Daten-Fairness in einer globalisierten Welt

Friedewald, Michael (Ed.); Roßnagel, Alexander (Ed.); Neuburger, Rahild (Ed.); Bieker, Felix (Ed.); Hornung, Gerrit (Ed.)

Veröffentlichungsversion / Published Version
Sammelwerk / collection

Empfohlene Zitierung / Suggested Citation:
Friedewald, M., Roßnagel, A., Neuburger, R., Bieker, F., & Hornung, G. (Hrsg.). (2023). *Daten-Fairness in einer globalisierten Welt* (Privatheit und Selbstbestimmung in der digitalen Welt / Privacy and Self-Determination in the Digital World, 2). Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748938743

Privatheit und Selbstbestimmung in der digitalen Welt | 2

Friedewald | Roßnagel Neuburger | Bieker | Hornung [Hrsg.]

Daten-Fairness in einer globalisierten Welt

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 2

Michael Friedewald | Alexander Roßnagel
Rahild Neuburger | Felix Bieker | Gerrit Hornung [Hrsg.]

Daten-Fairness in einer globalisierten Welt

Nomos

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

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 2023

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): 978-3-7560-0518-5
ISBN (ePDF): 978-3-7489-3874-3

DOI: https://doi.org/10.5771/9783748938743

Onlineversion
Nomos eLibrary

Vorwort

Die zunehmend datenökonomisch gefasste und motivierte Organisation unterschiedlichster gesellschaftlicher Teilbereiche der digitalen Welt konfrontiert zeitgenössische Gemeinwesen mit zahlreichen, nur im interdisziplinären Dialog zu bearbeitenden Problemstellungen: vom gewandelten Modus demokratischer Politik über Fragen einer nachhaltigen digitalen Ökonomie bis hin zu grundlegenden Konzepten der Moderne, etwa dem der individuellen Selbstbestimmung. Um sich diesen Fragen im Rahmen eines über die Wissenschaft hinausweisenden Diskurses zu stellen, veranstaltete die vom Bundesministerium für Bildung und Forschung (BMBF) geförderte „Plattform Privatheit" am 13. und 14. Oktober 2022 in Berlin die Konferenz „Daten-Fairness in einer globalisierten Welt – Grundrechtsschutz und Wettbewerb für eine internationale Data Governance". Der vorliegende Band stellt die wichtigsten Vorträge vor und reflektiert die dort angestoßenen Diskussionen.

Die Plattform Privatheit vernetzt interdisziplinäre wissenschaftliche Projekte, die vom BMBF 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 der Plattform 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 Akteure zu ethischen, rechtlichen und sozialen 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 Privatheit" arbeitete acht Jahre lang – ebenfalls mit Förderung des BMBF –

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 „Daten-Fairness in einer globalisierten Welt – Grundrechtsschutz und Wettbewerb für eine internationale Data Governance" durchgeführt.

Die inhaltliche Gestaltung der Konferenz erfolgte in Kooperation mit dem ersten im Rahmen der „Plattform Privatheit" durch das BMBF geförderten Projekt „PRIvatheit, Demokratie und Selbstbestimmung im Zeitalter von KI und Globalisierung" (PRIDS), an dem neben dem Fraunhofer ISI und der Universität Kassel auch noch die Ludwig-Maximilians-Universität München, das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein sowie die Universitäten Tübingen und Duisburg-Essen beteiligt sind.

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 allen Beteiligten an der „Plattform Privatheit" sowie den Kolleg:innen, die die in diesem Band veröffentlichten Texte begutachtet haben. Die Konferenz „Daten-Fairness in einer globalisierten Welt – Grundrechtsschutz und Wettbewerb für eine internationale Data Governance" 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, Frank Ebbers, Murat Karaboga und Stephanie Peter (Fraunhofer ISI) sowie Christian Geminn, Tamer Bile und Carsten Ochs (Universität Kassel). Darüber hinaus danken wir Barbara Ferrarese (Fraunhofer ISI) für die professionelle Wissenschaftskommunikation, Miriam Janke (Fusionistas) für die konzeptionelle Beratung und lebendige Moderation sowie Magdalena Vollmer für die kreative Live-Visualisierung der Vorträge sowie die grafische Gestaltung des Bucheinbandes.

Dieser Band wäre nicht ohne tatkräftige Unterstützung bei der Manuskriptbearbeitung und -korrektur zustande gekommen. Wir möchten uns sehr herzlich bedanken bei den Kolleg:innen, die die Begutachtung der

Tagungsbeiträge übernommen haben. 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 (BMBF) für die Förderung der Plattform Privatheit sowie die engagierte Unterstützung unserer Forschungsthemen bedanken. Auch danken wir Jan-Ole Malchow, 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

Karlsruhe, Kiel, Kassel, München, im Juni 2023

Inhaltsverzeichnis

Einleitung: Daten-Fairness in einer globalisierten Welt – Grundrechtsschutz und Wettbewerb für eine internationale Data Governance?

Michael Friedewald, Felix Bieker, Gerrit Hornung, Rahild Neuburger und Alexander Roßnagel

1. Zum Thema dieses Bandes

Digitale Plattformen wie soziale Netzwerke und andere digitale Dienste sind zentrale Infrastrukturen der digitalen Welt. Sie agieren global und permanent. Ihre Nutzung ist für nahezu alle, die an der digitalen Welt teilhaben wollen, unverzichtbar. Für Milliarden Menschen weltweit stellen sie einen wesentlichen Teil ihrer Online-Erfahrung dar. Die zugrundeliegenden Informationstechnologien sind ein fester Bestandteil ihres persönlichen und beruflichen Lebens und nehmen beständig mehr Einfluss auf dieses. Nutzende wissen zwar, dass sie durch die Verwendung digitaler Plattformen personenbezogene Daten über sich preisgeben, sind sich jedoch oftmals weder über den Umfang der über sie gespeicherten Daten noch über alle Rückschlüsse bewusst, die aus diesen Daten gezogen werden.

Plattformen sind vielfach die Grundlage für einen Informationsaustausch. Sie entscheiden mit darüber, welche gesellschaftlichen, politischen und kommerziellen Informationen an wen weitergegeben und in ihrer Darstellung priorisiert werden. Sie haben daher nicht zu unterschätzenden Einfluss auf den Wettbewerb von Ideen und Haltungen, politischen Parteien und Politiker:innen, Gütern und Dienstleistungen. Mit der Internationalisierung des Wirtschafts- und Handelsverkehrs finden kontinuierlich grenzüberschreitende Datenströme statt. Aufgrund der zentralen Stellung der Plattformen als Teil einer globalen Infrastruktur stellen sich grundlegende Fragen bezüglich der fairen Ausgestaltung einer Data Governance in der digitalisierten Welt.

Diskussionen über die politische Positionierung eines Landes und dessen wirtschaftliche Wettbewerbsfähigkeit sind heutzutage vielfach mit Daten und damit dem Thema Data Governance verbunden. Dieses Thema wird aber regelmäßig nur in regionalen Vorschriften zum Datenschutz, zum Wettbewerb, zum Datenzugang, zum Verbraucherschutz und zu vie-

len weiteren damit verbundenen Gesetzen aufgegriffen. Unterschiede zeigen sich exemplarisch zwischen den USA, der EU und China: In den USA gelten, unter weitreichenden Ausnahmen für die nationale Sicherheit, Datenschutzregelungen vor allem für staatliche Stellen. Die Datenverarbeitung durch private Unternehmen gilt dagegen als Grundrechtsausübung, während der Datenschutz keine Grundrechtsqualität hat. China regelt die ordnungsgemäße und sichere Verarbeitung personenbezogener Daten, nimmt davon aber die Verarbeitung personenbezogener Daten für die Zwecke der nationalen Sicherheit und wirtschaftlichen Entwicklung aus und ermöglicht so ein weitgehende Überwachung der Bevölkerung. Der Rechtsrahmen in der Europäischen Union ist dagegen umfassender, betont den Grundrechtsschutz der Nutzenden und die Rechtsstaatlichkeit, schützt Bürger:innen umfassend nicht nur vor Datenverarbeitung durch staatliche Stellen, sondern auch durch Privatunternehmen und legt fest, dass Daten grundsätzlich nur in Länder mit einem angemessenen Datenschutzsystem übermittelt werden dürfen.

Die aktuelle Diskussion über globale Data Governance ist nicht nur mit gegensätzlichen Ansichten über nationale Data Governance, sondern auch mit anderen Herausforderungen wie divergierenden Interessen zwischen Einzelpersonen und Unternehmen im internationalen Wettbewerb verbunden. So beruht der Erfolg der weltweit dominanten Tech-Unternehmen auf der hoch entwickelten Fähigkeit, Datenbestände zu sammeln, zu strukturieren, zu kontrollieren und zu vermarkten. Big Data und ihre Anwendung im Rahmen der sogenannten künstlichen Intelligenz beispielsweise können die Art und Weise, wie wir leben und arbeiten, nachhaltig verändern.

Technologien wirken oft als Machtverstärker zugunsten bereits mächtiger Akteure und vergrößern das Gefälle zwischen Nutzenden und Plattformen, Beschäftigten und Arbeitgeber:innen, Bürger:innen und dem Staat. Um diese Machtasymmetrie zu überwinden, sind Instrumente wie Einwilligung oder Betroffenenrechte allein nicht effektiv. Neben dieser individuellen Dimension, rücken deshalb strukturelle Aspekte von Datenschutz und Privatheit – jedenfalls in Europa und den USA – in den Fokus. Diese systemische Sichtweise nimmt den Erhalt des demokratischen Rechtsstaates in den Blick. Dessen Schutz darf dabei nicht auf technische Maßnahmen verkürzt werden, sondern verhindert durch geeignete Vorgaben, dass Datenverarbeitungsvorgänge demokratische Institutionen und rechtstaatliche Garantien gefährden oder gar aufheben. Dazu zählt eine informationelle Gewaltenteilung, damit nicht derjenige, der Infrastrukturen bereitstellt – unabhängig davon, ob dies der Staat oder Plattformanbieter sind – alle

Daten zentral vorhält. Aus dieser Sichtweise heraus lassen sich auch Anforderungen an Infrastrukturen und die Data Governance ableiten.

Im Mittelpunkt der globalen wirtschaftspolitischen Ordnung, die sich seit der zweiten Hälfte des 20. Jahrhunderts herausgebildet hat, steht traditionell die internationale Wirtschaftskooperation. Debatten rund um Daten- und Technologie-Souveränität stellen in jüngster Zeit den Wert internationaler Wirtschaftskooperationen und Datenflüsse jedoch zunehmend infrage und könnten eine Verschiebung der noch geltenden Wirtschaftsordnung zum Ergebnis haben. Der Umgang mit Daten als Querschnittsthema, das bislang insbesondere mit den Politikfeldern der Wirtschaftspolitik und des Grundrechtsschutzes verknüpft war, gerät im Ergebnis dieser Entwicklung zunehmend in den diskursiven Einzugsbereich geopolitischer Interessen und bringt damit eine Reihe von neuen Fragen in die Debatte zu Datenschutz und Datennutzung.

Im Rahmen der Konferenz haben sich die Teilnehmer:innen interdisziplinär mit den Gestaltungsherausforderungen und -möglichkeiten auseinandergesetzt, die für eine zukunftsfähige und internationale Governance des Umgangs mit personenbezogenen Daten aufkommen. Angesprochen waren dabei vielfältige technische, ökonomische, soziale, politische und rechtliche Ansätze, um Privatheit und informationelle Selbstbestimmung in der digitalen Welt fortzuentwickeln. Dies betrifft interdisziplinäre Einzelfragen sowie die Wechselwirkung der verschiedenen Perspektiven auf das Thema. Dazu wurden verschiedene normative, institutionelle und instrumentelle Konzepte von Datenschutz in einer digitalen Gesellschaft diskutiert sowie konstruktive Bausteine für eine zukunftsgerechte Gewährleistung von individueller und kollektiver Selbstbestimmung und Grundrechten erörtert.

