechte abzubilden. Besonders die *Fundamentalists* und *Pragmatists*, die zusammen mehr als die Hälfte der Nutzenden ausmachen, zeigen eine hohe Affinität zu Angeboten, die Transparenz und Intervenierbarkeit gewährleisten.

13 *Hanneke* u.a., GDPR Privacy Type Clustering: Motivational Factors for Consumer Data Sharing, 2023.

14 Siehe z. B. *Westin*, Social and Political Dimensions of Privacy, 2003.

4.3.4 Zusammenfassung der Ökonomischen Implikationen

Die drei Studien verdeutlichen, dass Transparenz und Intervenierbarkeit nicht nur rechtliche Anforderungen bedienen, sondern wesentliche ökonomische Erfolgsfaktoren im digitalen Wettbewerb darstellen. Unternehmen, die in leicht zugängliche, transparente Informationsangebote und flexible Steuerungsmöglichkeiten für ihre Nutzenden investieren, können nicht nur regulatorische Risiken minimieren, sondern auch das Vertrauen stärken und dadurch ihre Marktposition verbessern. Die Zahlungsbereitschaft für datenschutzfreundliche Angebote ist insbesondere bei den datensensiblen Konsumentensegmenten hoch und kann durch intelligente Kombination mit Anreizsystemen gesteigert werden.

Somit eröffnen Transparenz und Intervenierbarkeit neue ökonomische Potenziale für Plattformanbietende, die zunehmend auch als strategische Assets im digitalen Wettbewerb betrachtet werden müssen.

5. Implikationen für die Gestaltung effektiver Datenschutzinitiativen

Die Gestaltung erfolgreicher Datenschutzinitiativen erfordert mehr als die Erfüllung regulatorischer Vorgaben. Eine effektive Umsetzung muss Nutzerbedürfnisse berücksichtigen, rechtliche Anforderungen praxisnah integrieren und wirtschaftliche Rahmenbedingungen einbeziehen. Die im PERISCOPE-Projekt gewonnenen Erkenntnisse zeigen, dass Datenschutzmaßnahmen nur dann nachhaltig wirksam sind, wenn sie verständlich, zugänglich und wirtschaftlich tragfähig gestaltet werden. Dabei spielen drei zentrale Dimensionen eine Rolle: User Experience, rechtliche Präzision und ökonomische Anreize. Die folgenden Prinzipien und Gestaltungsempfehlungen verdeutlichen, wie Datenschutzinitiativen sowohl aus Nutzer- als auch aus Unternehmensperspektive optimiert werden können.

Die User Experience Erkenntnisse zeigen, dass die Gestaltung von Datenschutzinitiativen maßgeblich durch die Wahrnehmungen und Erlebnisse der Nutzer bestimmt wird. Ein rein regulatorischer Ansatz reicht nicht aus, um Datenschutzmaßnahmen effektiv nutzbar zu machen. Stattdessen sollten Datenschutzlösungen gezielt so gestaltet werden, dass sie den Bedürfnissen und Erwartungen der Nutzer gerecht werden. Dazu sollten Entwickler und Unternehmen folgende Prinzipien berücksichtigen:

- *Unmittelbares Feedback bereitstellen*, um Unsicherheiten zu vermeiden und die Nutzung zu erleichtern. Echtzeit-Rückmeldungen und kontextbezogene Anleitungen helfen, Betroffenenrechte effektiv wahrzunehmen.
- *Komplexität reduzieren*, indem Fachbegriffe vermieden und Datenschutzoptionen klar strukturiert und verständlich präsentiert werden.
- *Visuelle Unterstützung nutzen*, um abstrakte Datenschutzinformationen leichter erfassbar zu machen. Infografiken und intuitive Symbole verbessern die Verständlichkeit.
- *Interaktive Elemente integrieren*, um Nutzern mehr Kontrolle zu geben. Dynamische Datenschutzeinstellungen und Chatbots erleichtern die Verwaltung persönlicher Daten.
- *Datenschutz als Nutzermehrwert* begreifen, indem Datenschutzoptionen aktiv zur positiven Nutzungserfahrung beitragen, statt als reine Pflichtinformationen zu erscheinen.

Die rechtlichen Analysen des PERISCOPE-Projekts zeigen, dass eine späte Integration rechtlicher Vorgaben zu ineffizienten Anpassungen führt. Ein frühzeitiger rechtskonformer Gestaltungsansatz erleichtert die Umsetzung und reduziert unnötigen Mehraufwand.

- *Relevante Anforderungen frühzeitig priorisieren:* Viele anfänglich definierte Vorgaben erwiesen sich als überflüssig oder nicht *umsetzungsrelevant*. Eine gezielte Auswahl essenzieller rechtlicher Aspekte verbessert die Effizienz der Implementierung.
- *Datenschutzrechtliche Verantwortlichkeiten klären:* Unklarheiten über die Rolle des Systemanbieters führten zu *übermäßig* detaillierten Analysen. Eine frühzeitige Festlegung der Verantwortlichkeit optimiert den Entwicklungsprozess.

Die ökonomischen Erkenntnisse zeigen, dass ein „One-size-fits-all"-Ansatz bei der Gestaltung von Datenschutzinitiativen weder aus Nutzersicht noch aus wirtschaftlicher Perspektive optimal ist. Stattdessen sollten Unternehmen:

- *Differenzierte Datenschutzoptionen anbieten*, die verschiedenen Nutzersegmenten gerecht werden, von den *Fundamentalists* bis hin zu den *Unconcerned*.
- *Transparenz als Wettbewerbsvorteil* nutzen, indem sie verständliche und leicht zugängliche Informationen über Datennutzungspraktiken bereitstellen.

- *Anonymisierungstechnologien* einsetzen, um sowohl Wertschöpfungspotenziale zu realisieren als auch Nutzervertrauen zu stärken.
- *Rabattstrukturen und monetäre Anreize strategisch* einsetzen, um die Bereitschaft zur Datenfreigabe zu erhöhen, dabei jedoch die unterschiedlichen Präferenzen der Nutzersegmente berücksichtigen.
- *Intervenierbarkeit und Kontrolle* als *wesentliche* Faktoren für die Nutzerzufriedenheit und -bindung erkennen und entsprechende Funktionen implementieren.

Die wirtschaftlichen Implikationen der Untersuchung verdeutlichen, dass datenschutzfreundliche Geschäftsmodelle nicht zwangsläufig im Widerspruch zu ökonomischen Interessen stehen, sondern bei intelligenter Gestaltung sogar zu einem Wettbewerbsvorteil werden können[1]. Durch das Verständnis der unterschiedlichen Nutzerpräferenzen und die entsprechende Anpassung von Geschäftsmodellen können Plattformunternehmen sowohl regulatorische Anforderungen erfüllen als auch wirtschaftliche Ziele erreichen.

6. Limitationen und zukünftige Arbeit

Die im PERISCOPE-Projekt gewonnenen Erkenntnisse liefern interdisziplinäre Impulse für die Gestaltung datenschutzfreundlicher Technologien und zeigen, wie Transparenz und Intervenierbarkeit effektiv umgesetzt werden können. Gleichzeitig eröffnen sie neue Fragestellungen, die in zukünftiger Forschung weiter vertieft werden sollten, um die Anwendbarkeit und den langfristigen Nutzen dieser Prinzipien weiter zu optimieren.

Ein zentraler Aspekt zukünftiger Untersuchungen ist die langfristige Wirkung von Datenschutzmaßnahmen. Während die Studie die unmittelbare Wahrnehmung und Nutzung der Datenschutzinitiative analysiert, bleibt offen, wie sich diese Maßnahmen über einen längeren Zeitraum auf das Verhalten und das Vertrauen der Nutzer auswirken. Eine Langzeitbetrachtung könnte aufzeigen, inwiefern wiederholte Nutzungserfahrungen die Akzeptanz stärken und ob es effektive Mechanismen gibt, um eine nachhaltige Einbindung der Nutzer zu fördern.

Darüber hinaus bietet die Skalierbarkeit der Erkenntnisse ein wichtiges Forschungsfeld. Die im Projekt getesteten Maßnahmen wurden in einem definierten Anwendungskontext evaluiert. Zukünftige Arbeiten sollten untersuchen, wie sich die entwickelten Lösungen auf groß angelegte Plattformen mit heterogenen Nutzergruppen übertragen lassen. Besonders

relevant ist hierbei die Frage, wie sich Nutzer mit unterschiedlichem Vorwissen und verschiedenen Datenschutzpräferenzen in größeren Systemen orientieren und inwiefern sich die identifizierten UX-Prinzipien unter Bedingungen hoher Nutzerzahlen bewähren.

7. Fazit: Wege zu einem effektiveren und nutzerfreundlicheren Datenschutz

Dieser Beitrag liefert eine interdisziplinäre Perspektive auf die Gestaltung und Wirksamkeit von Datenschutzinitiativen und verknüpft Erkenntnisse aus den Bereichen User Experience, Recht und Ökonomie. Im Rahmen des PERISCOPE-Projekts wurden zentrale Herausforderungen und Potenziale datenschutzfreundlicher Technologien analysiert, wobei die Perspektiven verschiedener Stakeholdergruppen der Plattformökonomie berücksichtigt wurden. Durch die Kombination qualitativer und quantitativer Methoden konnten gezielte Implikationen für die Entwicklung effektiver Datenschutzmaßnahmen abgeleitet werden.

Drei empirische Studien – Usability-Tests, Tiefeninterviews und eine Online-Umfrage – ermöglichten eine umfassende Analyse der Nutzererfahrungen mit der Datenschutzlösung des Projekts. Während die Usability-Tests spezifische Nutzungshürden offenlegten, gaben die Tiefeninterviews detaillierte Einblicke in die Herausforderungen und Erwartungen der Plattformbetreiber. Die Online-Umfrage ergänzte diese Erkenntnisse um quantitative Daten zur Wahrnehmung und Akzeptanz von Datenschutzmaßnahmen unter realen Nutzern.

Die Untersuchungsergebnisse zeigen, dass Datenschutzinitiativen nicht nur regulatorische Anforderungen erfüllen, sondern konsequent an den Bedürfnissen der Nutzer ausgerichtet sein müssen. Unmittelbares Feedback, eine klare Informationsstruktur, visuelle Unterstützung und interaktive Elemente spielen eine entscheidende Rolle für die Akzeptanz und Nutzung von Datenschutztechnologien. Gleichzeitig wurde deutlich, dass eine frühzeitige und präzise rechtliche Einordnung notwendig ist, um ineffiziente Anpassungen im Entwicklungsprozess zu vermeiden. Darüber hinaus verdeutlichen die ökonomischen Erkenntnisse, dass datenschutzfreundliche Gestaltung nicht im Widerspruch zu wirtschaftlichen Interessen steht, sondern bei intelligenter Integration sogar zu einem Wettbewerbsvorteil werden kann.

Die gewonnenen Erkenntnisse tragen dazu bei, die Gestaltung von Datenschutzinitiativen zielgerichteter und nutzerfreundlicher zu machen. Die

interdisziplinäre Herangehensweise dieses Projekts zeigt, dass Datenschutz mehr ist als eine regulatorische Notwendigkeit – er kann als integraler Bestandteil digitaler Dienste gestaltet werden, um sowohl User Experience als auch wirtschaftliche Aspekte zu fördern.

Literatur

Astfalk, Stefanie; Schunck, Christian H. (2023): Balancing Privacy and Value Creation in the Platform Economy: The Role of Transparency and Intervenability. In: Roßnagel, H.; Schunck, C. H.; Günther, J. (Hrsg.): Open Identity Summit 2023. Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn: 2023, S. 135.

Baum, Lorenz; Hanneke, Björn und Hinz, Oliver (2024): A Recommender System for Privacy Friendly Platform Business Models. In: Proceedings der International Conference on Information Systems (ICIS) 2024. Bangkok, Thailand. Best Design Science Paper Nominee. Online verfügbar unter: https://aisel.aisnet.org/icis2024/security/security/3/.

Bundesministerium für Forschung, Technologie und Raumfahrt (o. D.): Periscope. Online verfügbar unter: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/periscope (besucht am 23.05.2025).

Hanneke, Björn; Baum, Lorenz und Hinz, Oliver (2023): GDPR Privacy Type Clustering: Motivational Factors for Consumer Data Sharing. In: Proceedings der European Conference on Information Systems (ECIS) 2023. Kristiansand, Norway. Online verfügbar unter: https://aisel.aisnet.org/ecis2023_rp/409/.

Hanneke, Björn; Baum, Lorenz; Schlereth, Christian und Hinz, Oliver (2023): Consumer Preferences for Privacy Management Systems. In: Proceedings der International Conference on Information Systems (ICIS) 2023. Hyderabad, India. Online verfügbar unter: https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/12/.

Kergroach, Sylvain (2021): SMEs Going Digital: Policy Challenges and Recommendations. In: OECD Going Digital Toolkit Notes, Nr. 15. Paris: OECD Publishing.

Mayring, Philipp (2021): Qualitative Content Analysis: A Step-by-Step Guide. London: Sage.

Nouwens, Maarten; Liccardi, Ilaria; Veale, Michael; Karger, David und Kagal, Lalana (2020): „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. New York: ACM, S. 1–13.

Periscope Project (2025): Periscope Ergebnisse. Online verfügbar unter: https://websites.fraunhofer.de/periscope-projekt/?page_id=490 (besucht am 23.05.2025).

Pfeiffer, Lars (2024): Datenzugang in der Plattformökonomie: Regulierungsinstrumente in P2B-VO, DMA und DSA. In: Buchheim, Bernd; Kraetzig, Lars; Mendelsohn, David; Steinrötter, Matthias (Hrsg.): Plattformen. Grundlagen und Neuordnung des Rechts digitaler Plattformen. Baden-Baden: Nomos, S. 53–76.

Pfeiffer, Lars (2024): Big-Tech-Data: Zugangsnotwendigkeit und Zugangsausgestaltung nach dem Digital Markets Act. In: Augsberg, Arndt; Düwell, Thomas; Müller, Christian (Hrsg.): Datenzugangsregeln. Zwischen Freigabe und Kontrolle. Frankfurt a. M.: Campus Verlag, S. 101–136. Online verfügbar unter: https://www.campus.de/e-books/wissenschaft/philosophie/datenzugangsregeln-18409.html

Pfeiffer, Lars; Astfalk, Stefanie; Baum, Lorenz; Hanneke, Björn; Schunck, Christian; Winterstetter, Matthias (2023): Anforderungen an die automatisierte Protokollierung von Datenverarbeitungstätigkeiten in einem Transaktionsjournal: Eine Multi-Stakeholder-Perspektive auf Motivation und Umsetzung. In: Friedewald, Frauke; Roßnagel, Rainer; Neuburger, Marion; Bieker, Anika; Hornung, Thilo (Hrsg.): Daten-Fairness in einer globalisierten Welt. Baden-Baden: Nomos, S. 117–144.

Privacy Recommender (2023): Privacy Recommender. Online verfügbar unter: https://privacy.wiim-research.de (besucht am 23.05.2025).

Schmitt, Hartmut; Schunck, Christian H.; Lo Iacono, Luigi (2024): Datenökonomie in digitalen Ökosystemen – Neue Herausforderungen für den Datenschutz. In: Datenschutz und Datensicherheit – DuD, 48 Online verfügbar unter: https://www.springerprofessional.de/datenschutz-und-datensicherheit-dud-2-2024/26674164.