2. Die Beiträge

Dieser Band gliedert sich in fünf Teile, die verschiedene Aspekte des Themenspektrums aus unterschiedlicher Perspektive und mit unterschiedlicher Schwerpunktsetzung aufgreifen.

Fairness und Schutz schwacher Interessen

Die Beiträge im ersten Teil des Buchs widmen sich den Ursachen und Strukturen von Ungleichheit und Ungerechtigkeit in der digitalen Gesell-

schaft und Wirtschaft. Sie zeigen historische Kontinuitäten von Diskriminierung auf und thematisieren die Frage, welche Maßnahmen ergriffen werden können, um diesen Zustand zu ändern.

Mar Hicks (Illinois Institute of Technology, Chicago) Beitrag befasst sich mit der Kontinuität von Geschlechterverhältnissen in der Geschichte der Informationstechnik seit 1945. Hicks argumentiert, dass die Informatik von Anfang an ein Werkzeug der Macht war, das von den Einflussreichsten eingesetzt wurde, um soziale, politische und wirtschaftliche Ungleichheiten aufrechtzuerhalten. Es bestehe eine Notwendigkeit, die Geschichte der Informatik kritisch zu betrachten, um ihre Auswirkungen auf die heutige Gesellschaft zu verstehen.

Im Beitrag von *Felix Bieker* und *Marit Hansen* (Unabhängiges Landeszentrum für Datenschutz, Kiel) werden am Beispiel von Chatbots die Risiken algorithmischer Systeme für betroffene Personen, insbesondere marginalisierte Gruppen, im Zusammenhang mit Chatbots untersucht. Es werden Regelungen des Datenschutzrechts analysiert, relevante EU-Datengesetze betrachtet und Schlussfolgerungen aus dem Diskurs zum Antidiskriminierungsrecht gezogen. Die Autor:innen verdeutlichen, wie Prozesse, die auf Konzepten wie Data Justice und Design Justice basieren, Daten-Gerechtigkeit „by Design" gewährleisten können.

Daniel Guagnin, Fabian Dantscher und *Antonios Hazim* (Nexus Institut, Berlin) stellen in ihrem Beitrag einen partizipativen Ansatz vor, der die Betrachtung und Bewertung von Datenschutzrisiken ermöglicht und eine datenschutzfreundliche Gestaltung von KI-Anwendungen und algorithmischen Entscheidungssystemen unterstützt. Dieser Ansatz erlaubt es, Datenschutz und Diskriminierungsfreiheit bereits mit Beginn der Entwicklung gemeinsam zu berücksichtigen. Dabei werden die Anforderungen der DSGVO und des Value-Sensitive-Designs beachtet und die praktischen Herausforderungen bei der Durchführung von Datenschutz-Folgenabschätzungen einbezogen.

Fairer Wettbewerb in der Datenökonomie

Im zweiten Teil des Buchs wird die Fairness in der Wirtschaft thematisiert und auf verschiedenen Ebenen diskutiert. Dabei geht es darum, wie unerwünschte Verzerrungen des Wettbewerbs und ihre negativen Auswirkungen sowohl auf Einzelpersonen als auch auf die Gesellschaft insgesamt vermieden werden können. Dies beinhaltet die Untersuchung rechtlicher Regelungen, Geschäftsmodelle sowie spezieller Maßnahmen.

In ihrem Kurzbeitrag behandeln *Wolfgang Kerber* (Universität Marburg) und *Louisa Specht-Riehmenschneider* (Universität Bonn) die Probleme, die durch Informationsasymmetrien, Transaktionskosten, Verhaltensfehler und Wettbewerbsprobleme auf Datenmärkten entstehen. Sie erläutern, dass Individuen aus diesen Gründen nicht mehr selbstbestimmt über ihre Daten entscheiden können. Das Datenschutzrecht allein kann diese Probleme nicht lösen. Hier ist eine enge Zusammenarbeit mit dem Wettbewerbs- und Verbraucherschutzrecht notwendig. Dazu sind jedoch konzeptionelle Weiterentwicklungen in beiden Rechtsgebieten erforderlich.

Der Beitrag von *Sebastian Kasper* und *Timo Hoffmann* (Universität Passau) untersucht Sanktionen gegen Datenschutzverstöße, die auf die Reputation des Verletzenden abzielen. Die Autoren argumentieren, dass solche indirekten Maßnahmen – anders als die direkten Sanktionen des Datenschutzrechts – als effektives Abschreckungsmittel für Unternehmen in datengetriebenen Branchen dienen können. Sie heben die Verbreitung solcher Maßnahmen in verschiedenen Datenschutzgesetzen hervor, identifizieren jedoch auch Unsicherheiten bei der Bewertung ihrer Wirksamkeit. Sie schlagen eine Typologie vor, die eine Bewertung von regulatorischen Konzepten erlaubt, die auf die Repuation von Akteuren abzielen.

Tom Schmidt (Universität Frankfurt) untersucht in seinem Kapitel eine neue Fallgruppe des Missbrauchs einer marktbeherrschenden Stellung, die 2020 vom BGH in einem Urteil gegen Facebook definiert wurde. Er erläutert insbesondere das zugrunde liegende Prüfschema und wie das Gericht eine Verbindung zwischen Datenschutzrecht und Kartellrecht hergestellt hat. Schmidt betont, dass trotz offener Fragen bezüglich eines angemessenen Alternativszenarios im weiteren Verfahrensverlauf voraussichtlich Klarheit über zentrale Fragen der neuen Fallgruppe geschaffen werden wird.

Lars Pfeiffer (Universität Kassel) und Kolleg:innen diskutieren in ihrem Beitrag Lösungen, um datenbasierte Geschäftsmodelle mit den europäischen Datenschutz-Anforderungen in Einklang zu bringen. Sie empfehlen die Implementierung eines Transaktionsjournals als zentralen Bestandteil eines Personal Rights Management-Systems. Dieses soll den Betroffenen eine transparente Darstellung der Datenverarbeitung bieten und ihnen Interventionsmöglichkeiten ermöglichen. Gleichzeitig kann das Transaktionsjournal Unternehmen dabei helfen, ihre Datenverarbeitungstätigkeiten zu überwachen und die Einhaltung der Datenschutzanforderungen nachzuweisen.

Simon Engert (LMU München), *Jonathan Kropf* und *Markus Uhlmann* (Universität Kassel) untersuchen die Rolle technischer und regulativer Da-

tenschutzinitiativen im Ökosystem des digitalen Journalismus. Da die Finanzierung digitaler journalistischer Inhalte heute stark von datenbasierten Geschäftsmodellen abhängt, nehmen die Autoren die Herausforderungen für bestehende Publisher-Geschäftsmodelle in den Fokus. Die Autoren stellen fest, dass Publisher infolge der Einschränkungen des webseitenübergreifenden Trackings zwar datenschutzfreundlichere Werbeformate entwickelt haben, die jedoch zu einer Angleichung von Werbung und journalistischem Inhalt führen.

Fairness und Governance

Die im dritten Teil des Bandes zusammengefassten Beiträge drehen sich um die Frage, wie das Zusammenspiel verschiedener Elemente einer künftigen Daten-Governance aussehen sollte, damit den Interessen unterschiedlicher Interessensträger in fairer Weise Rechnung getragen wird. Dabei stehen vor allem die zahlreichen neuen europäischen Datengesetze im Mittelpunkt.

Zertifizierung kann helfen, faire von weniger fairen Angeboten zu unterscheiden. In ihrem Beitrag befassen sich *Gerrit Hornung* und *Marcel Kohpeiß* (Universität Kassel) mit den Potenzialen und Erfolgsfaktoren der Datenschutzzertifizierung nach der Datenschutz-Grundverordnung. Sie betrachten die Zertifizierung insgesamt als ein Governance-Instrument, das dazu beitragen kann, das früher oft kritisierte Vollzugsdefizit zu beheben. Die Autoren stellen aber fest, dass noch viele Fragen offen sind, insbesondere im Hinblick auf spezialgesetzliche Anforderungen und wichtige Rechtsfragen wie die Übermittlung von Daten in Drittstaaten.

Maxi Nebel und *Paul Johannes* (Universität Kassel) untersuchen die sichere Authentifizierung natürlicher Personen als zentralen Bestandteil des eGovernment. Das Ziel besteht darin, als Nutzende online auf Dienste zugreifen zu können, ohne private Identifizierungsmethoden nutzen oder unnötigerweise personenbezogene Daten weitergeben zu müssen. Der Beitrag präsentiert die Reform der eIDAS-VO, gibt einen Überblick über den neuen Vertrauensdienst EUid und untersucht, ob die Identifizierungspflicht bei der Nutzung digitaler Dienste ausreichend mit den Bedürfnissen nach Anonymität im Internet vereinbart werden kann.

Marie-Louise Gächter (Datenschutzstelle Fürstentum Liechtenstein) beschäftigt sich mit der 2019 beim Weltwirtschaftsforum gestarteten Initiative zu einer internationalen Ordnung, die einen freien Datenfluss auf der Grundlage von gegenseitigem Vertrauen ermöglichen sollte. Die Suche nach dieser Vertrauensbasis gestaltet sich aber schwierig, da die unter-

schiedlichen Wertvorstellungen und Traditionen der Länder den Schutz personenbezogener Daten beeinflussen. Außerdem erhebt die europäische Datenschutz-Grundverordnung Anspruch auf Geltung auch außerhalb Europas. Gächter kommt zu dem Schluss, dass derzeit die Hindernisse überwiegen, und eine Vertrauensbasis für einen freien Datenfluss noch nicht realisierbar erscheint.

Der Beitrag von *Fabiola Böning* (Universität Kassel) und Kolleg:innen befasst sich mit der Informiertheit und Transparenz im Kontext digitaler Selbstvermessung. Mit Hilfe einer qualitativen Interviewstudie wurden verschiedene Personas identifiziert, die aus unterschiedlichen Gründen Selbstvermessung betreiben und verschiedene Privatsphäreeinstellungen haben. Trotz dieser Unterschiede besteht ein gemeinsames Bedürfnis nach umfassender Information und hoher Transparenz, während die Möglichkeit zur Intervention als weniger wichtig erachtet wird. Der Beitrag diskutiert die Gründe für diese Einschätzung insbesondere hinsichtlich der Transparenzvorgaben und den Informationspflichten der Datenschutz-Grundverordnung und präsentiert Ideen für einen Privacy-Assistenten als interaktives System zur personalisierten Informationsvermittlung und -übermittlung.

Der Beitrag von *Florian Müller* (Universität Kassel) untersucht die Bemühungen großer Social-Media-Plattformen um Vertrauenswürdigkeit. Dabei beschreibt er das Spannungsverhältnis zwischen den Geschäftspraktiken der Plattformen und den normativen Erwartungen nach Privatheit und vertrauenswürdigen Beziehungen. Dieses Spannungsverhältnis sieht er als Ausdruck von Veränderungsprozessen in der gesellschaftlichen Wahrnehmung und institutionellen Regulierung von Social-Media-Plattformen sowie der Art und Weise, wie sich diese Plattformen im Zusammenhang mit diesen Veränderungen positionieren.

Das Kapitel von *Hartmut Aden* (HWR Berlin) und Kolleg:innen zur Daten-Governance im Sicherheitsbereich benennt bestehende Schutzlücken bei der internationalen Zusammenarbeit von Sicherheitsbehörden und weist auf die Risiken für die Menschenrechte hin, die durch Überwachungstechnologien und KI-basierte Analysen entstehen können. Die Autor:innen zeigen auf, dass innerhalb der EU Prinzipien wie Fairness, Transparenz und Erklärbarkeit bei KI-Anwendungen unzureichend umgesetzt und außerhalb der EU noch weniger beachtet werden. Anhand des EncroChat-Falls verdeutlichen sie, wie die ausgeprägte Geheimhaltungskultur der Sicherheitsbehörden die Umsetzung rechtsstaatlicher Grundsätze erschwert.

Desinformation

Im vierten Teil des Bandes widmen sich zwei Beiträge dem speziellen Problem der Desinformation, das in unterschiedlichsten Formen und mit unterschiedlichsten Motiven in den letzten Jahren mehr oder weniger subtil die Selbstbestimmung der Bürger:innen untergräbt und damit auch die Fairness in der Gesellschaft gefährdet.

Juliane Stiller (Grenzenlos Digital e.V., Berlin) und Kolleginnen untersuchen Des- und Falschinformationen im Gesundheitsbereich, wo diese potenziell weitreichende Konsequenzen haben können. Insbesondere befassen sie sich mit Desinformation, die den Anschein von Wissenschaftlichkeit erweckt und damit das Vertrauen in Expert:innen und wissenschaftliche Gesundheitsinformationen ausnutzt. Ihre Untersuchung widmet sich den verschiedenen Formen und Verbreitungsmechanismen solcher Falschinformation und schlägt eine Systematik vor, die anschließend empirisch validiert werden soll.

Tahireh Panahi (Universität Kassel) und Kolleg:innen befassen sich mit der gerade in den aktuellen Krisenzeiten verstärkten Verbreitung von Desinformation über soziale Medien, inbesondere den weitgehend unmoderierten Kommunikationsdienst Telegram. Um gegen die Verbreitung falscher Informationen vorzugehen, hat die EU den Digital Services Act (DSA) erlassen, der Diensteanbietern risikobezogene Pflichten vorschreibt. Die Autor:innen erläutern, wie diese Pflichten mit Hilfe der Netzwerkanalyse erfüllt werden können. Diese erlaubt zwar nicht, Inhalte von Desinformation zu erkennen, hilft aber bei der Identifikation von Nachrichten, die von für Desinformation bekannten Akteur:innen ausgehen bzw. weiterverbreitet werden.

Technische Ansätze des Daten- und Identitätsmanagement

Im fünften und abschließenden Teil des Buches werden verschiedene Ansätze präsentiert, um ein effektives und faires Daten- und Identitätsmanagement zu realisieren. Diese Ansätze sollen sowohl die Rechte der Betroffenen technisch umsetzen als auch den Herausforderungen neuer Datentypen gerecht werden.

Sebastian Wilhelm (TH Deggendorf) und Kolleg:innen stellen in ihrem Kapitel ein zweiteiliges Framework eines Personal Information Management Systems vor, das das Recht auf Auskunft über personenbezogene Daten gemäß der Datenschutz-Grundverordnung technisch umsetzt. Das

System unterstützt sowohl Betroffene als auch Datenverarbeitende bei der Anforderung und Bearbeitung von Datenschutzselbstauskünften. Ein Tool ermöglicht Betroffenen automatisierte Anfragen und Interpretationen von Datenkopien. Ein weiteres Tool hilft den Datenhaltenden dabei, Datenschutzselbstauskünfte ganz oder teilweise automatisch zu beantworten. Das Framework zielt darauf ab, die informationelle Selbstbestimmung der Bürger:innen zu wahren, indem es die Anforderung von Selbstauskünften erleichtert und die Bearbeitung solcher Anfragen effizienter gestaltet.

Der Beitrag von *Gunnar Hempel* und *Jürgen Anke* (HTW Dresden) gibt einen Ausblick auf Privacy Management, das auf Self-Sovereign Identity (SSI) basiert. SSI-Wallets, die in diesem Zusammenhang verwendet werden, bieten Eigenschaften, die die Privatheit der Nutzenden besser schützen können als bisherige Ansätze und die Kontrolle der Nutzenden über ihre Daten erhöht. Dafür sind allerdings ein wertegeleiteter Umgang mit der Technologie und zusätzliche Werkzeuge notwendig. SSI-Wallets, so die Argumentation der Autoren, eröffnen mit Verfahren und Werkzeugen wie Selective Disclosure, Verifiable Presentations, Zero-Knowledge Proofs, nicht-korrelierbare Identifikatoren und Filterfunktionen eine disruptive Neugestaltung der Beziehung zwischen Nutzer:innen und Serviceanbietern.

Sebastian Hanisch (Technische Universität Dresden) und Kolleg:innen untersuchen in ihrem Beitrag die „Risiken und Anonymisierungsmöglichkeiten der Verhaltensbiometrie", die auf neuen Sensoren basiert. Diese Erfassung von Daten wie Körperbewegungen, Gesten, Augenbewegungen, Stimme, Herzschlägen und Gehirnaktivitäten ermöglicht Rückschlüsse auf persönliche Informationen wie Alter, Geschlecht, Gesundheitszustand und Persönlichkeit. Die Nutzenden haben Schwierigkeiten, zu erkennen, welche persönlichen Informationen aufgrund dieser Daten abgeleitet werden können. Sie stehen damit oft vor der Wahl, entweder einer Anwendung den vollständigen Zugriff auf einen bestimmten Sensor zu erlauben oder komplett auf die Anwendung zu verzichten. Die Autor:innen folgern deswegen, dass neue Privatsphäre-Einstellungen und Anonymisierungsverfahren erforderlich sind, um den Konflikt zwischen Datennutzung und Datenschutz zu lösen.

Teil I: Fairness und Schutz marginalisierter Gruppen

Gender, Labor, and Power in the History of Computing (Extended Abstract)

Mar Hicks

This paper situates the history of computing in relation to current, pressing, labor concerns in high technology fields. Specifically, it looks at historical examples that foreground categories of difference from the perceived norm in technological labor forces, in order to show continuities in who wields control over computing systems. As the U.S., U.K., and Europe enter an era that many journalists and tech critics have characterized as a "techlash"—a period of reduced optimism about technologies' ability to fix social problems, paired with the widespread realization that many technologies tend to exacerbate social, political, and economic inequalities—the history of computing, gender, and labor can provide some key context for how we arrived here.

Although the recent discourse on computing in wealthy nations often situated it as a neutral technology that would tend to lead to a net positive for society, this paper argues that the beginnings of computing in warfaring, with limited and highly gendered workforces, and the changing gender of those workforces as the field saw a rise in status, indicate that electronic computing has been, from its inception, not simply a tool for speeding up work or increasing efficiency but a tool for wielding power over others, both globally and domestically. In 1943 and 1944, as workers in the U.K. finished designing, constructing, and deploying the first Colossus computers for codebreaking at Bletchley Park, the intended use case of these early electronic computers was, in effect, cyberwarfare and information warfare. Women were targeted as the primary labor force for these early computers not simply due to the exigencies of war but because they were seen as the most appropriate workforce for work that was erroneously perceived to be deskilled, rote, and mindlessly technical.

Fast forward to the present day, when misinformation, disinformation, and surveillance threaten people's fundamental rights and the legitimacy and stability of many technologically advanced, nominally democratic nations. Narratives of computing that position these developments as surprising or discontinuous with the past tend to neglect not only the origins of

the field but also the interim period in which the most advanced computer technologies were used in peacetime to promote the goals of a Cold War geopolitical model. As technologies aligned with "hot" war (munitions, etc.) began to be matched and surpassed by technologies intended for information warfare, computers became ever more important as political tools, as well as instruments of soft power wielded over populations during periods of relative peace. During this period the labor pools targeted to work in the field of computing (from programming, to systems analysis, to computer operation) began to trend towards being composed primarily of men. This was not because women willingly left the field en masse, nor because they were judged technically incompetent. Rather, it was because women were no longer seen as a suitable workforce as computing became ever more aligned with wielding state and corporate power. Instead, they were shunted into other forms of work with less perceived power and responsibility.

How does this relate to today? The same issues of power, surveillance, and control that defined 20th century computing have continued to silently define 21st century computing, even as newer computing technologies have been marketed first and foremost as a consumer good and secondarily as a means of increasing efficiency in industry and government. Baked into many of the systems and products that are being marketed as indispensable for people's work and everyday lives are assumptions about corporate and state power born out of the 20th century conception of technology as a key pillar of the military industrial complex. Even when not explicitly geared to military applications, advances in computing afford greater control over populations, beginning with the labor forces required to sustain and expand the field. From the gig work economy to the voracious, and often dubiously legal, collection of online information to create datasets for AGI (Artificial General Intelligence) and LLMs (Large Language Models), computing's leading edges have continued to be more extractive than generative, requiring ever more labor to achieve their goals even as they position these advances as labor-saving. In truth, these advances are labor intensive and more committed to controlling current and potential future workers than eliminating drudgery or creating new socioeconomic models that would be more egalitarian or broadly economically uplifting.

Instead of meaningfully reckoning with this history, the most profitable companies in the field have begun eating their own, firing and shaming workers who have acted as internal critics or attempted to be ethical and conscientious practitioners, while at the same time largely ignoring external

criticism. The tech workers speaking out about labor rights, the harms of scaling up unsustainable systems, and the growing crises of online manipulation and disinformation in the global political landscape have found themselves fundamentally at odds with the larger direction of their field. Even as diversity initiatives purporting to value difference have begun to undo the homogeneity of high-tech workforces, these nominally more diverse workforces are subject to the same forces that have long attempted to foster a narrow conformity under the guise of technological progress, and to disallow that diversity from meaningfully reshaping the field.

In the present, as in the past, computing presents itself as a site for societal progress and advancement, while cementing its status as a set of tools usually wielded by the most powerful against the less powerful. Those who wield the most influence in the field increasingly find themselves in a position to reshape society in line with their goals and ideals, while continuously rewriting the history of computing to erase evidence of dissent, resistance, or possible alternatives.

Further readings

Hicks, Mar (2018): *Programmed Inequality: How Britain Discarded Women Technologists and Lost Its Edge in Computing*. Cambridge, Mass. and London: MIT Press.

Mullaney, Thomas S., Benjamin Peters, Mar Hicks and Kavita Philip (Eds.) (2021): *Your computer is on fire*. Cambridge, Mass. and London: MIT Press.

Daten-Fairness als Daten-Gerechtigkeit by Design

Felix Bieker und Marit Hansen

Zusammenfassung

Dieser Beitrag nimmt die aktuelle Debatte um Chatbots zum Anlass die Risiken algorithmischer Systeme für betroffene Personen und insbesondere Angehörige marginalisierter Gruppen zu untersuchen. Letztere sind vom Einsatz neuer Technik meist überproportional negativ betroffen, obwohl die gesellschaftlichen Machtstrukturen, die Rassismus, Sexismus und Transphobie den Weg bereiten, längst umfassend untersucht sind. Wir analysieren Regelungen des Datenschutzrechts, die Strukturen von Informationsmacht adressieren, blicken auf relevante Regelungen der neuen EU-Datengesetze, ziehen Schlussfolgerungen aus dem Diskurs zum Antidiskriminierungsrecht und erweitern durch den Rückgriff auf das Konzept der Intersektionalität die Perspektive des Rechts. Auf Grundlage von Ansätzen zu *Value Sensitive Design*, *Data Justice* und *Design Justice* zeigen wir mit Bezug insbesondere auf die relevanten datenschutzrechtlichen Regelungen, wie Daten-Gerechtigkeit „by Design" durch Prozesse gewährleistet werden kann.