Shah, Akshat; Banakar, Varad; Shastri, Sambit; Wasserman, Mark und Chidambaram, Vijay (2019): „Analyzing the impact of GDPR on storage systems". In: Proceedings des 11th USENIX Workshop on Hot Topics in Storage and File Systems (HotStorage 19). Berkeley: USENIX Association.

Tesfay, Weldegebriel B.; Hofmann, Philipp; Nakamura, Takeshi; Kiyomoto, Shinsaku und Serna, Juan (2018): „PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation". In: Proceedings des vierten ACM International Workshop on Security and Privacy Analytics. New York: ACM, S. 15–21.

Westin, Alan F. (2003): „Social and Political Dimensions of Privacy". Journal of Social Issues, 59(2), S. 431–453.

Privacy by Design: Schutz der Privatheit im Metaverse durch Designpraktiken am Beispiel ausgewählter Gefahren für Datenschutz und Persönlichkeitsrechte

Tom Hubert, Felix Büning, Marwan El-Rifaai, Florian Franke, Michael Kern, Sara Elisa Kettner, Otmar Lell, Markus Meyer, Runjie Xie, Benedikt Morscheuser, Christian Thorun und Andreas Wiebe[*]

Zusammenfassung
Das Metaverse eröffnet neue Möglichkeiten für digitale Interaktionen, birgt jedoch zugleich erhebliche Herausforderungen für den Schutz von personenbezogenen Daten und Persönlichkeitsrechten. Ein zentraler Ansatz zur Bewältigung dieser Herausforderungen ist das Konzept des „Privacy by Design", bei dem Datenschutz- und Persönlichkeitsrechte bereits in der Entwicklung virtueller Umgebungen berücksichtigt werden. Dieser Beitrag untersucht verschiedene Designstrategien, die zur Wahrung der Privatheit im Metaverse beitragen können. Die Untersuchung zeigt, dass wirksame Schutzmaßnahmen vor allem dann erfolgreich sind, wenn sie technisch umsetzbar und für die Nutzer intuitiv verständlich sind. Gleichzeitig bestehen Herausforderungen bei der praktischen Implementierung dieser Maßnahmen, insbesondere im Hinblick auf die Balance zwischen Nutzerfreundlichkeit und Vereinbarkeit mit den rechtlichen Anforderungen, wie insbesondere dem Datenschutzrecht.

1. Einleitung

Das Metaverse (Metaversum) birgt gewaltiges ökonomisches Potenzial und könnte alle Bereiche unseres täglichen Lebens, unserer Kultur und Gesellschaft durchdringen.[1] Bis heute existiert das Metaverse noch nicht, doch es wird als eine nächste Stufe des Internets betrachtet, die es Nutzern ermöglicht, neue soziale und interaktive Erlebnisse zu erfahren, deren Spektrum

* Die Autoren arbeiten gemeinsam im Projekt PRIME – Privatheit im Metaversum, in dem fachübergreifend erforscht wird, wie neue virtuelle Welten mit Persönlichkeitsrechten und Datenschutz in Einklang gebracht werden können. Das Projekt ist Teil der Plattform Privatheit und wird durch das BMBF unter dem Förderkennzeichen 16KIS1894K gefördert. Der Beitrag verwendet zwecks Leserlichkeit das generische Maskulinum, gemeint sind jedoch alle Geschlechter und Identitäten.

1 S. etwa *Gartner*, Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026, 2022.

von einer digitalen Erweiterung unserer Realität bis hin zu vollständig virtuellen Welten reicht.[2]

Mit der zunehmenden Verschmelzung von physischer und digitaler Realität im Metaverse rücken Fragen des Datenschutzes und des Schutzes von Persönlichkeitsrechten in den Mittelpunkt der Forschung. Die Nutzung immersiver Technologien führt zu neuen Bedrohungsszenarien, die die Privatheit der Nutzer gefährden, beispielsweise durch besonders intensive Datenerfassung, Verhaltensanalysen oder manipulative Eingriffe.

Ein zentraler Ansatz zur Sicherung von Persönlichkeitsrechten und Datenschutz im Metaverse liegt im Privacy-by-Design-Ansatz, der die Grundprinzipien des Schutzes von Rechten direkt in die Gestaltung von Plattformen, digitalen Medieninhalten und Technologien integriert. Vor diesem Hintergrund stellt sich die Frage, wie Privacy-by-Design in die Gestaltung des Metaverse und seiner Inhalte einfließen kann, um Risiken wirksam zu minimieren und gleichzeitig eine praktikable Umsetzung dieser Lösungen sicherzustellen. Die bisherige Forschung ist jedoch noch in ihren Anfängen und eine integrierte Betrachtung der juristischen, technischen und gesellschaftlichen Aspekte mit Bezug zu sowohl dem Schutz der Persönlichkeitsrechte als auch dem Schutz personenbezogener Daten findet kaum statt.

Als Forschungsfrage sei daher formuliert: *Wie lassen sich wirksame Privacy-by-Design-Lösungen zum Schutz von Persönlichkeitsrechten und personenbezogener Daten im Metaverse entwickeln sowie implementieren und welche Herausforderungen ergeben sich dabei in Bezug auf die Realisierbarkeit aus Nutzerperspektive?*

2. Das Metaverse – Immersive Realitäten

Der Begriff Metaverse, geprägt durch Neal Stephensons Roman *Snow Crash*[3], setzt sich aus „Μετά" (griechisch für „darüber hinaus") und „-verse" (Kurzform von „Universe", bedeutet „Gesamtheit von etwas") zusammen. Das Konzept ist vielschichtig und offen für Interpretationen.[4] Es umfasst ein breites Spektrum an Ansätzen, angefangen bei der digitalen Erweiterung der physischen Realität (d.h. Augmented Reality - AR) über vollständig virtuelle Welten (d.h. Virtual Reality - VR) bis hin zu virtuellen

2 *Accenture*, Meet Me in the Metaverse, 2022, S. 24.
3 *Stephenson*, Snow Crash, 1992.
4 *Dolata/Schwabe*, What is the Metaverse and who seeks to define it?, Journal of Information Technology 2023, 239.

Umgebungen, die wiederum durch reale Elemente ergänzt werden (z.B. augmentierte Virtualität - AV).

Experten betrachten das Metaverse als die nächste Entwicklungsstufe des Internets, die aus vernetzten persistenten 3D-Welten besteht, in denen Nutzer als Avatare auftreten und mit anderen Nutzern, virtuellen Objekten und KI-Agenten interagieren.[5] Ein zentrales Konzept des Metaverse ist die Interoperabilität, durch welche Nutzer nahtlos zwischen verschiedenen Welten wandeln können, während Identität und (virtueller) Besitz erhalten bleiben.[6] Ein weiterer wesentlicher Aspekt ist die Möglichkeit für Nutzer, nicht nur passiv zu konsumieren, sondern die virtuelle Welt aktiv mitzugestalten. Dabei können sie sich am Metaverse-Ökosystem beteiligen und zur Schaffung ökonomischer und sozialer Werte beitragen.[7]

Zentral für das Metaverse ist das Erleben von Präsenz, das subjektive Gefühl, tatsächlich in der virtuellen Welt anwesend zu sein.[8] Dieses Empfinden wird durch die wahrgenommene Immersion verstärkt, die durch einen kontinuierlichen Strom sensorischer Reize moderner Metaverse-Technologien, wie realistischer Grafik und räumlichem Sound, gezielt gefördert wird. Während das klassische Internet primär visuelle und auditive Sinneseindrücke anspricht, verfolgt das Metaverse die Vision, ein breiteres Spektrum an Sinneswahrnehmungen einzubeziehen. Einige dieser Reize sind derzeit noch nicht breit kommerziell verfügbar (z.B. Geruch oder Geschmack), andere hingegen, wie der Tastsinn durch haptische Technologien, der Gleichgewichtssinn durch simulierte Bewegungen oder die Propriozeption über präzises Körper-Tracking, werden bereits erfolgreich integriert. Dadurch entsteht eine Illusion realistischer Wahrnehmung, die die Grenzen zwischen Realität und Virtualität zunehmend auflöst.[9]

Ein vollständig durchgängiges Metaverse im idealen Sinne existiert heute noch nicht. Dennoch finden sich viele Grundideen des Metaverse bereits in bestehenden Technologien, etwa in Open-World-MMORPGs wie Second Life oder World of Warcraft, in sozialen Medien oder in cyberphysischen

5 *Davis u.a.*, Avatars, People, and Virtual Worlds, Journal of the Association for Information Systems 2009, 90.

6 *Dionisio u.a.*, 3D Virtual worlds and the metaverse, ACM Computing Surveys 2013, 34.

7 *Papagiannidis u.a.*, Making real money in virtual worlds, Technological Forecasting & Social Change 2008, 610.

8 *Witmer/Singer*, Measuring presence in virtual environments: A presence questionnaire, Presence: Teleoperators and Virtual Environments 1998, 225.

9 *Dincelli/Yayla*, Immersive virtual reality in the age of the Metaverse, The Journal of Strategic Information Systems 2022, 101717.

Systemen. Außerdem bieten viele Spieleentwickler bereits erste Proto-Metaverse-Plattformen an, die zahlreiche Merkmale des Metaverse gut abbilden, darunter Roblox, Fortnite und Minecraft.[10] Auch die Krypto- und NFT-Community hat ähnliche Ansätze geschaffen, wie beispielsweise Decentraland und The Sandbox.[11]

Das Metaverse könnte vielfältige Chancen für Unternehmen und die Gesellschaft bieten, wie zum Beispiel in den Bereichen Remote Work, Gesundheit und Bildung.[12] Gleichzeitig birgt es jedoch auch Schattenseiten, die das volle Potenzial des Metaverse hemmen können.[13] Diese Herausforderungen sind bereits auf den ersten Proto-Metaverse-Plattformen erkennbar und müssen frühzeitig angegangen werden, um die Grundlage für ein zukünftiges rechtskonformes Metaverse zu schaffen.

3. Risiken des Metaverse für die Privatheit

Unter den zahlreichen Herausforderungen des Metaverse ragt der Schutz der Privatsphäre als besonders problematisch hervor.[14] Privatheit ist ein multidimensionales Konzept, welches das Recht und die Fähigkeit umfasst, die eigene Person sowie persönliche Informationen, Gedanken und Handlungen vor dem Eingriff Dritter zu schützen.[15] Eine Verletzung der Privatheit greift sowohl die Persönlichkeitsrechte als auch die Datenschutzrechte der Nutzer an und kann zu erheblichen Beeinträchtigungen der individuellen Freiheit und Sicherheit führen.

---

10 *Schöbel/Leimeister*, Metaverse platform ecosystems, Electronic Markets 2023, 33 (12).

11 *Dolata/Schwabe*, What is the Metaverse and who seeks to define it? Mapping the site of social construction, Journal of Information Technology 2023, 38 (3).

12 *Marabelli/Newell*, Responsibly strategizing with the metaverse: Business implications and DEI opportunities and challenges, The Journal of Strategic Information Systems 2023, 101774.

13 *Dwivedi u.a.,* Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy, International Journal of Information Management 2022, 102542; *Dwivedi u.a.,* Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse, Information Systems Frontiers 2023, 2071.

14 *Xie/Kirchner-Krath/Morschheuser*, Towards an Ethical Metaverse: A Systematic Literature Review on Privacy Challenges, Proceedings of the 32nd European Conference on Information Systems (ECIS) 2024,6.

15 *Zhang u.a.*, Peer Privacy Concerns: Conceptualization and Measurement, MIS Quarterly 2022, 46 (1).

3.1 Gefahren für Persönlichkeitsrechte

Ein zentraler Aspekt privatheitsbezogener Herausforderungen ist der Schutz von Persönlichkeitsrechten, die Selbstbestimmung und individuelle Freiheit gewährleisten sollen. Aus der Perspektive des deutschen Rechts treten im Kontext des Metaverse besondere Gefährdungen für den Persönlichkeitsschutz auf. Diese werden insbesondere durch virtuelle zwischenmenschliche Interaktionen und der Präsenz automatisierter Software-Agenten bedingt.

3.1.1 Virtuelle Belästigung

Trotz der vergleichsweise noch geringen Zahl an Nutzern in virtuellen Welten, gibt es bereits vermehrt Berichte von Menschen, die mit ihren Avataren Opfer von virtuellen Belästigungen geworden sind.[16] Der Begriff der Belästigung kann weit gefasst werden und umfasst hier jedenfalls jedes bewusste, unerwünschte virtuelle Verhalten, wie beispielsweise Berührungen, Ansprechen oder das Herbeiführen von Begegnungen im Metaverse. Solche Belästigungen erhalten durch die avatarbasierte Kommunikation eine neue Qualität, da sie nicht mehr „nur" text- oder sprachbasiert erfolgen, sondern insbesondere auch durch Gestik, Mimik und Körpersprache der jeweiligen Avatare vermittelt werden können.

Erste Untersuchungen deuten darauf hin, dass Belästigungen im Metaverse deutlich belastender wahrgenommen werden können als vergleichbare Ereignisse auf „herkömmlichen" zweidimensionalen Plattformen.[17] Dies liegt in der Immersion des virtuellen Raums begründet: Die durch die VR-Technologie vermittelte realistische Wahrnehmung der virtuellen Umgebung sowie die dadurch bedingte „Verkörperung" der eigenen Person im Avatar führen dazu, dass die individuellen Grenzen des körperlichen Nähebewusstseins (Proxemik) in das Metaverse übertragen werden.[18] Unerwünschte Annäherungen fremder Avatare können daher als Verletzung der

16 *Benrimoh u.a.*, The Best Predictor of the Future, JMIR Mental Health 2022, 1 (4).
17 *Franks*, The Desert of the Unreal, UC Davis Law Review 2017, 499.
18 *Mello u.a.,* The influence of body expression, group affiliation and threat proximity on interactions in virtual reality, Current Research in Behavioral Sciences 2022, 100075.

individuellen Persönlichkeitssphäre wahrgenommen werden.[19] Gleichzeitig führt die realistische Wahrnehmung des Erlebten zu realen körperlichen Auswirkungen: Während Betroffene kurzfristig unter sog. Freeze-Zuständen leiden können, können mittel- und langfristig sogar psychosomatische Beschwerden wie etwa Angstzustände drohen.[20]

3.1.2 Social Bots

Social Bots sind (teil-)automatisierte Software-Agenten bzw. Computerprogramme, die unter Vortäuschung einer menschlichen Identität am öffentlichen Diskurs im Internet teilnehmen.[21] Im Metaverse können Social Bots insbesondere in Gestalt von Avataren auftreten. Es kommt für die Vortäuschung einer menschlichen Identität nicht darauf an, welche Erscheinungsform der Social Bot – also beispielsweise ob fotorealistisch oder nicht – hat. Entscheidend ist, ob die gewählte Erscheinungsform in der jeweiligen Umgebung eines Metaverse mit menschengesteuerten Avataren assoziiert wird. Als solche sind sie in der Lage, im virtuellen Raum menschenähnlich von „Angesicht zu Angesicht" mit anderen Nutzern zu interagieren.[22] Dies führt dazu, dass eine Unterscheidung zwischen softwaregesteuerten und menschengesteuerten Avataren oftmals gar nicht oder nur mit Mühe möglich ist.[23]

Dieses Täuschungspotential kann aufgrund der breiten Nutzungsmöglichkeiten des Metaverse eingesetzt werden, um umfassend auf Meinungen sowie Entscheidungsmuster menschlicher Nutzer einzuwirken. Social Bots könnten im Metaversum beispielsweise genutzt werden, um im Rahmen personalisierter Interaktionen gezielt Werbung zu verbreiten oder interessierte Nutzer vom Kauf bestimmter Produkte zu überzeugen.[24] Ebenso könnten Social Bots zur Durchführung großer Desinformationskampagnen

19 *Freeman u.a.*, Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality, Proceedings of the ACM on Human-Computer Interaction 2022, 1 (11).