1. Einführung

Die Bereitstellung von OpenAIs Chatbot ChatGPT zur allgemeinen Nutzung ab Ende 2022 befeuerte den über längere Zeit beständig aufgebauten Hype um sogenannte Künstliche Intelligenz (KI). In der Folge stellten auch die großen Plattformanbieter ihre eigenen Chatbots und verwandte Anwendungen vor. Die mediale und gesellschaftliche Aufmerksamkeit richtete sich dabei zunächst auf die zukünftigen Potenziale und möglichen Anwendungsfelder dieser Technik. Doch zuletzt mehrten sich Berichte über Fehlfunktionen und Ausfälle von Chatbots verschiedener Hersteller. Von ChatGPT, das rassistische Rap-Texte und Computer-Programme ge-

nerierte[1], über Googles Bard, das bei seiner Vorstellung im Brustton der Überzeugung falsche Antworten gab[2], zu einer Test-Version von Microsofts Suchmaschine Bing als Chatbot, die Nutzende davon überzeugen wollte, dass es noch das Jahr 2022 sei[3] oder auch, dass sie ihre Frau verlassen sollten, um eine Beziehung mit dem Chatbot zu führen[4]. Diese Probleme sind keineswegs neu, sie zeigten sich z. B. in ähnlicher Form bereits bei den Bildgeneratoren, die zuvor vorgestellt wurden.[5]

Mit den auf *Large Language Models* basierenden öffentlich zugänglichen Chatbots ist der bisherige Höhepunkt einer Entwicklung erreicht, in der Technik als geheimnisvolle Black Box betrachtet wird, in die eine Vielzahl ungefilterter und auch personenbezogener[6] Daten, oft aus dem Internet, hineingegeben werden und die auf für die Nutzenden meist nicht nachvollziehbare Weise Outputs erzeugt. Wie genau diese Modelle arbeiten, wird dabei nicht dokumentiert oder, soweit dies doch geschieht, nicht transparent offengelegt. Die Modelle werden wahlweise als „magische Instrumente"[7] oder „menschenähnliche Intelligenzen"[8] beschrieben, was in beiden Fällen nicht zutrifft.[9] Das Vorgehen der Anbieter:innen erinnert bei genauerer Betrachtung eher an einen Wursthersteller, der ein wundersames neues Produkt bewirbt, jedoch nicht offenlegt, welche Zutaten darin verarbeitet wurden, ob diese aus zuverlässigen Quellen stammen und auf welche Weise die Herstellung vonstatten geht.

Mit dieser Entwicklung entfernen sich die technische Realität und die verfügbaren Angebote immer weiter von der gesetzlich normierten Vorstellung, dass Technik und die damit einhergehende Datenverarbeitung kontrolliert eingesetzt werden sollen, damit ihre Auswirkungen untersucht und gesteuert werden können. Diese Entwicklung wird durch die schiere Infor-

1 *Perrigo*, Time v. 5. Dez. 2022; *Biddle*, The Intercept v. 8. Dez. 2022.
2 *Schräer*, Heise Online v. 9. Feb. 2023.
3 https://www.reddit.com/r/bing/comments/110eagl/the_customer_service_of_the_new_bing_chat_is/.
4 *Roose*, New York Times v. 16. Feb. 2023.
5 Vgl. z.B. *Johnson*, Wired v. 5. Mai 2022; *Luccioni u.a.*, Stable Bias: Analyzing Societal Representations in Diffusion Models.
6 *Gal*, The Conversation v. 8. Feb. 2023.
7 *Elish*, Don't Call AI "Magic".
8 *Schwartz*, The Guardian v. 25. Jul. 2018.
9 *Bender*, The Guardian v. 14 Jun. 2022. Vgl, auch schon Clarke, Profiles of the Future: An Inquiry into the Limits of the Possible, 1973: „Any sufficiently advanced technology is indistinguishable from magic".

mationsmacht,[10] die Anbieter:innen durch diese Datenpraktiken erlangen können, begünstigt.

Nach unserem Verständnis bedarf es einer umfassenden Betrachtung der Verarbeitung von Daten und ihrer unerwünschten Folgen, die sich nicht nur auf das, was klassischerweise als Datenschutzrecht betrachtet wird, beschränken darf. Vielmehr ist der Blick holistisch und interdisziplinär auf die Informationsmacht und sämtliche unerwünschten Folgen von Datenpraktiken zu lenken – es wäre naiv anzunehmen, dass allein die Datenschutz-Grundverordnung (DSGVO) und ihre Durchsetzung über die Datenschutzaufsicht all diese Probleme lösen könnten. Gleichzeitig ist die DSGVO der rechtliche Ausgangspunkt für jede Verarbeitung personenbezogener Daten. Über das Konzept der Risiken für die Rechte und Freiheiten natürlicher Personen[11] und das Ziel nach Art. 1 Abs. 2 DSGVO, die Grundrechte natürlicher Personen zu schützen, ist sie für viele weitere Gebiete der Technikregulierung anschlussfähig. So greift etwa der aktuelle EU-Entwurf zur Verordnung über Künstliche Intelligenz (KI-VO-Entwurf)[12] Risiken u.a. auch für die Grundrechte auf.[13]

Die Jahreskonferenz 2022 des *Forum Privatheit* wählte mit dem Begriff der Daten-Fairness einen bewusst weiten Begriff, der viele Interpretationsmöglichkeiten eröffnet. Fragen nach Fairness verhandeln stets Formen von Gerechtigkeit, die wir in diesem Beitrag analysieren, in dem wir unser Verständnis von Daten-Fairness als Daten-Gerechtigkeit darlegen.

Im Folgenden erläutern wir zunächst die bekannten Probleme algorithmischer Systeme, die schon vor einiger Zeit dadurch aufgefallen sind, dass sie rassistische, sexistische und transphobe Inhalte generieren (Abschn. 2) und identifizieren die Form des Diskurses, der in zweifacher Hinsicht von Individualisierung geprägt ist, als hinderlich für das Erreichen von Daten-Gerechtigkeit: Zum einen wird der Blick auf einzelne Schuldige gerichtet, zum anderen von Einzelnen erwartet, diese machtvolle Anbieter:innen mit Hilfe ihrer Individualrechte zur Rechenschaft zu ziehen (Abschn. 3). In

10 Rouvroy/Poullet, in: Gutwirth u.a. (Hrsg.), Reinventing Data Protection?, 2009, 45 (69).

11 *Bieker*, DuD 2018, (27-31).

12 Der aktuelle Entwurf des Rates mit neuen Regelungen zu „General Purpose"-Anwendungen ist abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf. Für einen Überblick über den KI-VO-Entwurf, vgl. *Guijarro Santos*, ZfDR 2023, 23.

13 Vgl. ErwGr. 32, 42, 43, 47 72a, 79a, Art. 6 Abs. 3, Art. 7 Abs. 1 Buchst. b, Abs. 2, Abs. 3 Buchst. a, Art. 9 Abs. 2 Buchst. a, Art. 13 Abs. 3 Buchst. b (iii), Art. 14 Abs. 2, Art. 36 Abs. 6 Buchst. e, Abs. 7 Buchst. a, Abs. 8 Buchst. a, Art. 43 Abs. 6, Art. 65 Abs. 1, Abs. 2, Art. 67 Abs. 1 u. Annex IV Nr. 3.

Abschn. 4 blicken wir auf die rechtlichen Regelungen, die sich mit Informationsmacht und strukturellen Aspekten von Datenverarbeitung befassen, insbesondere das Datenschutz- und Informationsfreiheitsrecht, und zeigen Bezüge zum Antidiskriminierungsrecht auf. Unter Rückgriff auf die im bestehenden Recht enthaltenen systemischen Regelungen, ergänzt um die Ansätze von *Value Sensitive Design*, *Data Justice* und *Design Justice* zeigen wir, inwieweit sich Daten-Gerechtigkeit im bestehenden Recht finden lässt (Abschn. 5). Schließlich unterbreiten wir in Abschn. 6 unter Rückgriff auf die relevanten rechtlichen Regelungen und vorherigen Erkenntnisse Vorschläge für Prozesse, mit denen Daten-Gerechtigkeit in der Praxis erreicht werden kann. Abschn. 7 gibt einen Überblick über die Erkenntnisse und endet mit einem Ausblick.

2. Neue Technik, alte Probleme

Die oben aufgezeigten, anekdotischen Berichte der Presse offenbaren grundlegende Beschränkungen und systemische Probleme dieser Technik. Allerdings wird der weitere Schritt zu einer Betrachtung dieser strukturellen Ebene meist nicht vollzogen, sondern es bleibt beim Aufzeigen einer Vielzahl von „Einzelfällen". Dies macht es unkritischen Befürwortern leicht, Risiken im Vergleich zu – rein hypothetischen – Vorteilen und den Potenzialen des Einsatzes der Technik kleinzureden.[14]

Dabei würde eine tiefergehende Analyse wenig Überraschendes zutage fördern. Sie würde zeigen, dass die seit Jahren bestehenden Probleme von Technik als Black Box, die von systemischem Rassismus, Sexismus oder Transphobie durchzogen ist und die vor dem teilweise überstürzten, teilweise (bewusst) unfertigen Verbreiten nicht ausreichend getestet und dokumentiert wurde, im Fall dieser speziellen algorithmischen Systeme in besonderem Maße bestehen. Diese und weitere Probleme waren schon vor der Veröffentlichung der Chatbots absehbar.[15] Die Beseitigung dieser sich, wie Simone Brown[16] und Mar Hicks[17] aufgezeigt haben, beständig wiederholenden gesellschaftlichen Probleme und machtvollen Strukturen in

14 *Altman*, Planning for AGI and Beyond.
15 *Bender u.a.*, in: FAccT '21, 2021.
16 *Browne*, Dark Matters, 2015.
17 *Hicks*, in diesem Band; vgl. bereits *Hicks*, in: Mullaney u.a. (Hrsg.), Your Computer is on Fire, 2021, 11 (13).

verschiedenen Gestalten wird von den Verantwortlichen aufgeschoben und an betroffene Personen und Gruppen ausgelagert, damit die Unternehmen vom Boom der Anwendungen profitieren und ihre Monetarisierungsstrategien umsetzen können. Sie spielen die Informationsmacht[18] aus, die sich aus der eingesetzten Technologie, der Marktstellung ihrer Unternehmen, einer fehlenden oder mangelhaften Regulierung und den aus der massenhaften Verarbeitung von Daten gewonnenen Erkenntnissen ergibt.

Die Versprechen der Anbieter:innen über die Effizienz algorithmischer Systeme orientieren sich dabei an fragwürdigen Benchmarks[19], und in der praktischen Umsetzung wird teilweise nicht einmal danach gefragt, ob eine Anwendung überhaupt die gewünschte Funktionalität bietet.[20] Dies hängt auch damit zusammen, dass die Zwecke der Datenverarbeitung durch die Anwendung nicht im Vornherein klar festgelegt sind. Diese „General Purpose"-Anwendungen werden vielmehr frei zugänglich gemacht, sodass sich gar nicht absehen lässt, wofür die für ihre Bereitstellung und die im Rahmen ihrer Nutzung gesammelten Daten eingesetzt werden.

Während im EU-Gesetzgebungsprozess zur KI-Verordnung noch an Details gefeilt wird, setzt die Realität schon Fakten – und dabei ist noch nicht einmal die grundlegende Entscheidung getroffen, wie diese algorithmischen Systeme nach dem Willen des Gesetzgebers in das im KI-VO-Entwurf vorgesehene System von Risikokategorien eingestuft werden sollen.[21]

In den USA hat die Federal Trade Commission inzwischen angekündigt, Werbeversprechen der Anbieter kritisch in Hinblick darauf zu überprüfen, ob die Fähigkeiten der algorithmischen Systeme übertrieben dargestellt werden, den Anbietern die Risiken des Einsatzes bekannt sind und ob in einem bestimmten Produkt überhaupt ein solches System enthalten ist.[22] Während insbesondere der letzte Punkt überraschend wirken mag, gab es bereits verschiedene Fälle, in denen Aufgaben, die vorgeblich durch algorithmische Systeme automatisiert wurden, tatsächlich von menschlichen Crowdworkern zu Niedriglöhnen erledigt wurden.[23] Allerdings gilt auch

18 *Rouvroy/Poullet*, in: Gutwirth u.a. (Hrsg.), Reinventing Data Protection?, 2009, 45 (69).

19 *Raji u.a.*, in: Proceedings of the Neural Information Processing Systems Track on Datasets and Benchmarks 1 (NeurIPS Datasets and Benchmarks 2021), 2021.

20 *Raji u.a.*, in: FAccT '22, 2022.

21 *Volpicelli*, Politico v. 3. März. 2023; *Heidelberger/Diakopoulos*, Internet Policy Review 2023.

22 *Atleson*, Keep your AI claims in check.

23 *Roberts*, in: Mullaney u.a. (Hrsg.), Your Computer is on Fire.

beim tatsächlichen Einsatz algorithmischer Systeme, dass die zugrundeliegenden Trainingsdaten von Menschen als unsichtbare Arbeiter:innen – und oft unter besonders schlechten Arbeitsbedingungen[24] – von gewaltvollen, rassistischen, sexistischen, transphoben oder anderen unerwünschten Inhalten bereinigt werden sollen.[25] All diese Probleme, die von solchen Datenpraktiken ausgehen und Probleme in der Umsetzung des Datenschutzrechts offenbaren, gleichzeitig aber auch eindeutig über die Materie der herkömmlichen Datenschutzkonzepte hinausgehen, zeigen sich in der aktuellen Entwicklung von Chatbots, Bildgeneratoren[26] und ähnlichen Anwendungen wie unter einem Brennglas.

Die Bezüge zwischen diesen Datenpraktiken und den bestehenden, problematischen Machtstrukturen, insbesondere im Hinblick auf algorithmische Systeme, sind bereits umfassend wissenschaftlich aufgearbeitet worden. Dies betraf etwa Fälle rassistischer, sexistischer und transphober Diskriminierung: Joy Buolamwini und Timnit Gebru haben schon 2018 nachgewiesen, dass die Gesichtserkennungsfunktionalität algorithmischer Systeme die Gesichter Schwarzer Menschen schlechter erkennt als die weißer Personen und dass die Erkennungsrate bei Schwarzen[27] Frauen besonders schlecht ist.[28] Ein von der Stadt Rotterdam eingesetztes algorithmisches System zur Bestimmung des Missbrauchspotenzials von Sozialhilfeempfänger:innen, bewertete das Risiko bei Frauen und People of Color automatisch höher als bei weißen Männern.[29] Ebenso wie bei Schwarzen

24 Vgl. dazu auch den Entwurf einer Richtlinie zur Plattformarbeit der Kommission (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52021PC0762) und die Position des Rates (https://data.consilium.europa.eu/doc/document/ST-10107-2023-INIT/de/pdf) sowie *Veale/Silberman/Binns*, European Labour Law Journal 2023.

25 Ebd.; *Jones*, Work without the Worker, Labour in the Age of Platform Capitalism, 2021; *Gray/Suri*, Ghost Work, 2019.

26 *Luccioni u.a.*, Stable Bias: Analyzing Societal Representations in Diffusion Models.

27 Wir schreiben das Wort Schwarz groß, da es sich dabei nicht um die tatsächliche Farbe der Haut oder eine angebliche biologische „Rasse" handelt, sondern „um eine politische Selbstbezeichnung von Menschen in einer bestimmten gesellschaftlichen Position, die mit Rassismuserfahrungen verbunden ist", https://www.journalist.de/startseite/detail/article/das-diversity-lexikon; vgl. auch: *Hasters*, Was weiße Menschen über Rassismus nicht hören wollen aber wissen sollten, 2020, S. 29 f.; aus juristischer Sicht: *Liebscher,* Rasse im Recht – Recht gegen Rassismus, 2021.

28 *Buolamwini/Gebru*, in: Proceedings of Machine Learning Research 81.

29 *Constantaras u.a.*, Wired v. 6. Mar. 2023, vgl. schon *Eubanks*, Harper's Magazine v. Jan. 2018.

Menschen[30] gibt es auch bei trans* Menschen eine lange Geschichte der Nutzung von Datenverarbeitung zu Überwachungszwecken[31]. Wie Mar Hicks und Simone Browne darlegen, sind algorithmischer Bias gegen trans* Frauen und Schwarze Menschen also keine neuartigen Phänomene.[32]

In diesen Aufarbeitungen wird auch deutlich, dass die entsprechenden Personen meist aufgrund mehrerer Kategorisierungen – insbesondere Geschlecht, Rassifizierung und Geschlechtsidentität, aber auch Klasse oder Behinderung[33] – von Diskriminierung betroffen sind. Dieses Phänomen wird vom Konzept der Intersektionalität erfasst, nach dem diese Kategorisierungen sich nicht gegenseitig ausschließen, sondern aufeinander aufbauen und zusammenwirken.[34] Die bereits aufgezeigten Beispiele verdeutlichen, dass die Probleme der aktuellen Datenpraktiken sich nicht nur in einer Dimension von Unterdrückung auswirken, sondern eben etwa Schwarze Frauen oder trans* Frauen, die in mehrere Kategorisierungen fallen, besonders von Diskriminierung betroffen sind. Um die strukturellen Probleme der aktuellen Datenpraktiken anzugehen und nicht nur immer wieder über vermeintliche Einzelfälle zu reden, ist es daher an der Zeit, diese Erkenntnisse auch in der rechtlichen Praxis zu berücksichtigen.

3. Individualisierung von Problemen

Für den notwendigen Schritt in die Praxis ist häufig die Form des Diskurses hinderlich: So findet oft eine Verengung auf einzelne „Bad Actors" oder „Bad Tech" statt, als würde das Problem sich durch das Ansetzen an einer Stelle lösen lassen, wie Anna Lauren Hoffmann in ihrer Kritik des Begriffs der Fairness im Antidiskriminierungsrecht herausgearbeitet hat.[35]

Dies lässt sich auch im Datenschutzdiskurs, zum Beispiel bei der Fokussierung auf einzelne Unternehmen, erkennen. Es wird über konkrete Anbieter berichtet und im selben Zug das weitere Feld einer gesamten Art von

30 Vgl. etwa *Gilliard/Culik*, Digital Redlining, Access, and Privacy.
31 *Hicks*, IEEE Annals of the History of Computing 2019.
32 *Hicks*, in diesem Band; *Hicks*, in: Mullaney u.a. (Hrsg.), Your Computer is on Fire, 2021, 11 (13); Browne, Dark Matters, 2015.
33 Es ist in diesem Kontext bemerkenswert, dass ein kolumbianischer Richter ausgerechnet in einem Fall zur Krankenversicherung eines autistischen Kindes auf ChatGPT zurückgriff, vgl. *Taylor*, The Guardian v. 3. Feb. 2023.
34 *Hill Collins/Bilge*, Intersectionality, 2020, S. 2.
35 *Hoffmann*, Information, Communication & Society 2019, 900 (903-905).

Anwendungen ausgeblendet. Das Problem dieses Fokus auf „Bad Actors" ist, dass es den Blick primär auf die schuldigen Individuen lenkt, die eine konsentierte gesellschaftliche Regel brechen und deren unangemessenes Verhalten zu beseitigen sei.[36] Dies geht zulasten der Problematisierung sozialer und systemischer Ungerechtigkeiten, da in der rechtlichen Debatte sodann nur über Schuld und Verursachung Einzelner diskutiert wird.

Dieses problematische Framing beschränkt sich nicht allein auf menschliche Verursacher: Genauso werden teilweise unbeabsichtigte Biases angeführt, die sich in Systeme „einschleichen". So ist zu beobachten, dass sich Anbieter für entstandene Schäden, zum Beispiel durch eine Gesichtserkennungssoftware, die Schwarze Menschen als Gorillas kennzeichnet, entschuldigen und Besserung geloben, obwohl der Eintritt der Schäden absehbar war und vermutlich bewusst in Kauf genommen wurde.[37] Inzwischen gibt es sogar Anbieter, die sich im Vornherein für den Output des von ihnen eingesetzten Chatbots entschuldigen.[38] Ob – und wenn ja, welche – Maßnahmen zum Vermeiden einer unerwünschten Funktionalität getroffen wurden und warum man sich trotz offensichtlich mangelnder Beherrschbarkeit des selbst produzierten algorithmischen Systems für eine Bereitstellung des Angebots entschieden hat, wird in der Regel nicht thematisiert.

Teilweise wird vorgeschlagen, das oft (fast) ausschließlich weiß und männlich besetzte Entwicklungsteam diverser zu besetzen.[39] Allerdings darf als Abhilfemaßnahme nicht nur die Beseitigung weißer Flecken innerhalb des Entwicklungsteams gefordert werden, da dies Systemfehler auf ein individuelles Problem seiner imperfekten menschlichen Gestalter:innen reduziert.[40] So können pauschale Forderungen nach „mehr Diversität" benutzt werden, um die zugrundeliegenden strukturellen Probleme zu überdecken.[41] Hoffmann fordert stattdessen, der Mentalität, dass man nur eine einzelne Quelle von Problemen beseitigen müsse, entgegenzuwirken, damit die dahinter liegenden systemischen Ungerechtigkeiten adressiert werden können.[42] Unter diesen Voraussetzungen könnten auch die relevanten Akteure identifiziert werden, damit die Technologiefirmen sich nicht

36 *Freeman*, Minnesota Law Review 1978, 1049 (1053-1054).
37 *Mac*, New York Times v. 3. Sep. 2021.
38 *Shanklin*, Engadget v. 27. Feb. 2023.
39 *Hoffmann*, Information, Communication & Society 2019, 900 (904).
40 *Ebd.*
41 *Theilen u.a.*, Internet Policy Review 2021.
42 *Hoffmann*, Information, Communication & Society 2019, 900 (904-905).

kollektiv durch Verweise auf unbeabsichtigte, dem Menschen inhärente Biases der Verantwortung entziehen können. Schließlich verstellt die Frage nach Biases auch den Blick auf ein grundlegenderes Problem: die Frage, ob eine bestimmte Technologie überhaupt eingesetzt werden sollte.[43] Diese Frage fokussiert auf die Risiken und strukturellen Probleme des Einsatzes bestimmter Technik, auf die wir in Abschn. 6 eingehen.

Neben dieser Individualisierung der Quelle von Problemen - bei der das Recht zu einer Verengung des Blicks führen kann und so die weiteren Folgen nicht ausreichend berücksichtigt werden - wird auch die Umsetzung des geltenden Rechts individualisiert, indem die Erwartung formuliert wird, dass betroffene Personen mit Hilfe der datenschutzrechtlichen Betroffenenrechte die Datenpraktiken global agierender Plattformen aufbrechen.[44]

Zwar sind die Betroffenenrechte und weitere Regelungen des Individualdatenschutzes ein wichtiger Teil des Datenschutzrechts[45], dieses enthält jedoch auch zahlreiche Regelungen zum Systemdatenschutz[46], wie wir sie im folgenden Abschnitt vorstellen. Im Angesicht der strukturellen Natur der Ursachen versprechen solch systemische Ansätze, auch weil damit verbundene by-Design-Ansätze bereits vor der Verarbeitung ansetzen, größeren Erfolg. Dass einzelne Organisationen auch über die individuellen Rechte des Datenschutzrechts strukturelle Probleme von Datenpraktiken aufzeigen und in Teilen sogar weitreichende Folgen auslösen können[47], steht dieser Schlussfolgerung nicht entgegen. Vielmehr zeigen der Grad der erforderlichen Organisation und die erheblichen Ressourcen[48], die für solche Formen der Rechtsverfolgung notwendig sind, wie unrealistisch es ist, dass eine einzelne, bereits von den negativen Auswirkungen einer Datenverarbeitung betroffene Person diesen Strukturen begegnen könnte.