20 *Wiederhold*, Sexual Harassment in the Metaverse, Cyberpsychology, Behavior, and Social Networking 2022, 479.

21 *Kern*, Die Verwendung von Social Bots, KIR 2024, 94 (94); Dürr, Social Bots, S. 7 ff.

22 *Kern*, Die Verwendung von Social Bots, KIR 2024, 94 (94).

23 *Falchuk u.a.*, The Social Metaverse, IEEE Technology and Society Magazine 2018, 52 (54).

24 *Falchuk/Loeb/Neff*, The Social Metaverse: Battle for Privacy, IEEE Technology and Society Magazine 2018 37(2), 52 (53 ff.).

sowie für politische Propaganda missbraucht werden.[25] Schließlich besteht die Gefahr, dass das Verhalten bestimmter Nutzer mittels Social Bots überwacht wird oder durch gezielte, automatisierte Ansprache unbemerkt persönliche Daten gesammelt werden.[26] Im Metaverse können Social Bots selbst auf zusätzlichen Verhaltensebenen menschliches Verhalten vortäuschen, aber auch auf zusätzliche Verhaltensdaten von Nutzern, beispielsweise die Mimik oder Gestik, zugreifen. Dadurch vergrößert sich das Gefahrenpotenzial.

3.2 Gefahren für den Datenschutz

Ein weiteres Feld privatheitsbezogener Probleme im Metaverse betrifft die Datenschutzherausforderungen. Diese ergeben sich vor allem aus der DSGVO, welche die meisten Regelungen zum Schutz natürlicher Personen vor der Verarbeitung ihrer personenbezogenen Daten enthält. Zentrale Herausforderungen im Metaverse stellen dabei die intensivere Datenerhebung sowie die unzureichenden Datenschutzerklärungen und -einwilligungen dar.

3.2.1 Intensität und Umfang der Datenerfassung

Ohne die Verarbeitung von personenbezogenen Daten sind moderne Internetanwendungen, wie z.B. Social Media, gar nicht denkbar.[27] Metaverse-Systeme könnten jedoch wesentlich intensiver Informationen sammeln als herkömmliche Systeme. *Happa et al.* äußern Bedenken darüber, dass sämtliche Sensordaten von Geräten potenzielle Quellen für bisher unbekannte multidimensionale Datenschutzrisiken darstellen könnten, die schwerwiegender sind als die aus früheren Technologien bekannten.[28]

---

25 *Dwivedi et al.*, Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse, Information Systems Frontiers 2023, 25, 2071 (2083).

26 *Falchuk/Loeb/Neff*, The Social Metaverse: Battle for Privacy, IEEE Technology and Society Magazine 2018, 37(2), 52 (53 ff.).

27 So auch *Kroschwald*, Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften, ZfDR 2023, 1 (4).

28 *Happa u.a.*, Privacy-certification standards for extended-reality devices and services, IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops, Lisbon 2021, 397 (397).

Ein wesentlicher Unterschied zwischen dem Metaverse und dem herkömmlichen Internet besteht dabei in der Echtzeitverfolgung von physiologischen Daten und von Bewegungsdaten.[29] Über Technologien wie z.B. VR-Brillen, Controller, spezielle Anzüge oder Schuhe, welche zur Interaktion zwischen Nutzern und dem Metaverse genutzt werden, können Gesichtsausdrücke, Gangart sowie Augen-, Kopf- und Handbewegungen verfolgt werden. Solche Headsets und andere Geräte könnten vielfältige biometrische Daten sammeln, einschließlich Stimmprofile, Gesichtsgeometrie, Iris- und Netzhautscans, Handabdrücke, Fingerabdrücke sowie Gehirn- und Herzsignale. Neurophysiologische Daten, wie Gehirnwellenmuster und neuronale Aktivitäten, können ebenfalls erfasst werden, entweder durch Sensoren oder Gehirn-Computer-Schnittstellen.

Die im Metaverse genutzten Avatare können zudem das Aussehen der realen Nutzer widerspiegeln.[30] Dies kann Aufschluss geben über ihre ethnische Herkunft und ihr Geschlecht.[31] Die Bewegungen und Gesichtsausdrücke der Nutzer können in den Avataren wiedergegeben werden, um ein realistischeres Erlebnis zu bieten.[32] Verhalten und Vorlieben können durch Interaktionen mit virtuellen Objekten und anderen Avataren[33] sowie durch

29 *Di Pietro/Cresci*, Metaverse: Security and Privacy Issues, IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications, Atlanta 2021, 281 (284); *Marloth u.a.*, Psychiatric Interventions in Virtual Reality, Cambridge Quarterly of Healthcare Ethics 2020, 574 (579 f.); *Ruiz Mejia/Rawat*, Recent Advances in a Medical Domain Metaverse, International Conference on Ubiquitous and Future Networks, Barcelona 2022, 357 (358).

30 *Awadallah u.a.*, Identity Threats in the Metaverse and Future Research Opportunities, International Conference on Business Analytics for Technology and Security, Dubai 2023, 1 (3); *Venugopal u.a.*, The realm of metaverse, Computer Animation and Virtual Worlds 2023, 1 (8).

31 *Maloney u.a.*, Anonymity vs. Familiarity, ACM Symposium on Virtual Reality Software and Technology 2020, 1 (7); *Vladimirov u.a.*, Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse, International Scientific Conference on Information, Communication and Energy Systems and Technologies, Ohrid 2022, 1 (1 f.); *Wang u.a.*, Shared realities, ACM on Human-Computer Interaction 2021, 1 (4).

32 *Awadallah u.a.*, Identity Threats in the Metaverse and Future Research Opportunities, International Conference on Business Analytics for Technology and Security, Dubai 2023, 1 (2); *Smith u.a.*, The World as an Interface, Hawaii International Conference on System Sciences 2023, 6045 (6048 f.).

33 *Fernandez/Hui*, Life, the Metaverse and Everything, IEEE International Conference on Distributed Computing Systems Workshops, Bologna 2022, 272 (273).

Eye-Tracking und physische Bewegungen[34] offengelegt werden. Emotionen können durch Kameras, drucksensitive Brillen für Gesichtsmuskulaturbewegungen,[35] Spracherkennung[36] oder aus anderen Daten wie Augen- und Körperbewegungen oder Herzfrequenz[37] abgeleitet werden.

Schließlich sehen *Falchuk et al.* noch das Risiko, dass Avatare auf der Metaverse-Plattform keine Möglichkeit haben, sich selbst vor der Datenerfassung zu verbergen.[38] Nutzer könnten sich daher unbeabsichtigt einer im Hintergrund stattfindenden Datenüberwachung aussetzen.[39]

Hinzu kommen Kontextdaten. Die Metaverse-Plattformen können mithilfe von Datenanalysesoftware die Aktivitäten der Avatare überwachen und analysieren, um Einblicke in die Nutzung der Dienste durch die Nutzer zu ermöglichen.[40] So ließen sich virtuelle Laufwege, Besuche virtueller Orte, Reaktionen der Nutzer auf Produkte oder Ereignisse und weitere Daten sammeln.

3.2.2 Immersive Datenschutzerklärungen und Einwilligungen

In aktuellen Metaverse-ähnlichen Systemen werden Nutzer selten umfassend über die Datenerhebung und -verarbeitung aufgeklärt.[41] Datenschutz-

34 *Dwivedi u.a.*, Exploring the Darkverse, Information Systems Frontiers 2023, 2071 (2075); *Smith u.a.*, The World as an Interface, Hawaii International Conference on System Sciences 2023, 6045 (6049); *Tricomi u.a.*, You Can't Hide Behind Your Headset, IEEE Access 2022, 9859 (9864).

35 *McStay*, The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons, Philosophy and Technology 2023, 1 (6).

36 *Smith u.a.*, The World as an Interface, Hawaii International Conference on System Sciences 2023, 6045 (6051 ff.).

37 *Abraham u.a.*, Implications of XR on Privacy, Security and Behaviour, Nordic Human-Computer Interaction Conference, Aarhus 2022, 1 (9); *Happa u.a.*, Privacy-certification standards for extended-reality devices and services, IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops, Lisbon 2021, 397 (397).

38 *Falchuk u.a.*, The Social Metaverse, IEEE Technology and Society Magazine 2018, 52 (55).

39 *Falchuk u.a.*, The Social Metaverse, IEEE Technology and Society Magazine 2018, 52 (54).

40 *Falchuk u.a.*, The Social Metaverse, IEEE Technology and Society Magazine 2018, 52 (53 f.); *Awadallah u.a.*, Identity Threats in the Metaverse and Future Research Opportunities, International Conference on Business Analytics for Technology and Security, Dubai 2023, 1 (3).

41 *Abraham u.a.*, Implications of XR on Privacy, Security and Behaviour, Nordic Human-Computer Interaction Conference, Aarhus 2022, 1 (5).

richtlinien sind oft unzureichend, besonders hinsichtlich VR-spezifischer Datensammlung,[42] und viele soziale Metaverse-Plattformen informieren Nutzer nicht ausreichend über ihre Datenschutzeinstellungen, was dazu führt, dass Daten möglicherweise unwissentlich (für Dritte) geteilt werden.[43] Die DS-GVO fordert, dass über Datenverarbeitungen transparent und verständlich kommuniziert wird, Art. 13, 14 DS-GVO; dies wird jedoch selten erfüllt.[44] Datenschutzerklärungen sind oft zu lang, unübersichtlich und in schwer verständlicher juristischer Fachsprache verfasst. Zum Beispiel umfasst die Datenschutzerklärung von Roblox[45] 13.607 Wörter, was etwa 26 DIN A4 Seiten entspricht und fast 62 Minuten Lesedauer erfordert. Erschwerend kommt hinzu, dass bereits der Mitteilungsweg der Datenschutzinformationen in Metaverse-Anwendungen unklar ist; denkbar sind z.B. Einblendungen, virtuelle Aushänge oder Verlinkungen auf Webseiten.[46]

Darüber hinaus müssen im Metaverse viele Datenverarbeitungsprozesse auf eine Einwilligung als Rechtsgrundlage gestützt werden (Art. 6 Abs. 1 lit. a, Art. 9 Abs. 2 lit. a DS-GVO), insbesondere wenn es um die Verarbeitung sensibler personenbezogener Daten wie Gesundheitsdaten (z. B. Herzfrequenz) geht. Nach Art. 4 Nr. 11 DS-GVO muss die Einwilligung in informierter Weise, freiwillig und granular bestimmt für alle Zwecke der Verarbeitung erfolgen.[47] Im Kontext herkömmlicher Websites wird dies häufig durch Cookie-Banner umgesetzt, die den Nutzern die Möglichkeit geben, über die Verwendung ihrer Daten zu entscheiden.

Im Metaverse gestaltet sich die Umsetzung dieser Anforderung jedoch ungleich komplexer. Das immersive Erlebnis, welches das zentrale Merkmal dieser virtuellen Welten ist, steht im Spannungsfeld mit den datenschutz-

42 *Adams u.a.*, Ethics Emerging, USENIX Symposium on Usable Privacy and Security 2018, 443 (451).

43 *Kang u.a.*, Security and Privacy Requirements for the Metaverse, IEEE Communications Magazine 2023, 148 (150 ff.); *Maloney u.a.*, Anonymity vs. Familiarity, ACM Symposium on Virtual Reality Software and Technology 2020, 1 (2 ff.).

44 *Kettner u.a.*, Innovatives Datenschutz-Einwilligungsmanagement, 2020, S. 12.

45 *Roblox*, Roblox-Datenschutz- und Cookie-Richtlinie, 2025.

46 Vgl. *Klar u.a.*, Datenschutz im Metaverse, BB 2022, 2691 (2694); *Benedikt*, in: Steege/Chibanguza, Metaverse, 2023, § 11, Rn. 57.

47 Vgl. zur Diskussion um die fragliche Freiwilligkeit bei Einwilligung im Kontext sozialer Netzwerke *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DS-GVO, Rn. 53 ff. m.w.N.

rechtlichen Vorgaben.[48] Auf zentralisierten Plattformen könnte es zwar möglich sein, datenschutzrechtliche Informationen in Textform im Vorfeld des „Eintauchens" bereitzustellen: Nutzer könnten vor dem Zugang zu einer immersiven Umgebung über die wesentlichen Verarbeitungszwecke aufgeklärt und um ihre Zustimmung gebeten werden.

Problematisch wird diese Vorgehensweise jedoch, wenn ein Blick auf die Vision des Metaverse geworfen wird: Durch seine grenzüberschreitende und dynamische Struktur soll es über die rein technischen und rechtlichen Grenzen eines einzelnen Anbieters hinausgehen. Wenn Nutzer in einen neuen Verantwortungsbereich überwechseln – beispielsweise beim Betreten eines virtuellen Raumes, der von einem anderen Anbieter bereitgestellt wird - -müsste erneut eine datenschutzrechtliche Information erfolgen und gegebenenfalls eine neue Einwilligung eingeholt werden.

Diese Anforderung kollidiert mit dem Prinzip einer nahtlosen, immersiven Erfahrung, da Unterbrechungen zur Information oder Einholung von Einwilligungen das Nutzungserlebnis beeinträchtigen könnten. Die Herausforderung besteht daher darin, ein datenschutzkonformes Informations- und Einwilligungsmanagement zu entwickeln, das einerseits den gesetzlichen Anforderungen entspricht und andererseits die immersiven Eigenschaften des Metaverse nicht beeinträchtigt.

4. Lösungsoptionen durch Privacy-by-Design-Praktiken

Um angesichts der genannten Herausforderungen den Schutz der Privatheit zu gewährleisten, ist es entscheidend, den Privacy-by-Design-Ansatz zu verfolgen. Dieser technische und strategische Managementansatz zielt darauf ab, dass der Schutz der Privatheit bereits zu Beginn proaktiv in die Konzeption und Entwicklung des Metaverses integriert werden muss, anstatt ihn erst im Nachhinein zu berücksichtigen.[49] Dadurch können Risiken präventiv und nachhaltig minimiert werden.

Der Europäische Gesetzgeber und andere Gesetzgeber legen großen Wert auf den Privacy-by-Design-Ansatz, um eine ausgewogene Balance

48 Dwivedi *u.a.,* Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse, Information Systems Frontiers 2023, 2071; Europäische Kommission, Datenschutz und Privatsphäre in virtuellen Welten, 2025.

49 *Spiekermann*, The challenges of privacy by design, Communications of the ACM 2012, 38.

zwischen den Privatheitsbedürfnissen der Nutzer und den Datenanforderungen von Unternehmen und der Regulierung zu erreichen.[50] Dennoch bleibt das Konzept oft abstrakt und schwer umzusetzen, da es an konkreten Anforderungen fehlt, insbesondere im Kontext aufkommender Technologien.[51] Daher wird in diesem Beitrag versucht, konkrete Implementierungen für das Metaverse zu erarbeiten, um ein sicheres und datenschutz- wie persönlichkeitsrechtsfreundliches Metaverse zu schaffen.

Die Entwicklung der Designvorschläge wurde mit einer systematischen Analyse der Forschungs-, Praxis- und Rechtsliteratur eingeleitet, ergänzt durch die Auswertung ausgewählter Metaverse-Plattformen sowie semistrukturierter Experteninterviews. Die Zielsetzung bestand zunächst in der Identifizierung der drängendsten Problemfelder des Metaverse. In einem nachfolgenden Schritt wurden die identifizierten Problemfelder und ersten Designvorschläge in einem partizipativen Format mit Experten diskutiert. Im Rahmen dieser Diskussion wurden die Vorschläge hinsichtlich ihrer Effektivität und Umsetzbarkeit priorisiert.

Die folgende Darstellung beschränkt sich auf einen Ausschnitt der Forschung und soll das Vorhaben und die Ergebnisse exemplarisch an ausgewählten Beispielen illustrieren. Ein besonderer Fokus liegt dabei auf dem persönlichkeitsrechtlichen Problemfeld der virtuellen Belästigung und dem datenschutzrechtlichen Problemfeld der Datenschutzerklärungen und Einwilligungen in immersiven virtuellen Welten. Aber auch weitere Designvorschläge sollen beispielhaft erläutert werden, um die Vielfalt der möglichen Ansätze anzudeuten.

4.1 Virtuelle Belästigung (Persönlichkeitsrechte)

Anders als in der realen Welt existieren im Metaverse (noch) keine spezifischen gesetzlichen Rahmenbedingung, die in der Lage wären, Belästigungen und andere „virtuell-physischen" Schädigungen zu verhindern. Bestehende Vorgaben des Strafrechts, des Persönlichkeitsrechts oder des Datenschutzrechts finden zwar grundsätzlich Anwendung, leiden jedoch unter einem generellen Durchsetzungsproblem und sind nicht zugeschnitten auf die besonderen Situationen und Probleme von Metaversen. Gleichzeitig

50 *Spiekermann*, The challenges of privacy by design, Communications of the ACM 2012, 38.

51 *Bu u.a.*, „Privacy by Design" implementation: Information system engineers' perspective, International Journal of Information Management, 102124, 3.

ist jedoch deutlich geworden, dass virtuelle Übergriffe mitunter ebenso einschneidend wahrgenommen werden können, wie vergleichbare Ereignisse in der „echten" Welt. Dies führt dazu, dass Plattformbetreiber mehr denn je in der Verantwortung stehen, virtuelle Belästigungen durch privatheitsfreundliche Designstrategien proaktiv zu verhindern oder jedenfalls zu erschweren. Dabei sollten Plattformdesigns im Vordergrund stehen, die einerseits Anreize für mögliche Belästigungssituationen reduzieren und andererseits Nutzern die jederzeitige Kontrolle über ihre Interaktionen ermöglichen. Daneben können Plattformbetreiber die Verantwortlichen auch sanktionieren. Maßnahmen könnten neben kurzfristigen Nutzungsverboten auch eine Sperrung des Kontos sein. Entsprechende Regelungen könnten Einzug in die Allgemeinen Geschäftsbedingungen der Nutzungsverträge finden.

Zur Prävention virtueller Belästigungen im Metaverse erscheinen insbesondere jene Designvorschläge geeignet, die durch eine privatheitsfreundliche Gestaltung des virtuellen Raums die Auswirkungen derartige Übergriffe so gering wie möglich halten. Eine potenzielle Designpraktik stellt etwa die Einrichtung einer virtuellen Sicherheitszone dar, in welcher Nutzer vor der Annäherung anderer Avatare geschützt sind. Bei dem „Scheinwerfer"-Design wird den angegriffenen Nutzern die Möglichkeit verschafft, besondere Aufmerksamkeit auf den Aggressor zu richten, sodass dieser von seinem Opfer ablässt. Darüber hinaus kann auch das generelle Design eines virtuellen Raums zur Prävention virtueller Belästigungen beitragen.

4.1.1 Helle Beleuchtung und soziale Kulisse durch Bots

Um virtuelle Belästigungen proaktiv vorzubeugen, wurde bei der Gestaltung öffentlicher virtueller Räume gezielt mit sogenannten Nudges gearbeitet, um situative Faktoren zu beeinflussen, die Belästigungen begünstigen können. Ein zentraler Auslöser für antinormatives und deviantes Verhalten ist der Enthemmungseffekt, der unter anderem durch die Unsichtbarkeit und dissoziative Anonymität entsteht.[52]

Dunkle, schwach beleuchtete Bereiche können das Gefühl der Anonymität und Verantwortungslosigkeit verstärken, da sich die Täter weniger sicht-

52 *Hirsch, u.a.,* Drunk, Powerful, and in the Dark: How General Processes of Disinhibition Produce Both Prosocial and Antisocial Behavior, Perspectives on Psychological Science 2011, 415.; *Suler*, The Online Disinhibition Effect, CyberPsychology & Behavior 2004.

bar und dadurch weniger identifizierbar fühlen.[53] Dies kann prosoziales Verhalten hemmen und unethisches Verhalten begünstigen.[54] Zudem zeigen Studien, dass helle Beleuchtung in öffentlichen Bereichen (z.B. Straßen oder Geschäften) Straftaten reduzieren kann.[55] Dieser Effekt könnte gezielt auf die Gestaltung virtueller Umgebungen übertragen werden, da Nutzer dazu neigen, vertraute Muster aus der physischen Welt auch im virtuellen Raum anzuwenden.

Zudem neigen Täter dazu, Opfer eher in isolierten Situationen zu belästigen, wo keine Dritten anwesend sind, die eingreifen könnten.[56] Solche Täter-Opfer-Szenarien können auch im Metaverse auftreten. Daher könnte eine gezielte Integration zusätzlicher, nicht von Nutzern gesteuerter Avatare diesem Risiko entgegenwirken, indem eine öffentlich wirkende Umgebung simuliert wird. Dadurch entsteht für potenzielle Täter der Eindruck, unter Beobachtung zu stehen, was die Hemmschwelle für Belästigungen erhöht und die Einhaltung respektvoller sozialer Normen stärkt.

4.1.2 Safe Zones

Ein weiterer Ansatz zum Schutz der Nutzer besteht im Erhalt ihres persönlichen Raums, da Belästigungen in virtuellen Welten häufig durch das unbefugte Eindringen in die physische Nähe eines Avatars entstehen.[57] Hier könnten sogenannte Safe Zones helfen – Schutzbereiche, die als Radius um den Avatar eines Nutzers eingerichtet werden und bei Betreten durch andere Avatare bestimmte Reaktionen auslösen. Solche Maßnahmen können auf unterschiedliche Weise umgesetzt werden, um unerwünschte Interaktionen zu minimieren und zu verhindern, dass fremde Avatare zu nahe kommen.

53 *Zhong u.a.*, Good Lamps Are the Best Police: Darkness Increases Dishonesy and Self-Interested Behavior, Psychological Science 2010.

54 *Liu u.a.*, Gender moderates the effect of darkness on ethical behaviors: An explanation of disinhibition, Personality and Individual Differences 2018.

55 *Fotios u.a.*, The Effect of Lighting on Crime Counts, Energies 2021, 4099; *Chalfin u.a.*, Reducing Crime Through Environmental Design, Journal of Quantitative Criminology 2022, 127; *Mitre-Becerril u.a.*, Can deterrence persist?, Criminology & Public Policy 2022, 865.

56 *Painter*, The influence of street lightning improvements on crime, fear and pedestrian street use, after dark. Landscape and Urban Planning 1996.

57 *Freeman u.a.*, Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality, Proceedings of the ACM on Human-Computer Interaction 2022.

Präventiv eingesetzt, bildet eine Safe Zone einen unsichtbaren Schutzkreis um den Avatar des Nutzers, sodass andere Avatare den dadurch bestimmten Abstand zum Avatar des Nutzers einhalten müssen, um gesehen und gehört zu werden. Bei Überschreiten dieser Grenze werden sie automatisch unsichtbar und stummgeschaltet. Die Sicherheitszone ist für andere Avatare individuell einstellbar, d.h. Nutzer können bestimmten Avataren (z.B. Freunden) erlauben, den Kreis zu betreten, ohne dass diese ausgeblendet werden.

Reaktiv eingesetzt, kann eine Safe Zone im Falle eines Übergriffs aktiviert werden. Der Schutzkreis dient in dieser Version dazu, den Sicherheitsabstand zu anderen Avataren zu erzwingen. Avatare, die sich innerhalb dieses Schutzkreises aufhalten, werden ebenfalls unsichtbar und unhörbar gemacht. Gleichzeitig wird der Avatar des Nutzers auch für andere Avatare ausgeblendet, sobald sie ihm zu nahe kommen.

In manchen Fällen reicht eine Safe Zone allein nicht aus, da Belästigungen auch aus der Distanz durch zulässige Interaktionsmöglichkeiten erfolgen können. Deshalb ist es sinnvoll, diesen Schutzmechanismus mit weiteren Funktionen, wie z.B. einer Blockfunktion zu kombinieren. Dadurch können Avatare der Täter und ihre Handlungen unabhängig von der Entfernung für betroffene Nutzer unsichtbar und unhörbar gemacht werden. Gleichzeitig werden auch der Avatar und die Aktivitäten des Opfers in der virtuellen Umgebung für die Täter nicht mehr sichtbar oder hörbar.

4.2 Kennzeichnung von Social Bots und Bot-freie Zonen (Persönlichkeitsrechte)

Im Hinblick auf Social Bots kann den Gefahren einer Identitätstäuschung insbesondere mittels einer identifizierenden Kennzeichnung KI-gesteuerter Avatare oder durch vorgelagerte Identitätskontrollen begegnet werden. Die visuelle Kennzeichnung von Bots könnte beispielsweise durch Beschriftungen, Symbole, Umrandungen oder durch die Verwendung bot-spezifischer Avatare umgesetzt werden, um Nutzern die Interaktion mit einer KI offenzulegen. Eine solche visuelle Kennzeichnung ist für „Verwender" von Social Bots auch verpflichtend nach § 18 Abs. 3 Medienstaatsvertrag.[58] Nach der KI-Verordnung gilt eine vergleichbare Kennzeichnungspflicht mittlerweile

58 *Kern*, Die Verwendung von Social Bots, KIR 2024, 94 (95).

auch für Entwickler, Art. 50 KI-Verordnung.[59] Betreiber von Metaversen werden nicht durch § 18 Medienstaatsvertrag oder Art. 50 KI-Verordnung in die Pflicht genommen. Entwickler und auch Verwender von Social Bots sind jedoch oftmals von den technischen Gegebenheiten und Vorgaben von Plattformbetreibern abhängig. Deshalb besteht eine Effektuierungspflicht für Plattformbetreiber nach § 93 Medienstaatsvertrag. Demnach sollen zumutbare Anstrengungen zur Sicherstellung einer Kennzeichnung vorgenommen werden.[60] Vorgelagerte, privatheitsfreundliche Identitätskontrollen könnten mithilfe der flächendeckenden Einführung von 3D-Captchas ermöglicht werden: Avatare, die als Bots verdächtigt werden, müssten demnach kleine Aufgaben in der 3D-Umgebung lösen, um ihre menschliche Identität zu bestätigen.

Um einige der genannten Gefahren zu verhindern, z.B. potenzielle Bot-gestützte Desinformationskampagnen, kann es notwendig sein, über eine reine Kennzeichnungspflicht hinauszugehen. Neben einem kompletten Verbot von Social Bots in Metaversen können bot-freie Zonen als weniger intensive Maßnahme konstituiert werden. Bot-freie Zonen sind Bereiche, in denen die Verwendung von KI-gesteuerten Avataren generell unterbunden wird, sodass Nutzer dort nur auf menschengesteuerte Avatare treffen können.

4.3 Sensorhinweise (Datenschutz)

Zur Reaktion auf die gesteigerte Intensität und den gesteigerten Umfang der Datenerfassung könnten u.a. dauerhafte Sensorhinweise, punktuelle Aktivierungsabfragen sowie eine standardmäßige Zeitbegrenzung der Sensortätigkeiten dienen. Ersteres wäre durch farbliche Hinweise im Sichtfeld des Nutzers umsetzbar, die z.B. auf das Tracking von Pulsmessern oder Eye-Tracking hinweisen. Die punktuelle Aktivierungsabfrage fordert, abhängig von der jeweiligen Anwendungssituation, gezielt die Zustimmung des Nutzers zur Aktivierung bestimmter Sensoren an, und schafft dadurch ein erhöhtes Bewusstsein für die Datenerfassung in sensiblen Situationen. Berechtigungsabfragen haben sich in mobilen Anwendungskontexten bereits als wirksames Mittel erwiesen, um das Risikobewusstsein der Nutzer in Bezug auf ihre Privatheit zu stärken. Kombiniert mit einer regelmäßig

59 *Kern*, Die Verwendung von Social Bots, KIR 2024, 94 (98).
60 *Kern*, Die Verwendung von Social Bots, KIR 2024, 94 (97).

zu erneuernden Freigabe der jeweiligen Datenströme, die den Nutzer daran erinnert, welche Sensoren aktiv sind und erneut um Freigabe der Datenströme bittet, wird die Datensouveränität der Nutzer gestärkt.

4.4 Datenschutzcockpits und Einwilligungsassistenten (Datenschutz)

Um Datenverarbeitungen in immersiven Umgebungen erfolgreich für Nutzer zu kommunizieren (immersive Datenschutzerklärungen), könnten Datenschutzcockpits eingesetzt werden.[61] Die Idee von Datenschutzcockpits wurde bereits im Kontext von Websites angedacht. Diese stellen Informationen zu Datenverarbeitungen sowie Verarbeitungszwecken nutzerfreundlich und in einer Übersicht mit Einstellungsmöglichkeiten dar, was sowohl plattformspezifisch als auch anwendungsspezifisch ausgestaltet sein kann.[62] Eine weitere Lösungsidee könnten unterstützende Gestaltungselemente als Teil der Datenschutzerklärung sein. Dies umfasst Datenschutzicons und Strukturierung durch Abschnittsstrukturen – ggf. auch videogestützt.

Eine immersivere und somit weitergehende Lösung für die datenschutzrechtlichen Herausforderungen im Metaverse könnte ein virtueller Informations- und Einwilligungsassistent („Stefan Schild“[63]) darstellen, der eine dynamische und nutzerfreundliche Verwaltung von datenschutzrechtlichen Informations- und Einwilligungsprozessen ermöglicht. Dieser Assistent sollte sich nahtlos in die immersive Umgebung integrieren und als ständiger Begleiter der Nutzer fungieren, um auf Wunsch relevante Datenschutzinformationen bereitzustellen und Einwilligungen einzuholen, ohne das immersive Erlebnis im Metaverse zu unterbrechen.

Stefan Schild könnte personalisiert und kontextsensitiv agieren. Sobald ein Nutzer in einen neuen Verantwortungsbereich eintritt, z.B. beim Wechsel von einer Plattform zu einer anderen oder beim Besuch eines virtuellen Raums, der von einem Drittanbieter verwaltet wird, würde der Assistent die jeweiligen datenschutzrechtlichen Anforderungen im Hintergrund analysieren. Er würde in Echtzeit eine benutzerfreundliche, kontextabhängige Benachrichtigung ausspielen, welche die wichtigsten Informationen zur

61 *Gerpott*, Datenschutzerklärungen – Materiell fundierte Einwilligungen nach der DS-GVO, MMR 2020, 739 (742).