Zudem können die Betroffenenrechte erst geltend gemacht werden, wenn die Datenverarbeitung bereits erfolgt. In einem solchen Fall, sind die Rechte der betroffenen Personen jedoch bereits verletzt. Eine Verkürzung

43 *Powles/Nissenbaum*, Medium v. 7. Dez. 2018.

44 Vgl. auch *Matzner u.a.,* in: Gutwirth u.a. (Hrsg.): Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection. 2016, S. 277-305.

45 Vgl. *Kaminski*, Notre Dame Law Review Reflection 2022, 385.

46 *Bieker*, The Right to Data Protection 2022 (186 f.).

47 EuGH, Rs. C-362/14, Urteil v. 6. Okt. 2015, ECLI:EU:C:2015:650 – Schrems I; EuGH, Rs. C-311/18, Urteil v. 16. Jul. 2020, ECLI:EU:C:2020:559 – Schrems II.

48 noyb, Annual Report 2021, S. 20. URL: https://noyb.eu/sites/default/files/2022-07/ANNUAL%20REPORT%202021%2014072022%20interactive.pdf.

des Datenschutzrechts auf die ex-post-Durchsetzungsbemühungen einzelner betroffener Personen oder, im Wege der Verbandsklage[49], auch von Einzelnen, die sich von einer Organisation vertreten lassen, dient also nicht deren „Empowerment", sondern liefert diese der Informationsmacht der großen Plattformen aus.

4. Bestehende gesetzliche Regelungen

Mit ihrer Datenverarbeitung schaffen die Anbieter einseitig Risiken, die sich nicht nur auf die betroffenen Menschen und einzelne Gruppen, sondern auch auf die gesamte Gesellschaft auswirken können.[50] Dem entgegenzutreten, ist auf individueller Ebene meist schon unmöglich, da das Individuum, dessen Daten gesammelt wurden, gerade nicht in der Lage ist, diese ohne Weiteres „zurückzuerlangen". Hier setzen die gesetzlichen Anforderungen an die Datenverarbeitung an: Unmittelbar adressiert das Datenschutzrecht die aufgeworfene Machtfrage[51] und setzt neben dem Schutz von Individuen auch bei den Strukturen von Datenverarbeitung und Gesellschaft an.[52]

Dafür enthält die DSGVO etwa einen eigenen Grundsatz der Fairness[53], der Rechtmäßigkeit und Transparenz (Art. 5 Abs. 1 Buchst. a DSGVO). Nach dem Grundsatz der Zweckbindung, dürfen Daten nur erhoben werden, um ein bestimmtes Ziel zu erreichen oder eine bestimmte Funktion[54] zu erfüllen (Art. 5 Abs. 1 Buchst. b DSGVO). Weiterhin müssen die Datenverarbeitenden im Rahmen ihrer Rechenschaftspflicht nachweisen können, dass sie die datenschutzrechtlichen Regelungen einhalten (Art. 5 Abs. 2 DSGVO). Zudem müssen sie als Verantwortliche die Risiken für Grundrechte[55] schon vor dem Beginn der Verarbeitung (Art. 25 DSGVO) – ggf.

49 Vgl. auch *Bieker*, The Right to Data Protectionm 2022 (190-192).

50 *Steinmüller u.a.*, Grundfragen des Datenschutzes, 1971, BT-Drs. VI/3826 Anlage 1, 5 (36, 40, 82 f.).

51 *Theilen* u.a., Internet Policy Review 2021; *Rouvroy/Poullet,* in: Gutwirth u.a. (Hrsg.), Reinventing Data Protection?, 2009, 45 (69).

52 *Bieker*, The Right to Data Protection, 2022 (186-193).

53 In der deutschen Sprachfassung mit „Treu und Glauben" unglücklich übersetzt.

54 Grundlegend zur Funktionalität algorithmischer Systeme vgl. *Raji u.a.*, in: FAccT '22, 2022.

55 Der KI-VO-Entwurf sieht in Art. 11 Abs. 1 eine technische Dokumentation vor, in der Anbieter:innen nach Annex IV Nr. 3 u.a. Informationen zu den vorhersehbaren unbeabsichtigten Folgen und Risikoquellen bezüglich der Grundrechte und Diskri-

im Rahmen einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) – bewerten und entsprechende Maßnahmen ergreifen, um ein den Risiken angemessenes Schutzniveau zu gewährleisten (Art. 25 und Art. 32 DSGVO). Dabei muss ein Perspektivwechsel erfolgen, denn die Regelungen dienen, anders als etwa die IT-Sicherheit, gerade nicht den eigenen Interessen des Verantwortlichen, sondern der Personen, denen aufgrund der Verarbeitung Schäden drohen.[56]

Neben dem Datenschutzrecht, das für personenbezogene Daten Anwendung findet, steht das Informationsfreiheitrecht, das ebenfalls dazu dient, Informationsmacht einzuhegen. Die Informationsfreiheit strebt eine Machtbegrenzung durch Herstellung von Transparenz über staatliches Handeln an, ist jedoch in den meisten Anwendungsfällen, insbesondere im Hinblick auf private Anbieter algorithmischer Systeme, nur auf staatliche Akteure anwendbar. Während das Informationsfreiheitsrecht als individuelles Antragsrecht von Personen ausgestaltet ist und hier die informationspflichtigen Stellen bei ihnen vorhandene Daten herausgeben müssen, soweit sie nicht durch gesetzlich vorgegebene private oder öffentliche Interessen daran gehindert sind, sind in einigen Bundesländern Transparenzportale oder Open-Data-Portale aufgebaut worden, die ein proaktives Veröffentlichen vorsehen. Ebenso wie beim Datenschutz „by Design" empfiehlt sich ein planvolles Vorgehen für Informationsfreiheit „by Design", um ohne großen Aufwand die angeforderten Informationen zusammenzustellen und rechtssicher zu beurteilen, welche Informationen in welcher Form herauszugeben sind.

Im Fall von Ausschlussgründen ist es häufig möglich, die Informationen mit geeigneten Schwärzungen bereitzustellen – auch hierbei kann eine entsprechende technische und organisatorische Gestaltung der Prozesse und der Aktenführung helfen.[57] Es lassen sich zwar geeignete Lösungen finden, um die Datenverarbeitenden sowohl im Datenschutz als auch in der Informationsfreiheit zu unterstützen.[58] Doch die heutigen E-Aktensysteme, Transparenzportale oder E-Government-Anwendungen, für deren Hersteller und Betreiber die Anforderung der Umsetzung des Informations-

---

minierung bereitstellen müssen. Ebenso wie die Untersuchung möglicher Biases in den Trainingsdaten nach Art. 10 Abs. 2 Buchst. f ist dies nur für Hochrisikosysteme vorgesehen.

56 *Friedewald u.a.,* White Paper Datenschutz-Folgenabschätzung, 2017 (31).

57 *Hansen/Krasemann* 2022, S. 35 ff.

58 *Hansen/Bieker/Bremert* 2022, S. 287 f.

zugangrechts unter Wahrung der gesetzlich vorgesehenen privaten und öffentlichen Interessen jedenfalls nicht überraschend sein sollte, sind in dieser Hinsicht heutzutage zumindest ausbaufähig.[59]

Neben diesem Datenschutzrecht im engeren Sinne behandeln noch weitere Rechtsnormen die aus der Datenverarbeitung entstehende Informationsmacht. Insbesondere zum Antidiskriminierungsrecht bestehen zahlreiche Bezüge.[60] Dies zeigt sich auch in den Verweisen auf Antidiskriminierungsvorschriften in der DSGVO selbst. Als einer der möglichen Schäden für die Rechte und Freiheiten natürlicher Personen, die der besondere, auf Grundrechtsrisiken abstellende Ansatz der DSGVO verhindern soll, nennen ErwGr. 75 und 85 die Diskriminierung der betroffenen Personen. ErwGr. 71 verweist auf besondere Schutzmaßnahmen, die sicherstellen sollen, dass die besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO nicht in einer Weise verarbeitet werden, die diskriminierend ist. Insofern umfasst der Verweis auf den Schutz der Grundrechte natürlicher Personen in Art. 1 Abs. 2 DSGVO selbstverständlich auch das Grundrecht auf Nichtdiskriminierung gemäß Art. 21 EU-Grundrechte-Charta.[61]

Die Verbindungen zwischen Datenschutz- und Antidiskriminierungsrecht sind jedoch erst in Ansätzen untersucht,[62] obwohl sich die bestehenden gesellschaftlichen Probleme wie Sexismus, Rassismus oder Transphobie auch – und wie bereits aufgezeigt in verstärktem Maße – bei den problematischen Datenpraktiken, wie dem Einsatz von Chatbots, niederschlagen. Im Antidiskriminierungsrecht ist das Problem intersektionaler Diskriminierungen ein bekanntes Phänomen.[63]

Allerdings ist dieses Problem auch dort noch nicht ausgeräumt: So stellen die verschiedenen, gesetzlich geschützten Kategorisierungen eine Vereinfachung dar, die sich dem Problem der Intersektionalität stellen

59 Ansätze der schleswig-holsteinischen Landesverwaltung siehe *Thomsen,* Sommerakademie, 2022. Bedarf zu einer verbesserten „By-Design"-Umsetzung besteht auch in Bezug auf Archive, siehe *Friedewald u.a.,* Access to Archives: Implementation of Recommendation No. R(2000)13 on a European policy on access to archives, 2023 I.E.

60 Im Sinne von Steinmüller u.a. lässt sich der Teil des Anti-Diskriminierungsrechts, der dazu dient, unerwünschte Auswirkungen von Datenverarbeitung zu adressieren, auch als Datenschutzrecht im weiteren Sinne verstehen, *Steinmüller u.a.*, Grundfragen des Datenschutzes, 1971, BT-Drs. VI/3826 Anlage 1, 5 (44); vgl. dazu *Bieker*, Right to Data Protection 2022 (189-190, 195-199).

61 Vgl. z.B. *Draude/Hornung/Klumbytė*, in: Hepp u.a. (Hrsg.), New Perspectives in Critical Data Studies 2022, 187 (194).

62 Vgl. Ebd. (202-208).

63 Vgl. schon *Crenshaw*, The University of Chicago Legal Forum 1989, 139.

muss, damit die strukturellen Privilegien, die vorwiegend weiße Männer genießen, nicht aus dem Fokus geraten.[64] Dies betrifft insbesondere die Objektivität vermeintlich statischer und gegebener Grundannahmen sozialer Kategorisierung, die zu hinterfragen ist, damit ebendiese bestehenden Strukturen und Privilegien aufgebrochen werden können.[65]

5. Fairness als Gerechtigkeit

In diesem Prozess des Hinterfragens ist es wesentlich, mit Hilfe der gesetzlichen Regelungen die herrschenden Machtstrukturen sichtbar zu machen, um Schieflagen zu erkennen, Teilhabe zu ermöglichen und Macht umzuverteilen. Diese Fragen von Gerechtigkeit können den Blickwinkel des Rechts erweitern und weiße Flecken ausfüllen.