62 Vgl. *Kettner u.a.*, Wege zur besseren Informiertheit, 2018, S. 71 ff., die das Konzept „Privacy Bots“ nennen. Ebenso *Nüske u.a.*, Privacy Bots, DuD 2019, 28.

63 Bei „Stefan Schild“ handelt es sich um einen willkürlichen Arbeitstitel, der lediglich einen illustrierenden Mehrwert hat.

Datenverarbeitung kurz und prägnant zusammenfasst. Zudem könnte der Assistent die erforderliche Einwilligung einholen.

Anstelle aufdringlicher Pop-ups könnte Stefan Schild in Form eines diskreten, interaktiven Avatars oder einer symbolischen Benutzeroberfläche auftreten, die jederzeit ansprechbar ist. So könnten Nutzer durch einfache Sprachbefehle, Gesten oder Klicks mehr Details zu den Datenschutzinformationen abrufen oder ihre Einwilligung für spezifische Verarbeitungen erteilen oder verweigern. Dadurch könnte Stefan Schild zudem fortlaufend Transparenz gewährleisten, indem er Nutzer aktiv darüber informiert, welche Daten wann und zu welchem Zweck verarbeitet werden. Um das Erlebnis mit Stefan Schild motivierender zu gestalten, könnten Gamifizierungselemente wie Belohnungssysteme, Personalisierung und eine spannende Hintergrundgeschichte integriert werden. Der Assistent könnte wiederum mit anderen Ansätzen kombiniert werden, wie etwa Icons oder Videos.

5. Testung der Designs in Fokusgruppen

Die beschriebenen Designoptionen können nur dann zum Schutz der Privatheit im Metaverse beitragen, wenn sie von den Nutzern des Metaverse als unterstützend und sinnvoll wahrgenommen werden. Die Reaktionen potenzieller Nutzer auf die Designoptionen wurden daher in einem qualitativen und explorativen Format in Fokusgruppen getestet. Durch ein Marktforschungsinstitut wurden insgesamt vier Gruppen zusammengestellt. Davon waren zwei Gruppen mit „metaverse-affinen" Nutzern besetzt, die selbst im Besitz einer VR-Brille waren, die in den zwei anderen Gruppen vertretenen Nutzer besaßen keine VR-Brille. Ansonsten waren alle Gruppen divers zusammengesetzt mit Blick auf Geschlecht, Altersverteilung, Bildungsstand und Wohnort (ländlich/städtisch). Drei Gruppen hatten jeweils sieben Teilnehmer, die Gruppe der metaverse-affinen Nutzer im Bereich der Persönlichkeitsrechte hatte sechs Teilnehmer.

In jeweils zwei Fokusgruppen wurden vertieft die Designoptionen zum Schutz der Persönlichkeitsrechte sowie die Designoptionen aus dem Bereich des Datenschutzes getestet. Dabei wurde zu jedem Teilaspekt des Vorhabens einmal die Perspektive metaverse-affiner Nutzer untersucht und einmal die Perspektive sonstiger Nutzer.

5.1 Quantitative Auswertung der Fokusgruppen

In den Rückmeldungen aus den Fokusgruppen wurden deutliche Unterschiede zwischen der Wahrnehmung der Designs in den Bereichen Persönlichkeitsrechte und Datenschutz erkennbar, wie nachstehend im Einzelnen beschrieben wird. Eine Übersicht zur Wahrnehmung der Designoptionen ist in der Abbildung enthalten. Als quantitative Wertung haben die von den Probanden der Fokusgruppen getroffenen Einschätzungen aufgrund der geringen Anzahl der Teilnehmer nur eine begrenzte Aussagekraft. Sie werden daher im Folgenden vor allem zu dem Zweck genannt, um die nachstehend erläuterten qualitativen Einschätzungen der Probanden zu illustrieren (vgl. Tabelle 1).

5.2 Qualitative Auswertung der Fokusgruppen

Mehr noch als die quantitativen Ergebnisse ist die qualitative Auswertung der Fokusgruppen für die Implementierung eines Privacy-by-Design-Ansatzes im Metaverse relevant. In den Fokusgruppen wurde zunächst jeweils die allgemeine Haltung der Teilnehmer zu Fragen der Privatheit im Metaverse diskutiert, sodann die Wahrnehmung unterschiedlicher Designoptionen zum Schutz der Privatheit. Die qualitative Auswertung der Fokusgruppen wird nachstehend gegliedert nach den Aspekten der Persönlichkeitsrechte und des Datenschutzes wiedergegeben.

5.2.1 Persönlichkeitsrechte

5.2.1.1 Risikowahrnehmung

In allen Fokusgruppen wurden die Risiken des Metaverse im Bereich der Persönlichkeitsrechte als relevant angesehen; für etliche Probanden auch als Grund genannt, das Metaverse selbst nicht nutzen zu wollen (*„wenn ich jetzt da regelmäßig belästigt würde im Metaverse, wieso benutzt man es dann überhaupt noch?“*). Es wurde allgemein als wahrscheinlich angesehen, dass die aus der digitalen Welt bereits bekannten Persönlichkeitsrechtsverletzungen im Metaverse eine neue Intensitätsstufe erreichen würden. Dabei fiel auf, dass die weiblichen Teilnehmer der Fokusgruppen eine deutlich höhere Sensibilität gegenüber den Bedrohungen ihrer Persönlichkeitsrechte zeigten als die männlichen Teilnehmer. Unterschiedlich wurde auch einge-

schätzt, inwieweit die Technik imstande sein wird, die Risiken im Bereich der Persönlichkeitsrechte zu minimieren. Auf Seiten einiger männlicher Probanden war ein ausgeprägter Technikoptimismus festzustellen, während von einigen der weiblichen Probanden eher auf die Zusammenhänge zu generellen Fragen im Verhältnis der Geschlechter verwiesen wurde.

Tabelle 1: Übersicht zur Wahrnehmung der Designoptionen

Design	**Gruppe**	**Positiv**[64]	**Neutral**	**Negativ**
Helle Beleuchtung	Affin	0	3	4
	Nicht-affin	1	1	4
	Gesamt	1	4	8
Safe Zones	Affin	4	3	0
	Nicht-affin	0	6	0
	Gesamt	4	9	0
Botkennzeichnung	Affin	6	1	0
	Nicht-affin	4	2	0
	Gesamt	10	3	0
Bot-freie Zonen	Affin	3	4	0
	Nicht-affin	5	1	0
	Gesamt	8	5	0
Sensorhinweise	Affin	1	5	1
	Nicht-affin	5	1	1
	Gesamt	6	6	2
Zeitliche Begrenzung der Sensortätigkeit	Affin	2	3	2
	Nicht-affin	7	0	0
	Gesamt	9	3	2
Datenschutzcockpit	Affin	0	7	0
	Nicht-affin	5	2	0
	Gesamt	5	9	0
Einwilligungsassistent	Affin	0	7	0
	Nicht-affin	3	1	3
	Gesamt	3	8	3

64 Die Probanden wurden jeweils gefragt: Halten Sie die vorgestellten Designoptionen für wirksam? Die Zahl der Probanden, welche die Designoption für wirksam hielten, wird jeweils mit „Positiv" angegeben, die Zahl der Probanden, welche die Designoption für unwirksam hielten, mit „Negativ", die Zahl der Probanden, welche unentschieden waren, wird mit „Neutral" angegeben.

5.2.1.1 Wahrnehmung der Designoptionen

Entsprechend dieser generellen Haltung wurde die Zielsetzung der Designs zum Schutz der Persönlichkeitsrechte allgemein befürwortet und gutgeheißen. Mit Blick auf ihre Wirksamkeit wurden die verschiedenen Designoptionen jedoch unterschiedlich eingeschätzt; außerdem eröffneten die Rückmeldungen aus den Fokusgruppen wichtige Perspektiven zu unbeabsichtigten Nebenwirkungen und zu alternativen Ausgestaltungsmöglichkeiten.

Das Problem der Social Bots war den Probanden aus sozialen Netzwerken bekannt. Daher war auch die Sorge verbreitet, dass sich dieses im Metaverse noch verstärken könnte. Zudem wurde auch das Risiko des Identitätsdiebstahls diskutiert, etwa dass im Metaverse eine reale Person optisch nachgebaut werden könnte. Die Kennzeichnungspflicht für Bots wurde dementsprechend allgemein für gut befunden. In der Ausgestaltung wurden solche Varianten befürwortet, die Bots intuitiv und deutlich von Menschen unterschieden. Die Umsetzbarkeit der Bot-Kennzeichnung wurde allerdings von einigen angezweifelt, da es den Metaverse-Unternehmen an wirksamen Anreizen fehlen würde, für eine Transparenz der Bots zu sorgen. Viel Zuspruch bekam auch die Idee, bot-freie Zonen einzurichten.

Wenig Unterstützung fand demgegenüber der Vorschlag, Metaverse-Umgebungen generell hell auszuleuchten und dadurch potentielle Übergriffe zu erschweren. Zum einen wurde schon die Wirksamkeit dieser Maßnahme in Zweifel gezogen (*„wenn man sich jetzt unsere echte Welt anschaut, passiert sowas schon im Schwimmbad am helllichten Tag"*). Zum anderen wurde kritisiert, dass schummrige Orte eben auch zum Nutzererlebnis des Metaverse gehören würden und dass die gesuchte Atmosphäre durch die helle Ausleuchtung zerstört würde.

Die Idee einer Safe Zone, die vor Übergriffen schützt, fand allgemein Unterstützung. Hier gab es allerdings zur Ausgestaltung einige beachtenswerte Hinweise: Ein punktuelles Scheinwerferlicht auf eine Gefährdungssituation wurde als unwirksam bezeichnet, da die hierdurch erzeugte Aufmerksamkeit möglicherweise genau das sei, was die übergriffige Person suche. Eine „Bubble", in der eine angegriffene Person für den Angreifer unsichtbar wird, wurde als unfair kritisiert, da sie eher das Opfer als den Gefährder belasten würde; eigentlich sollte der Gefährder ausgeblendet werden. Eine Teilnehmerin schlug vor, dass anstelle der Aktivierung einer Safe Zone im Falle eines Übergriffs von vornherein Mindestabstandszonen programmiert sein sollten, die nur mit expliziter Einwilligung reduziert oder geöffnet werden könnten. Schließlich wurde wiederholt die Idee einer

Moderation des sozialen Geschehens im Metaverse vorgeschlagen, um auch im Vorfeld von technischen Barrieren eine einladende und kommunikationsfördernde Atmosphäre im Metaverse zu schaffen.

5.2.2 Datenschutz

5.2.2.1 Risikowahrnehmung

Im Bereich des Datenschutzes war das Risiko- und Problembewusstsein weniger eindeutig als im Bereich der Persönlichkeitsrechte. Das Thema Datenschutz wurde von einem Probanden als „*sehr aufgebläht*" bezeichnet, und allgemein war eine Resignation gegenüber den datenschutzinvasiven Geschäftsmodellen der heutigen digitalen Welt erkennbar („*die Datensammelei und die Analyse können wir eh nicht komplett abschaffen*").

Interessant waren vor diesem Hintergrund die Einschätzungen der Probanden zu ihrem persönlichen Umgang mit den Datenschutzrisiken im Metaverse. Insbesondere die eher digital- und metaverseaffinen Probanden fanden die invasive Datenerhebung zwar ärgerlich, sahen darin letztlich aber keinen Grund, das Metaverse nicht zu nutzen („*Man hat ja ein Ziel (…) und dann kommen da diese Cookie-Meldungen, und dann klickt man die halt weg, (…) und ich denk mal hier wird es dann genauso sein*"). Es gab aber auch andere Haltungen, die in der Quantität und Granularität der im Metaverse erfassten Daten eine neue Risikoqualität sahen („*Das ist, als wäre ich an einen Lügendetektor angeschlossen*").

Bemerkenswert ist auch, dass es keine Bereitschaft der Probanden gab, das Metaverse über Bezahlmodelle zu nutzen, bei denen keine personenbezogenen Daten ökonomisch verwertet würden. Ein wichtiger Beweggrund hierfür war die Sorge, dass der Datenschutz ansonsten kommerzialisiert würde und es zu einer „*Zwei-Klassen-Gesellschaft*" kommen würde.

Dagegen stieß die Forderung, die kommerzielle Nutzung von personenbezogenen Daten durch eine gesetzliche Regelung generell zu verbieten, auf ganz überwiegende Zustimmung – auch im Bewusstsein dessen, dass in der Folge Metaverse-Umgebungen nur in Bezahlformaten nutzbar wären. Trotz der verbreiteten Resignation gegenüber den allgegenwärtigen Praktiken der Datensammlung war ein hohes Problembewusstsein gegenüber den gesellschaftlichen Folgen der trackingbasierten Geschäftsmodelle feststellbar („*Wie viele süchtige Kinder wollen wir uns denn noch heranzüchten?*"). Die Notwendigkeit einer politischen Lösung wurde gerade angesichts der neuen Gefährdungsqualität im Metaverse betont („*Das ist nochmal so ein*

richtig tiefer Schritt in Richtung gläserner Kunde(…) und deshalb muss man politisch eine Reglung treffen").

5.2.2.2 Wahrnehmung der Designoptionen

Die Rückmeldungen zu den Designvorschlägen im Bereich des Datenschutzes waren unterschiedlich danach, ob die Designs nur zusätzliche Informationen vermittelten oder ob sie die eigentlich gewünschte Nutzung störten. Insbesondere die aktiven Nutzer machten in der Diskussion sehr deutlich, dass Datenschutz die Interaktion und das Erlebnis im Metaverse nicht stören solle.

Vor diesem Hintergrund wurden Sensorhinweise, die deutlich machen, welche Daten auf welchen Wegen gerade erhoben werden, allgemein befürwortet – solange sie nicht mit dem eigentlichen Nutzungserlebnis in Konkurrenz stehen. Allerdings wurde von einigen Nutzern gefordert, dass gleichzeitig mit dem Hinweis auf die Datenerhebung auch der Zweck der Datenverarbeitung deutlich gemacht werden solle.

Auch das Datenschutzcockpit, das Datenverarbeitungen und Datenverarbeitungszwecke transparent macht, stieß auf Zustimmung. In der quantitativen Abfrage wurde auch eine automatische zeitliche Begrenzung der Sensoraktivität eher befürwortet (z.B. das Ausschalten der Kamera nach einer Stunde Nutzung mit der Möglichkeit, die Kamera manuell wieder einzuschalten). Allerdings gibt die geäußerte Abneigung gegen Unterbrechungen Anlass zu Zweifeln, ob ein solches Modell praktisch auf Akzeptanz stoßen würde.

Die immersive Umsetzung von Datenschutzerklärungen und Einwilligungen über den digitalen Assistenten Stefan Schild stieß bei den meisten Probanden auf Widerstand. Viele empfanden den digitalen Assistenten als störend und zeitraubend und zeigten keine Bereitschaft, sich damit auseinanderzusetzen („*Wenn ich muss, würde ich nicht darauf achten oder aufs Klo gehen*"). Datenschutzhinweise sollten nach Meinung der meisten Probanden optional angezeigt werden, sodass man sie bei Interesse nachlesen könne, aber nicht gezwungen sei, sich damit auseinanderzusetzen („*eher ein Datenschutzstand oder eine Säule im Shop, wo ich freiwillig hingehen kann*"). Ohne dass hiernach gefragt wurde, kam von einigen Probanden der Vorschlag, dass die datenschutzrechtliche Einwilligung beim Betreten einer Metaverse-Plattform einmalig vorab geklärt werden sollte und dann während der Nutzung der Plattform keine weiteren Einwilligungen mehr

abgefragt werden sollten (Es sei ein „*Abturner*", wenn man bei jedem Eintritt in einen Shop neu entscheiden müsse – „*gut wäre, wenn es einmalig ist und dann nicht nochmal*", wenn man sich im Anschluss an eine Vorabeinwilligung nur noch mit Datenschutzfragen befassen müsste, wenn man die ursprüngliche Entscheidung revidieren wolle).

6. Braucht das Metaverse Personal Information Management Systems (PIMS)?

Wie sich aus der bisherigen Darstellung abzeichnet, sind nicht alle rechtlichen Probleme allein durch Designs lösbar. Besonders anspruchsvoll gestalten sich Designvorschläge zu datenschutzrechtlichen Informationen und Einwilligungen. Das Phänomen der sinkenden Bereitschaft, sich mit datenschutzrechtlichen Fragestellungen zu beschäftigen, ist auch aus „herkömmlichen" datenschutzrechtlichen Informations- und Einwilligungssituationen bekannt und wird dort treffend als sog. „Abnutzungserscheinungen"[65] bei den Betroffenen beschrieben. Wo zunächst eine grundsätzliche Bereitschaft besteht, sich mit dem Schutz der eigenen personenbezogenen Daten zu beschäftigten, lässt diese nach, sobald der Nutzer zu häufig informiert bzw. nach seiner Einwilligung gefragt wird. Hier bedarf es Lösungen, welche die Interessen der Nutzer berücksichtigen, aber zudem mit dem geltenden Recht vereinbar sind. Wie in den Fokusgruppen angedeutet, könnte eine solche Lösung in zentralisierten, vorweggenommenen Mechanismen liegen, die den Nutzerkomfort erhöhen und das Interesse aufrechterhalten. Ob diese wiederum (in allen Fällen) mit dem Datenschutzrecht vereinbar sind, steht auf einem anderen Blatt.

6.1 Vorteile und Reichweite einer zentralen Datenschutzerklärung und Einwilligung

Eine zentrale Datenschutzerklärung ist ein Dokument oder eine digitale Information, die Nutzern umfassend und transparent erklärt, wie und zu welchen Zwecken ihre personenbezogenen Daten verarbeitet werden. Sie enthält gem. Art. 13, 14 DS-GVO Angaben über die Verantwortlichen der

65 *Spindler/Förster*, Privacy-compliant design of Cookie Banners according to the GDPR, JIPITEC 2023, 2 (31).

Datenverarbeitung, die betroffenen Datenkategorien, die Rechtsgrundlagen der Verarbeitung sowie die Rechte der betroffenen Personen. Im Kontext des Metaverse würde eine zentrale Datenschutzerklärung alle relevanten Datenverarbeitungsprozesse auf einer Plattform oder einem Ökosystem abdecken und idealerweise plattformübergreifend gelten, um eine einheitliche und konsistente Informationsbasis für Nutzer zu schaffen.

Eine zentrale Einwilligung bezeichnet die datenschutzrechtliche Zustimmung einer betroffenen Person zu mehreren, u.U. gleichartigen Datenverarbeitungen, die in einem zusammenhängenden, digitalen oder realen Ökosystem stattfinden. Sie ermöglicht es Nutzern, einmalig ihre Einwilligung zu einer Vielzahl von Verarbeitungszwecken zu erteilen, anstatt wiederholt separate Einwilligungen geben zu müssen.

Eine zentrale und vor allem vor das „Eintauchen" in die Metaverse-Welt vorweggenommene Durchführung des datenschutzrechtlichen Informations- und Einwilligungsprozesses böte den Vorteil, dass Nutzer möglichst einmalig ihre Belange des Datenschutzes regeln können und im weiteren Verlauf des Erlebnisses nicht mehr damit behelligt werden.

Die Reichweite einer zentralen Datenschutzerklärung und Einwilligung stellt im Metaverse-Kontext jedoch eine besondere Herausforderung dar. Aufgrund der dynamischen Natur dieser virtuellen, bestenfalls polypolistischen Welt wird es nicht immer möglich sein, im Vorfeld eine Einwilligung für alle Datenverarbeitungsprozesse einzuholen bzw. im Vorhinein umfassend zu informieren. Insbesondere bei plattformübergreifenden Interaktionen oder beim spontanen Wechsel zwischen unterschiedlichen Verantwortungsbereichen wird die traditionelle Einwilligungspraxis an ihre Grenzen stoßen.

Denn wechselt der Verantwortliche für die konkrete Datenverarbeitung, muss neu informiert und neu eingewilligt werden. Dies gilt spätestens ab dem Punkt, wo die Vision des Metaverse als eine virtuelle Realität, in der Verantwortlichkeitsbereiche verschwimmen, erreicht ist. Wenn stetig und in Echtzeit neue Anbieter von Diensten und Interaktionen auf den Metaverseplattformen auftauchen, kann eine solche Entwicklung unmöglich in einer zentralen Datenschutzerklärung und Einwilligung dargestellt werden.

6.2 Lösung durch Einsatz von Personal Information Management Systems (PIMS)?

Eine mögliche Lösung für die besonderen Anforderungen an zentrale Informations- und Einwilligungsmechanismen im dynamischen Kontext des Metaverse könnte im Einsatz von Personal Information Management Systems (PIMS) liegen.[66] Diese technischen Systeme ermöglichen eine zentralisierte Verwaltung von Einwilligungen durch voreingestellte, automatisierte Entscheidungen basierend auf individuellen Präferenzen der Nutzer.[67] Der Vorteil dieser Systeme liegt auf der Hand: Sie reduzieren die Notwendigkeit ständiger Einwilligungen, minimieren sogenannte „Abnutzungserscheinungen" bei den Nutzern und gewährleisten eine konsistentere Datenschutzkontrolle.[68]

Der wesentliche Vorteil gegenüber einer zentralen Einwilligung durch den Nutzer selbst liegt darin, dass die PIMS nach der entsprechenden Einrichtung durch den Nutzer die Einwilligung für diesen übernehmen. Tritt ein neuer Verarbeitungskontext auf, willigen die PIMS nach den Präferenzen des Nutzers für diesen in die Verarbeitung ein. Der Nutzer selbst wird erst mit dem Verarbeitungskontext konfrontiert, wenn dieser nicht mit seinen Voreinstellungen in Einklang zu bringen ist. Allerdings sind die rechtlichen Fragen rund um die Zulässigkeit und die konkrete Ausgestaltung von PIMS bisher nicht abschließend geklärt.

6.2.1 Zulässigkeit einer Einwilligungsstellvertretung durch PIMS

Ein zentraler rechtlicher Streitpunkt ist die Frage, ob PIMS(-Betreiber) als Einwilligungsstellvertreter agieren dürfen.[69] Wird dies bejaht, könnten Nutzer dem PIMS-Betreiber eine Art „Einwilligungs-Vollmacht" erteilen

66 So a. *Bender-Paukens/Werry*, Datenschutz im Metaverse, ZD 2023, 127 (130).

67 Vgl. *Hunter u.a.*, Informationspflichten und Einwilligung bei der Nutzung von PIMS, ZD 2024, 603 (603); *Botta*, Delegierte Selbstbestimmung?, MMR 2021, 946 (946 f.).

68 Vgl. *Schuchardt*, Die (ferne) Zukunft der Cookie-Einwilligung: PIMS und der Weg zu datenschutzfreundlichen Lösungen, DSB 2025, 103 (103); *Kühling/Sauerborn*, PIMS vs. Einwilligung vs. Browsereinstellungen, ZD 2022, 596 (596): „Cookie-Click-Fatigue".

69 Vgl. zu rechtlichen Herausforderungen *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7 DS-GVO, Rn. 33 ff.; *Jandt*, in: Jandt/Steidle, Datenschutz im Internet, 2025, Kap. IV, Rn. 122 ff.; *Hunter u.a.*, Informationspflichten und Einwilligung bei der Nutzung von PIMS, ZD 2024, 603 (605).

und damit den Prozess der Einwilligung auslagern. Nach Art. 8 Abs. 1 S. 2 DS-GVO können bei Minderjährigen die Sorgeberechtigten an ihrer Stelle die Einwilligung erteilen, was für die grundsätzliche Zulässigkeit einer Einwilligungsvertretung spricht. Die Stellungnahme des Europäischen Datenschutzbeauftragten (EDSB) stützt ebenfalls die Möglichkeit, in bestimmten Fällen Einwilligungen in Stellvertretung rechtlich wirksam abzugeben.[70] Dennoch fehlt bisher eine explizite Regelung in der DS-GVO für den allgemeinen Einsatz von PIMS als Stellvertreter, was eine entsprechende Normierung in künftigen Datenschutzregelungen wünschenswert macht.[71]

6.2.2 PIMS für sachgleiche Datenverarbeitungen

Weniger problematisch ist die Nutzung von PIMS für gleichartige Datenverarbeitungsvorgänge. Für (wohl auch) im Metaverse relevante Trackingverfahren wie z.B. Cookies ist gem. § 3 Abs. 1 der Einwilligungsverwaltungsverordnung (EinwV) die Einführung von PIMS möglich. So könnten etwa Cookies, von deren technischer Relevanz für Metaverseanwendungen bis auf Weiteres auszugehen ist, im Falle des Ablaufes ihrer Gültigkeitsdauer durch die erneute Übermittlung der gültigen Einwilligung „erneuert" werden. Die EinwV setzt § 26 Abs. 1 TDDDG um, wonach Dienste zur Verwaltung von Einwilligungen nach § 25 Abs. 1 TDDDG anerkannt werden können. Die Voraussetzungen an die Einwilligung nach § 25 Abs. 1 TDDDG richten sich weiterhin nach der DS-GVO.[72]

Lediglich die anschließende Verwaltung der Einwilligung kann von einem gem. §§ 8 ff. EinwV anerkannten Dienst übernommen werden, d.h. dass dieser die getroffenen Einstellungen des Endnutzers speichert und dem jeweiligen Digitale-Dienste-Anbieter bei „jeder weiteren Inanspruchnahme des Dienstes" übermittelt (§ 3 Abs. 1 EinwV).[73] Mit anderen Worten nimmt der anerkannte Dienst dem Nutzer „nur" die erneute Übermittlung einer gültigen Einwilligung ab. In Hinblick auf das oben skizzierte Problem

70 *EDSB*, Stellungnahme des EDSB zu Systemen für das Personal Information Management, 2016.

71 S. ausführlicher *Büning/Meyer*, PIMS und das Metaverse: Ein Weg aus dem „Einwilligungs-Banner-Dschungel"? (im Erscheinen).

72 Aufgrund des Umsetzungscharakters des § 25 Abs. 1 TDDDG von Art. 5 Abs. 3 ePrivacy-RL, welcher für die Voraussetzungen auf die DS-RL verweist, die gem. Art. 94 Abs. 2 S. 1 DS-GVO von der DS-GVO abgelöst wurde.

73 Ausführlich *Hunter u.a.*, Informationspflichten und Einwilligung bei der Nutzung von PIMS, ZD 2024, 603 (605); *Jandt*, in: Jandt/Steidle, Datenschutz im Internet, 2025, Kap. IV, Rn. 122 ff.; *Klement*, in: Simitis u.a., Datenschutzrecht, 2025, Art. 7

um die Dynamik in Bezug auf die datenschutzrechtlich Verantwortlichen und die Verarbeitungszwecke schafft die EinwV keinen echten Mehrwert, da die gespeicherte Einwilligung nur dann noch gültig ist, wenn der Verarbeitungsvorgang gänzlich unverändert ist, also sachgleich mit dem erstmaligen ist.

6.2.3 PIMS für bereichsmäßige Einwilligungen (Broad-Consent)

Um den besonders dynamischen Datenverarbeitungskontexten aufgrund wechselnder datenschutzrechtlicher Verantwortlicher zu begegnen, bedarf es eines ebenso dynamischen Einwilligungsmechanismus. PIMS müssen nicht nur eine bereits erteilte Einwilligung des Nutzers in sachgleichen Verarbeitungsprozessen neu übermitteln, sondern auch in neue Verarbeitungskontexten gegenüber neuen Verantwortlichen eine interessengerechte rechtskonforme Einwilligung erteilen können. Nur dann kann es gelingen, den Abnutzungserscheinungen bisheriger Instrumente Abhilfe zu schaffen. Ein rechtlicher Ansatzpunkt könnte dabei eine bereichsbezogene Einwilligung darstellen, angelehnt an den Rechtsgedanken aus ErwG 33 DS-GVO, der den sogenannten Broad-Consent für wissenschaftliche Forschungszwecke erlaubt. Dabei wird eine allgemeine Einwilligung für einen bestimmten Verarbeitungsbereich erteilt, während konkrete Verarbeitungsdetails zum späteren Zeitpunkt durch eine Instanz – in den Fällen der medizinischen Forschung etwas das Krankenhaus, dass die Patientendaten erhoben hat – spezifiziert werden können.

Ob dieser Ansatz schon grundsätzlich auf kommerzielle Datenverarbeitungen übertragbar ist, bleibt ungeklärt.[74] Erschwerend hinzu kommt der Umstand, dass es im originären Sinne des Broad-Consent lediglich um Spezifikationen der Zwecke der Datenverarbeitung geht; der Betroffene willigt bei der Erhebung der Daten informiert in die Nutzung der Daten zu Forschungszwecken ein, die spezifische Forschung wird jedoch später durch den Verarbeiter bestimmt (z.B. Verarbeitung zu Zwecken der Forschung an Krebs oder aber Alzheimer). In Metaversekonstellationen ginge es aber häufig nicht nur um eine Zweckspezifikation durch PIMS, sondern zusätzlich um eine Verantwortlichenauswahl. Selbst wenn unterstellt würde, dass

DS-GVO, Rn. 34; *Klink-Straub/Straub*, Und bist du nicht willig, so brauch' ich … PIMS, ZD-Aktuell 2024, 01820.

74 Allgemein *Specht-Riemenschneider u.a.*, Die Datentreuhand, MMR-Beilage 2021, 25 (41 ff.).

PIMS in kommerziellen Datenverarbeitungen zu Zweckspezifikationen eingesetzt werden dürften, würde dem Ausgangsproblem der besonderen Verantwortlichendynamik im Metaverse damit nur bedingt Abhilfe geschaffen werden können. Resümierend lässt sich mithin statuieren, dass PIMS technisch große Vorteile bringen könnten, wenn sich sowohl die datenschutzrechtliche Information als auch die Einwilligung damit automatisieren bzw. auslagern ließen. Aus rechtlicher Perspektive ist wenigstens eine effiziente Umsetzung dieser Systeme jedoch (noch) unzulässig.[75]

7. Fazit

Privatheitsfreundliches Design kann erheblich zum Schutz von personenbezogenen Daten und Persönlichkeitsrechten beitragen. Das Konzept „Privacy by Design" ermöglicht es, Datenschutz- und Persönlichkeitsrechte von Anfang an in die Gestaltung virtueller Welten zu integrieren. Dies ist besonders im Metaverse relevant, wo durch immersive Technologien neue Bedrohungsszenarien wie virtuelle Belästigung, Social Bots und besonders intensive Datenerhebung entstehen. Designmaßnahmen können helfen, diese Risiken zu minimieren und eine sicherere digitale Umgebung zu schaffen. Besonders geeignete Designstrategien sind solche, die sowohl technisch wirksam als auch für Nutzer intuitiv bedienbar sind. Weniger geeignete Designlösungen sind solche, die entweder ineffektiv sind oder von den Nutzern als störend empfunden werden. Insbesondere im Bereich des Datenschutzes zeigte sich, dass klassische Einwilligungsmechanismen, wie sie etwa in Cookie-Bannern üblich sind, auf alte Probleme wie Abnutzungserscheinungen treffen, auch wenn sie in neuem Gewand, wie einem virtuellen Assistenten mit Chat-Funktion, präsentiert werden. Hinzu kommen weitere, metaversespezifische Probleme. Hier sehen sich designbasierte Lösungen rechtlichen Hürden gegenüber, denen ggf. nur regulatorisch – z.B. durch Rechtsgrundlagen für bestimmte Strategien wie Personal Information Management Systems (PIMS) – abgeholfen werden kann.