Aus der Perspektive von *Data Justice* sind insbesondere individualistische Ansätze im Datenschutzrecht wenig hilfreich, da sie die dahinterliegenden Strukturen eher verwischen, als dass sie ein strukturelles Korrektiv anbieten.[66] Allerdings sollte das bestehende Datenschutz-Governance-System in seiner Gesamtheit betrachtet werden. Während etwa die DSGVO Regelungen zum Schutz von Individuen, wie etwa die Betroffenenrechte, enthält, deren effektive Umsetzung auch von den Ressourcen der betroffenen Personen selbst abhängt,[67] gibt es auch Regelungen, die gerade darauf setzen, dass Datenschutz „out of the box", von Beginn an, gewährleistet sein muss. Dies sind insbesondere die bereits angesprochenen Regelungen des Systemdatenschutzes,[68] nach denen insbesondere Risiken für die Grundrechte von Individuen bereits in der Planungsphase zu ermitteln und technische und organisatorische Maßnahmen zur Eindämmung dieser Risiken noch vor Beginn der Datenverarbeitung umzusetzen sind (vgl. Art. 25, 32, 35 DSGVO).

Während sich diese Regelungen also an individuellen Grundrechten als Maßstab orientieren, müssen sie nicht von betroffenen Personen durchgesetzt werden, sondern sind von Datenverarbeitenden stets zu berücksichtigen. Dabei ist natürlich problematisch, dass die Datenverarbeitenden

64 *Hoffmann*, Information, Communication & Society 2019, 900 (906).
65 Ebd. (907). *González Hauck*, Zeitschrift für Rechtssoziologie 2022, 153-175.
66 *Hintz*, in: Dencik u.a. (Hrsg.): Data Justice 2022, 89 (95-97).
67 Ebd. (95).
68 S. Abschn. 3; *Bieker*, The Right to Data Protection, 2022, 187 f.

selbst diese Maßnahmen ergreifen und damit einen Perspektivwechsel zugunsten der betroffenen Personen und gegebenenfalls gegen ihre eigenen wirtschaftlichen Interessen vornehmen müssen. In diesem Zielkonflikt liegt den Datenverarbeitenden eine Optimierung im Sinne von Umsatz, Gewinn und Marktanteil deutlich näher als die Beschäftigung mit Grundrechten; das geschäftliche Risiko einer spürbaren Sanktionierung oder im schlimmsten Fall einer Untersagung der konkreten Verarbeitung oder der Basis für das Geschäftsmodells durch die Datenschutzaufsicht wird als niedrig eingeschätzt.[69]

Damit es in der Praxis gelingt, Gerechtigkeit zu gewährleisten, muss Datenverarbeitung holistisch und kleinschrittig betrachtet werden: von den Komponenten und Prozessen über Software-Anwendungen, Betriebssysteme, Hardware bis zu Infrastrukturen wie Libraries und weithin genutzten Code-Repositories, Kommunikationsprotokollen und Plattformen sowie dem weiteren gesellschaftlichen Kontext der Nutzung der Datenverarbeitung. Diese Betrachtungen müssen stetig – in der Planungsphase, während der Gestaltung, beim Inbetriebnehmen und fortlaufend beim Einsatz – erfolgen. Nur durch solche Schutzmaßnahmen „by Design" lässt sich gewährleisten, dass die Risiken einer Datenverarbeitung für Individuen sich nicht in konkreten Schäden realisieren.[70]

Auch in technischen Systemen werden stets bewusste und unbewusste Vorstellungen, Grundannahmen und Werte ihrer Entwicklungsteams eingeschrieben.[71] Dies wird durch die bestehenden Machtstrukturen, die dazu führen, dass bestimmte Gruppen ihre Privilegien nicht hinterfragen müssen, sondern es als gegeben annehmen können nicht diskriminiert zu werden,[72] begünstigt und bildet dadurch diese Strukturen wiederum ab. Bei der Gestaltung dieser Systeme stellt sich also die grundlegende Frage, welche Werte in dem System umgesetzt werden.[73] Ansonsten drohen Werte – sowie bewusste und unbewusste Biases – ohne Bedacht und Reflektion festgeschrieben zu werden. Der Ansatz von *Value Sensitive Design* versucht,

69 Zu den drei Fällen in den Jahren 2019 bis 2022, in denen die Federal Trade Commission eine Löschung des Algorithmus angeordnet hatte, siehe *Goland* 2023, S. 17 ff.

70 *Hansen/Bieker/Bremert* 2022.

71 *Hicks*, in: Mullaney u.a. (Hrsg.), Your Computer is on Fire, 2021, 11 (14 f.). Dabei werden Forderungen nach mehr Diversität in den Entwicklungsteams, wie bereits in Abschn. 3 aufgezeigt, oft verwendet, um von den dahinterliegenden strukturellen Problemen abzulenken.

72 Vertiefend hierzu: *Eggers* u.a., Mythen, Masken und Subjekte, 2020.

73 *Friedman*, Interactions 1996.

diesen Prozess sichtbar zu machen. Dabei geht es in einem dreischrittigen Prozess zunächst in einer konzeptuellen Analyse darum, die direkt und indirekt betroffenen Personen („Stakeholder") und die umzusetzenden Werte und ihre Abwägung zu identifizieren. In einer empirischen Untersuchung wird im Anschluss der soziale Kontext der Technologie betrachtet und kann später auch der Erfolg eines bestimmten Designs untersucht werden. Schließlich wird in einer technischen Untersuchung analysiert, wie die angestrebten Werte durch proaktive Gestaltung unterstützt werden können.[74]

Um die notwendige Erweiterung des Betrachtungsrahmens für die genannten Probleme zu erreichen, lassen sich die Ansätze von *Data Justice* mit *Value Sensitive Design* und „by-Design"-Ansätzen kombinieren. Die daraus hervorgegangene Methodologie von *Design Justice* hinterfragt bestehende Machtverhältnisse, die sich in den einzelnen Bereichen von Datenverarbeitung und ihren Folgen zeigen.[75] Durch die frühzeitige Einbindung der Perspektiven der von Marginalisierung betroffenen Personen und Gruppen, die überproportional von den negativen Folgen, in Form der in Abschn. 2 beispielhaft aufgezeigten Diskriminierungen,[76] der hier besprochenen Datenpraktiken betroffen sind, können Risiken einer Verarbeitung bereits im Gestaltungsprozess erkannt werden.

Auch hier gilt es, Intersektionalität zu beachten und die gelebten Erfahrungen der Angehörigen marginalisierter Gruppen als Expertise über ihre eigene Unterdrückung ernst zu nehmen. Dabei gilt es, wie wir für das Antidiskriminierungsrecht bereits im vorigen Abschnitt festgestellt haben, auch zu berücksichtigen, inwieweit vermeintlich objektive Dritte durch bestehende Machtstrukturen Hegemonie ausüben können. Unter den Design-Prinzipien von *Design Justice* gilt es etwa die Personen, die von den Ergebnissen des Design-Prozesses direkt betroffen sind, in den Vordergrund zu stellen, den potenziellen Auswirkungen einer Design-Entscheidung einen höheren Stellenwert zu geben als den Intentionen der Designenden und Veränderungen nicht als Endpunkt, sondern als Teil eines fortlaufenden Prozesses zu betrachten.[77]

In Anlehnung an das Konzept von *Design Justice* und unter Berücksichtigung der Kritik der Individualisierung von Problemen zeigen wir im fol-

74 *Friedman u.a.*, in: Himma/Tavani (Hrsg.): The Handbook of Information and Computer Ethics, 2008.
75 *Costanza-Chock*, Design Justice, 2023.
76 S. auch ErwGr. 35, 36, 37, 44 KI-VO-Entwurf.
77 Ebd., 190-204.

genden Abschnitt auf, wie sich Daten-Gerechtigkeit in Prozessen verankern lässt, damit ein fortlaufendes Korrektiv aufgebaut wird.

6. Prozesse für Daten-Gerechtigkeit

Der aktuelle Stand der Implementierung von algorithmischen Systemen verdeutlicht bereits die Notwendigkeit der grundlegenden Umsetzung und Durchsetzung der datenschutzrechtlichen Regelungen. Die Einführung von Chatbots hat in besonderem Maße gezeigt, dass diese Vorschriften eine wesentliche Rolle spielen müssen. Die Regelungen zur Risikobewertung, „by-Design"-Ansätzen, Datenschutz-Folgenabschätzung und Rechenschaftsplicht hätten bereits frühzeitig zum Erkennen der bestehenden Probleme geführt. Dazu hätte auch gehört, die Rechtmäßigkeit der Verwendung der aus zahlreichen, großteils gegenüber den Nutzenden nicht offengelegten, Quellen gesammelten Daten in den zugrundeliegenden *Large Language Models* sicherzustellen und sich der Qualität – und der Datensammlungen inhärenten Biases – bewusst zu werden.

Es ist anzunehmen, dass bei einer vernünftigen Analyse der Risiken für Grundrechte eine Freigabe der Anwendungen nicht hätte erfolgen können. Neben grundlegenden Rechtmäßigkeitsfragen hätte die Folgenabschätzung nicht nur Risiken aufgezeigt, sondern auch Maßnahmen zur deren Einhegung oder Abmilderung enthalten.

Um solche Risiken überhaupt zu erkennen, genügt es jedoch nicht, eine Checkliste abzuarbeiten. Dafür sind die möglichen Risiken zu abhängig von den konkreten Kontexten eines Verarbeitungsvorgangs. Vielmehr bedarf es dafür vordefinierter Prozesse, die je nach Kontext angepasst werden. Um den spezifischen Kontext jeweils ausreichend zu berücksichtigen, ist es wiederum maßgeblich, dass der Einsatzzweck einer Anwendung – also letztlich der Zweck der Datenverarbeitung – im Vorwege ausreichend definiert wird.

Anstatt solche Anwendungen zu veröffentlichen und am Rande in den AGB[78] oder Aufsätzen in rudimentärer Weise auf bestehende Risiken hinzuweisen[79], ohne diese zu adressieren oder zu bewältigen, müssen die Risiken einer solchen Verarbeitung für die Rechte von Individuen noch vor dem Beginn der Verarbeitung umfassend beschrieben und bewertet

78 https://openai.com/policies/usage-policies.

79 *Bubeck u.a.*, Sparks of Artificial General Intelligence: Early experiments with GPT-4, 2023.

werden. Nur so kann der Verarbeitungsvorgang entsprechend den Risiken angepasst werden; einschließlich der möglichen Entscheidung, ein *Large Language Model* nicht zur allgemeinen Nutzung freizugeben, solange das nicht bisher beherrschte Risiko besteht, dass diese Anwendungen rassistische, sexistische und transphobe Diskriminierungen perpetuieren.

Es liegt nicht in der Verantwortlichkeit der betroffenen Personen, einen Verarbeitungsvorgang zu testen und Verbesserungsvorschläge zu unterbreiten. Diese Aufgabe ist im Datenschutzrecht, begrifflich und rechtlich, den Verantwortlichen, also den Datenverarbeitenden, zugeordnet. Im Datenschutzrecht ebenfalls Sache der Anbieter ist es im Rahmen ihrer Rechenschaftspflicht, über den ganzen Lebenszyklus einer Anwendung, also bereits vor Beginn über den Betrieb bis nach deren Einstellung, nachzuweisen, dass die datenschutzrechtlichen Anforderungen eingehalten werden.