75 Ein rechtsdogmatischer Vorschlag bei *Büning/Meyer*, PIMS und das Metaverse: Ein Weg aus dem „Einwilligungs-Banner-Dschungel"? (im Erscheinen).

Literatur

Abraham, Melvin; Saeghe, Pejman; Mcgill, Mark und Khamis, Mohamed (2022): Implications of XR on Privacy, Security and Behaviour: Insights from Experts. *Nordic Human-Computer Interaction Conference*, 30, S. 1-12. https://doi.org/10.1145/3546155.3546691

Accenture (2022): Technology Vision 2022, Meet Me in the Metaverse, The continuum of technology and experience, reshaping business, S. 1-96.

Adams, Devon; Bah, Alseny; Barwulor, Catherine; Musabay, Nureli; Pitkin, Kadeem und Redmiles, Elissa M. (2018): Ethics emerging: the story of privacy and security perceptions in virtual reality. *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*, S. 443-458.

Awadallah, Abeer M.; Damiani, Ernesto; Zemerly, Jamal und Yeun, Chan Yeob (2023): Identity Threats in the Metaverse and Future Research Opportunities. *2023 IEEE International Conference on Business Analytics for Technology and Security (ICBATS)*, S. 1-6. https://doi.org/10.1109/ICBATS57792.2023.10111122

Bender-Paukens, Leonie; Werry, Susanne (2023): Datenschutz im Metaverse. *Zeitschrift für Datenschutz*, S. 127-131.

Benrimoh, David; Chheda, Forum D. und Margolese, Howard C. (2022): The Best Predictor of the Future – the Metaverse, Mental Health, and Lessons Learned From Current Technologies, *JMIR Mental Health*, 9(10), S. 1-9. https://doi.org/10.2196/40410

Botta, Jonas (2021): Delegierte Selbstbestimmung? PIMS als Chance und Risiko für einen effektiven Datenschutz. *Multimedia und Recht*, S. 946-951.

Büning, Felix; Meyer, Markus (2025): PIMS und das Metaverse: Ein Weg aus dem "Einwilligungs-Banner-Dschungel". (im Erscheinen).

Chalfin, Aaron; Hansen, Benjamin; Lerner, Jason und Parker, Lucie (2022): Reducing Crime Through Environmental Design: Evidence from a Randomized Experiment of Street Lighting in New York City. *Journal of Quantitative Criminology*, 38, S. 127-157. https://doi.org/10.1007/s10940-020-09490-6

Davis, Alanah; Murphy, John; Owens, Dawn; Khazanchi, Deepak und Zigurs, Ilze (2009): Avatars, People, and Virtual Worlds: Foundations for Research in Metaverses. *Journal of the Association for Information Systems*, 10(2), S. 91-117. https://doi.org/10.17705/1jais.00183

Dincelli, Ersin und Yayla, Alper (2022): Immersive virtual reality in the age of the Metaverse: A hybrid-narrative review based on the technology affordance perspective. *The Journal of Strategic Information Systems*, 31(2), 101717, S. 1-22. https://doi.org/10.1016/j.jsis.2022.101717

Dionisio, Jahn David N.; Bruns III, William G. und Gilbert, Richard (2013): 3D Virtual worlds and the metaverse: Current status and future possibilities. *ACM Computing Surveys*, 45(3), 34, S. 1-38. https://doi.org/10.1145/2480741.2480751

Di Pietro, Roberto und Cresci, Stefano (2021): Metaverse: Security and Privacy Issues. *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, S. 281-288. https://doi.org/ 10.1109/TPSISA52974.2021.00032

Dolata, Mateusz und Schwabe, Gerhard (2023): What is the Metaverse and who seeks to define it? Mapping the site of social construction. *Journal of Information Technology*, 38(3), S. 239-266. https://doi.org/10.1177/02683962231159927

Dwivedi, Yogesh K.; Kshetri, Nir; Hughes, Laurie; Rana, Nripendra P.; Baabdullah, Abdullah M.; Kar, Arpan Kumar; Koohang, Alex; Ribeiro-Navarrete, Samuel; Belei, Nina; Balakrishnan, Janarthanan; Basu, Sriparna; Behl, Abhishek; Davies, Gareth H.; Dutot, Vincent; Dwivedi, Rohita; Evans, Leighton; Felix, Reto; Foster-Fletcher, Richard; Giannakis, Mihalis; Gupta, Ashish; Hinsch, Chris; Jain, Animesh; Patel, Nina Jane; Jung, Timothy; Juneja, Satinder; Kamran, Qeis; Mohamed AB, Sanjar; Pandey, Neeraj; Papagiannidis, Savvas; Raman, Ramakrishnan; Rauschnabel, Philipp A.; Tak, Preeti; Taylor, Alexandra; tom Dieck, M. Claudia; Viglia, Giampaolo; Wang, Yichuan und Yan, Meiyi (2023): Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse. *Information Systems Frontiers*, 25(5), S. 2071-2114. https://doi.org/10.1007/s10796-023-10400-x

EDSB (2016): Stellungnahme des Europäischen Datenschutzbeauftragten zu Systemen für das Personal Information Management (PIM): Hin zu einer intensiveren Einbindung der Nutzer in das Management und die Verarbeitung personenbezogener Daten, Brüssel: Europäischer Datenschutzbeauftragter. URL: https://www.edps.europa.eu/sites/default/files/publication/16-10-20_pims_opinion_de.pdf (besucht am 28.02.2025).

Europäische Kommission (2025): Datenschutz und Privatsphäre in virtuellen Welten. URL: https://digital-strategy.ec.europa.eu/policies/virtual-worlds-data-protection-privacy (besucht am 12.05.2025).

Falchuk, Ben; Loeb, Shoshana und Neff, Ralph (2018): The Social Metaverse: Battle for Privacy. *IEEE Technology and Society Magazine*, 37(2), S. 52-61. https://doi.org/10.1109/MTS.2018.2826060

Fernandez, Carlos Bermejo und Hui, Pan (2022): Life, the Metaverse and Everything: An Overview of Privacy, Ethics, and Governance in Metaverse. *2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, S. 272-277. https://doi.org/10.1109/ICDCSW56584.2022.00058

Fotios, Steve A.; Robbins, Chloe J. und Farall, Stephen (2021): The Effect of Lighting on Crime Counts. *Energies*, 14(14), 4099, S. 1-14. https://doi.org/10.3390/en14144099

Franks, Mary-Ann (2017): The Desert of the Unreal: Inequality in Virtual and Augmented Reality. *UC Davis Law Review*, 51(2), S. 499-538.

Freeman, Gou; Zamanifard, Samaneh; Maloney, Divine und Acena, Dane (2022): Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW1), 85, S. 1-30. https://doi.org/10.1145/3512932

Gartner (07. Februar 2022): Gartner Predicts 25% of People Will Spend At Least One Hour Per Day in the Metaverse by 2026, gartner.com. URL: https://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-metaverse-by-2026 (besucht am 28.02.2025).

Gerpott, Torsten J. (2020): Datenschutzerklärungen – Materiell fundierte Einwilligungen nach der DS-GVO. Empirischer Forschungsstand und Verbesserungsfelder. *Multimedia und Recht*, S. 739-744.

Happa, Jassim; Steed, Anthony und Glencross, Mashhuda (2021): Privacy-certification standards for extended-reality devices and services. *2021 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*, S. 397-398. https://doi.org/10.1109/VRW52623.2021.00085

Hunter, Julian; Ebert, Andreas und Spieker genannt Döhmann, Indra (2024): Informationspflichten und Einwilligung bei der Nutzung von PIMS: Probleme und Potenziale der Einwilligungsverwaltung de lege lata. *Zeitschrift für Datenschutzrecht*, S. 603-610.

Jandt, Silke und Steidle, Roland (Hrsg.) (2025): Datenschutz und Internet. 2. Auflage. Baden-Baden: Nomos.

Kang, Giluk; Koo, Jahoon und Kim, Young-Gab (2024 Security and Privacy Requirements for the Metaverse: A Metaverse Applications Perspective. *IEEE Communications Magazine*, 62(1), S. 148-154. https://doi.org/10.1109/MCOM.014.2200620

Kern, Michael (2024): Die Verwendung von Social Bots – Transparenzpflichten gemäß Medienstaatsvertrag und KI-VO sowie deren Umsetzung in virtuellen Welten. *KI und Recht*, S. 94-99.

Kettner, Sara Elisa; Thorun, Christian und Spindler, Gerald (2020): Innovatives Datenschutz-Einwilligungsmanagement: Abschlussbericht im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz, Berlin: BMJV. URL: https://www.conpolicy.de/data/user_upload/Studien/ConPolicy_Innovatives_Einwilligungsmanagement.pdf (besucht am 28.02.2025).

Kettner, Sara Elisa; Thorun, Christian und Vetter, Max (2018): Wege zur besseren Informiertheit. Verhaltenswissenschaftliche Ergebnisse zur Wirksamkeit des One-Pager-Ansatzes und weiterer Lösungsansätze im Datenschutz. Vorgelegt bei der: Bundesanstalt für Landwirtschaft und Ernährung (BLE), Bonn. URL: https://www.conpolicy.de/data/user_upload/Studien/Bericht_ConPolicy_2018_02_Wege_zur_besseren_Informiertheit.pdf (besucht am 05.05.2025).

Klar, Manuel; Wegmann, Simon Clemens und Galandi, Michaela (2022): Datenschutz im Metaverse. *Betriebsberater*, S. 2691-2696.

Klink-Straub, Judith und Straub, Tobias (2024): Und bist du nicht willig, so brauch‘ ich … PIMS – Entwurf der Einwilligungsverwaltungsverordnung nach § 26 TDDDG. Newsdienst ZD-Aktuell, 01820.

Kroschwald, Steffen (2023): Nutzer-, kontext- und situationsbedingte Vulnerabilität in digitalen Gesellschaften: Schutz, Selbstbestimmung und Teilhabe „by Design“ vor dem Hintergrund des Art. 25 DS-GVO und dem KI-Verordnungsentwurf. *Zeitschrift für Digitalisierung und Recht*, S. 1-22.

Kühling, Jürgen; Sauerborn, Cornelius (2022): PIMS vs. Einwilligung vs. Browsereinstellungen. *Zeitschrift für Datenschutz*, S. 596-599.

Maloney, Divine; Zamanifard, Samaneh und Freeman, Guo (2020): Anonymity vs. Familiarity: Self-Disclosure and Privacy in Social Virtual Reality. *Proceedings of the 26th ACM Symposium on Virtual Reality Software and Technology*, 25, S. 1-9. https://doi.org/10.1145/3385956.3418967

Marloth, Maria; Chandler, Jennifer und Vogeley, Kai (2020): Psychiatric Interventions in Virtual Reality: Why We Need an Ethical Framework. *Cambridge Quarterly of Healthcare Ethics*, 29(4), S. 574-584. https://doi.org/10.1017/S0963180120000328

McStay, Andrew (2023): The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons. *Philosophy and Technology*, 36, 13, S. 1-26. https://doi.org/10.1007/s13347-023-00613-y

Mello, Manuel; Dupont, Lennie; Engelen, Tahnée; Acciarino, Adriano; de Borst, Aline und de Gelder, Beatrice (2022): The influence of body expression, group affiliation and threat proximity on interactions in virtual reality. *Current Research in Behavioral Sciences*, 3, 100075, S. 1-8. https://doi.org/10.1016/j.crbeha.2022.100075

Mitre-Becerril, David; Tahamont, Sarah; Lerner, Jason und Chalfin, Aaron (2022): Can deterrence persist? Long-term evidence from a randomized experiment in street lighting. *Criminology & Public Policy*, 21(4), S. 865-891. https://doi.org/10.1111/1745-9133.12599

Nüske, Niclas; Olenberger, Christian; Rau, Daniel und Schmied, Fabian (2019): Privacy Bots. Digitale Helfer für mehr Transparenz im Internet. *Datenschutz und Datensicherheit*, S. 28-32.

Papagiannidis, Savvas; Bourlakis, Michael und Li, Feng (2008): Making real money in virtual worlds: MMORPGs and emerging business opportunities, challenges and ethical implications in metaverses. Technological Forecasting and Social Change, 75(5), S. 610-622. https://doi.org/10.1016/j.techfore.2007.04.007

Roblox (22. Januar 2025): Roblox-Datenschutz- und Cookie-Richtlinie, roblox.com URL: https://en.help.roblox.com/hc/article_attachments/20961293100820 (besucht am 28.02.2025).

Rosenblat, Mariana Olaizola (2023): Reality Check: How to Protect Human Rights in the 3D Immersive Web, Ney York City: NYU Stern Center for Business and Human Rights. URL: https://bhr.stern.nyu.edu/wp-content/uploads/2023/09/NYUCBHRMetaverse_Sep5ONLINEFINALCOVER1ADA.pdf (besucht am 28.02.2025).

Ruiz Mejia, Jose M. und Rawat, D. B. (2022): Recent Advances in a Medical Domain Metaverse: Status, Challenges, and Perspective. *2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, S. 357-362. https://doi.org/10.1109/ICUFN55119.2022.9829645

Schuchardt, Lisa-Marie (2025): Die (ferne) Zukunft der Cookie-Einwilligung: PIMS und der Weg zu datenschutzfreundlichen Lösungen, *Datenschutz-Berater*, S. 103-106.

Simitis, Spiros; Hornung, Gerrit und Spiecker genannt Döhmann, Indra (Hrsg.) (2025): Datenschutzrecht. 2. Auflage. Baden-Baden: Nomos.

Smith, Carl H.; Molka-Danielsen, Judith; Rasool, Jazz und Webb-Benjamin, Jean-Brunel (2023): The World as an Interface: Exploring the Ethical Challenges of the Emerging Metaverse. *Proceedings of the 56th Hawaii International Conference on System Sciences*, S. 6045-6054. https://hdl.handle.net/10125/103367

Specht-Riemenschneider, Louisa; Blankertz, Aline; Sierek, Pascal; Schneider, Ruben; Knapp, Jakob und Henne, Theresa (2021 Die Datentreuhand: Ein Beitrag zur Modellbildung und rechtlichen Strukturierung zwecks Identifizierung der Regulierungserfordernisse für Datentreuhandmodelle. *Multimedia und Recht Beilage*, S. 25-48.

Spindler, Gerald und Förster, Lydia (2023): Privacy-compliant design of Cookie Banners according to the GDPR. *JIPITEC*, 14(1), S. 2-33.

Steege, Hans und Chibanguza, Kuuya J. (Hrsg.) (2023): Metaverse: Rechtshandbuch. Baden-Baden: Nomos.

Stephenson, Neal (1992): Snow Crash. New York City: Bantam Books.

Tricomi, Pier Paolo; Nenna, Federica; Pajola, Luca; Conti, Mauro und Gemberini, Luciano (2023): You Can't Hide Behind Your Headset: User Profiling in Augmented and Virtual Reality. *IEEE Access*, 11, S. 9859-9875. https://doi.org/10.1109/ACCESS.2023.3240071

Venugopal, Jothi Prakash; Subramanian, Arul Antran Vijay und Peatchimuthu, Jegathesh (2023): The realm of metaverse: A survey. *Computer Animation and Virtual Worlds*, 34(5), S. 1-28. https://doi.org/10.1002/cav.2150

Vladimirov, Ivaylo; Nenova, Maria; Nikolova, Desislava und Terneva, Zornitsa (2022): Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse: A Survey. *2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)*, S. 1-4. https://doi.org/10.1109/ICEST55168.2022.9828791

Wang, Cheng Yao; Sriram, Sandhya und Stevenson Won, Andrea (2021): Shared Realities: Avatar Identification and Privacy Concerns in Reconstructed Experiences. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 337, S. 1-25. https://doi.org/10.1145/3476078

Wiederhold, Brenda (2022): Sexual Harassment in the Metaverse. Cyberpsychology, Behavior, and Social Networking, 25(8), S. 479-548. https://doi.org/10.1089/cyber.2022.29253.editorial

Xie, Runjie; Kirchner-Krath, Jeanine und Morschheuser, Benedikt (2024): Towards an Ethical Metaverse: A Systematic Literature Review on Privacy Challenges. *Proceedings of the 32nd European Conference on Information Systems (ECIS 2024),6.*

Mitarbeiterinnen und Mitarbeiter dieses Bandes

Lorenz Baum
ist wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl von Prof. Dr. Oliver Hinz für Wirtschaftsinformatik und Informationsmanagement an der Goethe-Universität Frankfurt und Teil des interdisziplinären Konsortialprojekts „PERISCOPE", gefördert vom Bundesministerium für Bildung und Forschung. E-Mail: baum@wiwi.uni-frankfurt.de

Andreas Baur
ist wissenschaftlicher Mitarbeiter am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen und Fellow am Critical Infrastructure Lab Amsterdam. E-Mail: a.baur@uni-tuebingen.de

Dr. Felix Bieker
ist juristischer Mitarbeiter imForschungsbereich des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und untersucht Digitale Infrastrukturen, Plattformen und das EU-Datenrecht.

Dr. Andreas Bischof
ist Juniorprofessor für „Soziologie mit Schwerpunkt Technik" an der Technischen Universität Chemnitz und koordiniert das Verbundprojekt „Simplications – Implikationen (vermeintlich) einfacher Sensordaten für Privatheit im Zuhause", das vom BMFTR gefördert wird. E-Mail: andreas.bischof@hsw.tu-chemnitz.de

Felix Büning
ist Mitarbeiter im interdisziplinären Konsortialprojekt „PRIME", gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt und wissenschaftlicher Mitarbeiter am Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Rechtsvergleichung, Multimedia- und Telekommunikationsrecht an der Georg-August-Universität Göttingen. E-Mail: felix.buening@jura.uni-goettingen.de

Marwan El-Rifaai
war Mitarbeiter im interdisziplinären Konsortialprojekt „PRIME", gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt und bis Juni 2025 wissenschaftlicher Mitarbeiter am Lehrstuhl für Bürgerliches Recht, Recht der Datenwirtschaft, des Datenschutzes und der Künst-

lichen Intelligenz beschäftigt. Derzeit arbeitet er als wissenschaftliche Hilfskraft bei der Rechtsanwaltskanzlei Tölle Wagenknecht in Bonn. E-Mail: elrifaai@posteo.de

Florian Franke
ist Mitarbeiter im interdisziplinären Konsortialprojekt „PRIME", gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt und Projektmanager beim ConPolicy-Institut für Verbraucherpolitik in Berlin. E-Mail: f.franke@conpolicy.de

Dr. Michael Friedewald
leitet das Geschäftsfeld „Informations- und Kommunikationstechnik" am Fraunhofer-Institut für System- und Innovationsforschung ISI in Karlsruhe. Er ist Koordinator der „Plattform Privatheit". E-Mail: michael.friedewald@isi.fraunhofer.de

Dr. Christian Geminn
ist Privatdozent für Öffentliches Recht und Recht der digitalen Gesellschaft sowie Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel und geschäftsführender Gesellschafter der Datenrecht Beratungsgesellschaft (DRBG). E-Mail: c.geminn@uni-kassel.de

Mario Göbel
ist Mit-Gründer der VREEDA GmbH, einer IoT-Plattform, die ein Ökosystem für smarte Geräte mit klarer Ausrichtung auf Datensouveränität und transparente Datenflüsse aufbaut. Die VREEDA GmbH ist Projektpartner im BMBF-geförderten Forschungsprojekt „Opt-IN": Optimierung informationeller Nachhaltigkeit für Bürgerinnen und Bürger in Datenökosystemen". Heute begleitet er zudem Start-ups als Projektleiter eines öffentlichen Inkubator-Programms und engagiert sich für ein starkes Gründungsökosystem. E-Mail: mario.goebel@vreeda.com

Björn Hanneke
ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik und Informationsmanagement (Prof. Dr. Oliver Hinz) der Goethe-Universität Frankfurt sowie im interdisziplinären Konsortialprojekt „PERISCOPE", das vom Bundesministerium für Bildung und Forschung gefördert wird. E-Mail: hanneke@wiwi.uni-frankfurt.de

Dr. h.c. Marit Hansen
ist die Landesbeauftragte für Datenschutz und Informationszugang des Landes Schleswig-Holstein. Die Diplom-Informatikerin leitet das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD). E-Mail: marit.hansen@datenschutzzentrum.de

Dr. Jessica Heesen
ist Leiterin des Forschungsschwerpunkts Medienethik, Technikphilosophie und KI am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen. E-Mail: jessica.heesen@uni-tuebingen.de

Dr. Martin Hennig
ist Teamleiter im Bereich Medienethik und Digitalisierung am Internationalen Zentrum für Ethik in den Wissenschaften (IZEW) der Universität Tübingen. E-Mail: martin.hennig@uni-tuebingen.de

Dr. Simon Hensellek
ist Juniorprofessor für Entrepreneurship und Digitalisierung an der Technischen Universtität Dortmund und Projektleiter des BMBF-geförderten Projekts „Opt-IN: Optimierung informationeller Nachhaltigkeit für Bürgerinnen und Bürger in Datenökosystemen". Er ist außerdem Gründer des European Academic Coworking Network (www.eacn.network), einem europaweiten Netzwerk von Forschenden zur Förderung kollaborativer, interdisziplinärer und ortsunabhängiger Wissenschaftspraxis. E-Mail: simon.hensellek@tu-dortmund.de

Tom Hubert
ist Mitarbeiter im interdisziplinären Konsortialprojekt „PRIME", gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt und wissenschaftlicher Mitarbeiter am Institut für Rechtswissenschaften an der Technischen Universität Braunschweig. E-Mail: tom.hubert@tu-braunschweig.de

Paul C. Johannes
ist wissenschaftlicher Mitarbeiter in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informations-Technikgestaltung (ITeG) an der Universität Kassel. Er ist geschäftsführender Gesellschafter der Datenrecht Beratungsgesellschaft (DRBG) und Rechtsanwalt. E-Mail: paul.johannes@uni-kassel.de.

Dr. Murat Karaboga
ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für System- und Innovationsforschung ISI in Karlsruhe. E-Mail: murat.karaboga@isi.fraunhofer.de

Michael Kern
war Mitarbeiter im interdisziplinären Konsortialprojekt „PRIME", gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt und bis April 2025 wissenschaftlicher Mitarbeiter am Lehrstuhl für Bürgerliches Recht, Recht der Datenwirtschaft, des Datenschutzes und der künstlichen Intelligenz an der Universität Bonn beschäftigt, jetzt Rechtsreferendar am Oberlandesgericht Köln.

Lennart Kiss
ist wissenschaftlicher Mitarbeiter am Universität Stuttgart am Institut für Arbeitswissenschaft und Technologiemanagement IAT in Stuttgart. E-Mail: lennart.kiss@iat.uni-stuttgart.de

Dr. Sara Elisa Kettner
ist Mitarbeiterin im interdisziplinären Konsortialprojekt „PRIME", gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt und Projektmanagerin beim ConPolicy-Institut für Verbraucherpolitik in Berlin. E-Mail: s.e.kettner@conpolicy.de

Dr. Heiner Koch
war wissenschaftlicher Mitarbeiter im ethischen Teilprojekt von DiversPrivat am Lehrstuhl für praktische Philosophie der Universität Passau. E-Mail: koch.heiner@gmail.com

Huda Koulani
ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Wirtschaftsinformatik und Systementwicklung an der Universität Kassel. E-Mail: koulani@uni-kassel.de

Dr. Nicole Krämer
ist Professorin für Sozialpsychologie: Medien und Kommunikation an der Universität Duisburg-Essen in der Fakultät für Informatik sowie PI im vom BMFTR geförderten Projekt *DiversPrivat* (Diversitätsgerechter Privatheitsschutz in Online-Umgebungen). Zudem ist sie Gründungsmitglied des *Research Centers for Trustworthy Data Science and Security* der Universitätsallianz Ruhr. E-Mail: nicole.kraemer@uni-due.de

Dr. Otmar Lell
ist Mitarbeiter im interdisziplinären Konsortialprojekt „PRIME", gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt und Projektmanager beim ConPolicy-Institut für Verbraucherpolitik in Berlin. E-Mail: o.lell@conpolicy.de

Maximilian Lukat
ist wissenschaftlicher Mitarbeiter am Alexander von Humboldt Institut für Internet und Gesellschaft, Berlin. E-Mail: maximilian.lukat@hiig.de

Markus Meyer
ist Mitarbeiter im interdisziplinären Konsortialprojekt „PRIME", gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt und wissenschaftlicher Mitarbeiter am Lehrstuhl für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Rechtsvergleichung, Multimedia- und Telekommunikationsrecht an der Georg-August-Universität Göttingen. E-Mail: markus.meyer@jura.uni-goettingen.de

Dr. Johanna E. Möller
vertritt die Professur für Mediensoziologie an der Justus-Liebig-Universität Gießen. Sie ist Projektleiterin im interdisziplinären Forschungsprojekt "DIPCY –Disruptionen vernetzter Privatheit" an der TU Dresden. E-Mail: johanna.moeller@sowi.uni-giessen.de

Dr. Benedikt Morschheuser
ist Mitarbeiter im interdisziplinären Konsortialprojekt „PRIME", gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt und Professor und Inhaber des Lehrstuhls für Wirtschaftsinformatik an der Otto-Friedrich-Universität Bamberg. E-Mail: benedikt.morschheuser@uni-bamberg.de

Dr. Maxi Nebel
ist wissenschaftliche Mitarbeiterin in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel sowie geschäftsführende Gesellschafterin der Datenrecht Beratungsgesellschaft. E-Mail: m.nebel@uni-kassel.de

Dr. German Neubaum
ist Juniorprofessor für „Psychologische Prozesse der Bildung in sozialen Medien" an der Universität Duisburg-Essen. In seiner Forschung untersucht er, wie sich die Nutzung von Technologie auf politische Meinungen,

moralische Werte, Privatheit und zwischenmenschliche Beziehungen auswirken kann. Er ist Associate Editor beim *Journal of Media Psychology*. E-Mail: german.neubaum@uni-due.de

Dr. Carsten Ochs
ist aktuell Gastprofessor für Technik- und Innovationssoziologie am Intitut für Soziologie der Technischen Universität Berlin und koordiniert ansonsten das Verbundprojekt „BeDeNutz: Die Beratung der Nutzenden" am Fachgebiet Soziologische Theorie der Universität Kassel. Email: carsten.ochs@uni-kassel.de

Sebastian Rehms
ist wissenschaftlicher Mitarbeiter und Doktorand im interdisziplinären Forschungsprojekt "DIPCY –Disruptionen vernetzter Privatheit" an der TU Dresden. E-Mail: sebastian.rehms@tu-dresden.de

Dr. Delphine Reinhardt
ist W3-Professorin an der Georg-August-Universität Göttingen und leitet dort die Forschungsgruppe Computer Sicherheit und Privatheit. E-Mail: reinhardt@cs.uni-goettingen.de

Dr. Karoline Reinhardt
ist Professorin für Angewandte Ethik an der Universität Passau. Dort ist sie PI im vom BMFTR geförderten Projekt *DiversPrivat* (Diversitätsgerechter Privatheitsschutz in Online-Umgebungen). E-Mail: karoline.reinhardt@uni-passau.de

Dr. Alexander Roßnagel
ist Seniorprofessor für öffentliches Recht mit dem Schwerpunkt Recht der Technik und des Umweltschutzes an der Universität Kassel, Sprecher der Plattform Privatheit sowie Datenschutzbeauftragter des Landes Hessen. E-Mail: a.rossnagel@uni-kassel.de

Volkan Sayman
ist wissenschaftlicher Mitarbeiter am nexus Institut für Kooperationsmanagement und interdisziplinäre Forschung, Berlin. E-Mail: sayman@nexus-institut.de

Rachelle Sellung
ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO in Stuttgart. E-Mail: rachelle.sellung@iao.fraunhofer.de

Dr. Ina Schiering
ist Professorin an der Ostfalia Hochschule für angewandte Wissenschaften und leitet dort das Institut für Verteilte Systeme. E-Mail: i.schiering@ostfalia.de

Luisa Schmied
ist wissenschaftliche Mitarbeiterin in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel. E-Mail: luisa.schmied@uni-kassel.de

Lukas Schmitz
ist wissenschaftlicher Mitarbeiter und Doktorand im interdisziplinären Forschungsprojekt "DIPCY –Disruptionen vernetzter Privatheit" an der TU Dresden. E-Mail: lukas.schmitz@tu-dresden.de

Dr. Ingrid Schneider
ist Professorin für Politikwissenschaft; sie forscht und lehrt zu Ethik und Governance von IT am Fachbereich Informatik der Universität Hamburg. E-Mail: Ingrid.Schneider@uni-hamburg.de

Clara Strathmann
ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Sozialpsychologie: Medien und Kommunikation an der Universität Duisburg-Essen in der Fakultät für Informatik. Dort ist sie Doktorandin im vom BMFTR geförderten Projekt *DiversPrivat* (Diversitätsgerechter Privatheitsschutz in Online-Umgebungen). E-Mail: clara.strathmann@uni-due.de

Dr. Christian Thorun
ist Mitarbeiter im interdisziplinären Konsortialprojekt „PRIME", gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt und Geschäftsführer des ConPolicy-Instituts für Verbraucherpolitik in Berlin. E-Mail: c.thorun@conpolicy.de

Dr. Andreas Wiebe
ist Mitarbeiter im interdisziplinären Konsortialprojekt „PRIME", gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt und Professor und Inhaber des Lehrstuhls für Bürgerliches Recht, Wettbewerbs- und Immaterialgüterrecht, Medien- und Informationsrecht an der Georg-August-Universität Göttingen. E-Mail: lehrstuhl.wiebe@jura.uni-goettingen.de

Runjie Xie
ist Mitarbeiter im interdisziplinären Konsortialprojekt „PRIME", gefördert vom Bundesministerium für Forschung, Technologie und Raumfahrt und wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik an der Otto-Friedrich-Universität Bamberg. E-Mail: runjie.xie@uni-bamberg.de