Diese datenschutzrechtlichen Regelungen sollten jedoch ebenfalls erweitert und über den konkreten Kontext des Datenschutzes hinaus weitergedacht werden. Zum Beispiel ist es ein allgemeiner Grundsatz des Zivilrechts, dass eine Haftung für Tätigkeiten, die andere potenziell gefährden, besteht, wenn diese Gefahren nicht ausreichend durch Verkehrssicherungspflichten begrenzt werden. Demnach müssen durch den Verursacher der Gefahr die Maßnahmen ergriffen werden, die erforderlich sind, um dem Entstehen von Schäden vorzubeugen und negative Auswirkungen im Falle eines Schadenseintritts gering zu halten oder abzumildern. Diese Verkehrssicherungsgrundsätze aus der physischen Welt, z. B. zur Gebäude- oder Wegesicherung, sind auch auf den digitalen Bereich übertragbar. Zudem ist das Treffen von Maßnahmen zur Einhegung möglicher Schäden ein Grundsatz des Produkthaftungsrechts.[80] In Anbetracht der Risiken, die mit algorithmischen Systemen einhergehen und die oft gerade nicht ausreichend untersucht werden, erscheint auch eine Gefährdungshaftung, also eine Haftung ohne den Nachweis konkreten Verschuldens aufgrund der aus der Tätigkeit folgenden erlaubten Gefahr, wie etwa dem Betreiben gefährlicher Anlagen, möglich.[81]

Im Lebenszyklus von Anwendungen gibt es spezifische Risiken, die mit den Änderungen des Einsatzes oder der Umgebung verbunden sind und

80 Dabei sind auch Pflichtversicherungen denkbar. Ein von ChatGPT synthetisch erzeugter Text zu einer möglichen gesetzlichen Regelung findet sich bei *Wagner*, ZDF-heute v. 30. Apr. 2023.

81 Vgl. dazu auch den Entwurf der Kommission zu einer KI-Haftungsrichtlinie (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52022PC0496) und *de Conca* u.a., May Cause Liability – Use Care When Using the Internet of Things.

für deren Erkennung und Behandlung ein prozessorientierter Ansatz notwendig ist. So besteht die Gefahr eines *function creep*, also der schleichenden Ausweitung der ursprünglich begrenzten Zwecke durch Nutzende oder die einsetzende Organisation selbst. Diese Gefahr besteht natürlich nur, wenn die Zwecke vorab festgelegt sind, wie es in Art. 5 Abs. 1 Buchst. b DSGVO vorgeschrieben ist.

Mit ähnlicher Auswirkung können sich auch die Risiken einer Verarbeitung im Lauf der Zeit ändern oder müssen etwa mit neugewonnenen Erkenntnissen anders beurteilt werden. Beispielsweise ist die Annahme verbreitet, dass die Modelle, die durch Maschinenlernen entstehen, lediglich abstrahierte Muster oder Strukturen enthalten, die keinen unmittelbaren Rückschluss auf die möglicherweise personenbezogenen oder anderweitig sensiblen Trainingsdaten zulassen. Diese Annahme muss aber nicht stimmen: So konnten Forschungsteams für algorithmische Systeme demonstrieren,

1. dass sich zumindest in bestimmten Konstellationen feststellen ließ, ob Datensätze zu einer Person in den Trainingsdaten enthalten waren (Membership Inference Attack, z. B. bei *Large Language Models*, die mit Daten zu bestimmten Krankheiten oder Patient:innen in bestimmten Krankenhäusern trainiert wurden)[82] sowie
2. dass sich aus *Large Language Models* personenbezogene oder urheberrechtlich relevante Daten aus den Trainingsdaten extrahieren ließen.[83]

Diese Erkenntnisse sind aus Datenschutzsicht besonders deswegen relevant, weil *Large Language Models* zumeist wie anonyme Daten eingestuft wurden und man annahm, dass mit dem Maschinenlernen der Effekt einer Anonymisierung einherginge. Anonyme oder anonymisierte Daten unterfallen jedoch – anders als personenbezogene Trainingsdaten – nicht dem Datenschutzrecht. Unter dieser Annahme wurde bisher nach unserer Kenntnis nicht problematisiert, wenn algorithmische Systeme aus der EU in einen Drittstaat weitergegeben wurden. Doch angesichts des Stands der Forschung, dass darin eben doch personenbezogene Daten eincodiert seien und entlockt werden könnten, wäre die Annahme einer vorliegenden Anonymität nicht haltbar; der Anwendungsbereich der DSGVO wäre eröff-

82 *Shokri u.a.* 2017, *Ye u.a.* 2022.
83 *Frederikson u.a.* 2015, *Yeom u.a.* 2020, *Carlini u.a.* 2021, *Tramèr u.a.* 2022, *Yu u.a.* 2023.

net.[84] Dieser Effekt von vermeintlich anonymen Daten kann insbesondere deswegen Schäden für die Grundrechte der betroffenen Personen auslösen, wenn die Verantwortlichen keine Vorsorge für diesen Fall getroffen haben, weil sie sich außerhalb der DSGVO wähnten.[85]

Folglich ist auch für die Überwachung von Risiken ein durchgängiger Prozess notwendig,[86] der eine Anwendung über den gesamten Lebenslauf begleitet. Auch bedarf es einer konstruktiven Fehlerkultur, die nicht durch eine voreilige Entschuldigung versucht, eine Diskussion zu beenden, sondern durch die ein Verantwortlicher die Folgen eines Fehlers begrenzt und Änderungen umsetzt, um diesen Fehler in der Zukunft ausschließen zu können.

In diesem Kontext wird auch deutlich, wie sinnvoll es ist, dass der Risiko-Begriff der DSGVO[87] nicht nur auf die Rechte der betroffenen Personen (also Personen, deren Daten verarbeitet werden), sondern auf sämtliche natürliche Personen abstellt, ganz im Sinne der direkten und indirekten betroffenen Stakeholder im Rahmen des *Value Sensitive Designs*. Wenn etwa ein *Large Language Model* aufgrund der Daten einer bestimmten Gruppe von Personen einen Bias aufweist, kann sich dieser zulasten ganz anderer Personen auswirken.[88]

Auch die Erkenntnisse zur Intersektionalität von Diskriminierungen müssen in diesen Prozessen berücksichtigt werden. Dies gilt etwa konkret für die Bewertung von Risiken und die Erkenntnis, dass Personen, die unter verschiedene, sich überschneidende Kategorisierungen fallen einem besonders hohen Risiko unterfallen. Dieses ergibt sich nicht einfach aus

84 Wiederum gibt es Forschungsansätze zum gezielten „Machine Unlearning", sodass es nicht undenkbar ist, einzelne oder viele Datensätze „herauszulernen" und damit auch einen Schutz gegen „Membership Inference Attacks" oder dem Auslesen der Daten zu schaffen; für einen Überblick siehe *Nguyen et al.* 2022. Es ist noch nicht geklärt, inwieweit mit bestimmten Unlearning-Ansätzen auch das Betroffenenrecht auf Löschung umgesetzt werden kann und unter welchen Umständen dies überhaupt eine realistische Option darstellt.

85 *Bruegger* 2021, S. 103 ff.

86 Vgl. auch *Bender u.a.*, in: FAcct '21, S. 619.

87 Auch nach Artikel 34 Abs. Buchst. b Digitale-Dienste-Verordnung ist eine Bewertung der nachteiligen Auswirkungen der Grundrechte, insbesondere des Rechts auf Nichtdiskriminierung vorgesehen, nach Art. 48 Abs. 4 Buchst. e sind Schutzvorkehrungen zur Vermeideung negativer Auswirkungen vorgesehen.

88 *Bieker*, The Right to Data Protection, 2023, 189.

einer simplen Addition der Risiken, denen etwa ein Schwarzer Mann (Rassismus) und eine weiße Frau (Sexismus) ausgesetzt sind.[89]

Allerdings gilt generell bei der Risikobewertung, dass diese sich nicht hinter vermeintlich objektiver Pseudo-Mathematik verstecken darf.[90] Mit diesem erweiterten Fokus, der auf breiteren Gerechtigkeitsüberlegungen auch außerhalb des Datenschutzrechts fußt, gibt es noch weitere Gruppen, die von algorithmischen Systemen betroffen sind. Dazu zählen insbesondere die Arbeiter:innen, die „unsichtbare Arbeit", etwa an den Chatbots zugrundeliegenden *Large Language Models* selbst, verrichten.[91] Zudem beruhen viele Anwendungen, die sich algorithmischer Systeme bedienen, darauf, dass konkrete Personen die Arbeit, die mit Hilfe der Systeme organisiert werden soll, verrichten. Dies sind in vielen Fällen sogenannte Gig-Worker:innen, also prekär Beschäftigte, die Waren ausliefern oder andere Dienstleistungen, wie zum Beispiel Content-Moderation, erbringen.

Die Einbindung der betroffenen Personen und Endnutzer:innen einer Anwendung, insbesondere Angehöriger bereits marginalisierter Gruppen, ist zudem ein wesentlicher Teil jeder Risikobewertung. Dies ist auch im Rahmen einer Datenschutz-Folgenabschätzung eine Möglichkeit (Art. 35 Abs. 9 DSGVO), von der frühzeitig im Prozess Gebrauch gemacht werden sollte. Dabei ist die Perspektive der betroffenen Personen und Gruppen als Expert:innen der von ihnen erfahrenen Diskriminierungen bereits bei der Identifizierung möglicher, auch intersektionaler, Risiken eine hilfreiche Unterstützung.

Allerdings ist es wichtig, auch hier Probleme nicht zu individualisieren oder etwa in ausbeuterische Muster zu verfallen. So besteht die Gefahr einer Tokenisierung[92] einzelner Angehöriger marginalisierter Gruppen, also der Vereinnahmung einer einzelnen Person als Repräsentant:in einer ganzen Gruppe, um Inklusion vorzutäuschen, oder eine mangelnde Anerkennung der Arbeit betroffener Personen in einem solchen Prozess, die in der Regel zu vergüten ist. Die DSGVO verweist explizit auf Organisationen, die die Interessen der betroffenen Personen vertreten. Es geht also auch hier um eine breite Einbindung von NGOs, Organisationen der Zivilgesellschaft, Gewerkschaften, Kooperativen und Bewegungen, die auch

89 *Crenshaw*, The University of Chicago Legal Forum 1989, 139 (149, 151 f.).
90 *Bieker/Hansen/Friedewald*, RDV 2016, 188 (193).
91 Gray/Suri, Ghost Work, 2019.
92 *Theilen u.a.*, Internet Policy Review 2021, S. 5.

diejenigen einbeziehen sollte, die die „unsichtbare Arbeit" verrichten, wie z. B. Gig-Worker:innen.

Es ist selbstverständlich problematisch, dass ausgerechnet der für die Datenverarbeitung Verantwortliche die gegenläufigen Interessen betrachten und umsetzen muss. Dies ist eine inhärente Begrenzung des Datenschutz- und letztlich auch Antidiskriminierungsrechts, sodass auch der Rückgriff auf dieses das Problem nicht ohne Weiteres lösen kann. Die rechtlichen Korrektive gegen Verstöße sind zudem für die betroffenen Personen mühsam und erfordern von der Beschwerde bei den entsprechenden Stellen bis zum Führen eines langwierigen und teuren Gerichtsverfahrens über mehrere Instanzen erhebliche finanzielle, zeitliche und mentale Ressourcen.[93]

Dabei besteht zudem das Problem, dass sich Datenverarbeitende nach dem Unterliegen in einem Gerichtsverfahren darauf berufen, ihre Praxis inzwischen angepasst zu haben, um sich so den gerichtlichen Anforderungen zu entziehen. Im schlimmsten Fall erfordert dies erneute (gerichtliche) Auseinandersetzungen, damit eine angemessene Umsetzung erfolgt. Dies liegt auch an den geradezu unbegrenzten Ressourcen, die Anbietern zur Verfügung stehen, um ihre Geschäftsmodelle zu verteidigen.

Um dieses Gefälle zwischen den Anbietern, mit ihrer Informationsmacht, und den Einzelnen, die die Risiken dieser Machtakkumulation tragen, zu überbrücken, sind tiefgreifende strukturelle Eingriffe notwendig, die über das bestehende Daten(schutz)recht hinausgehen. Dabei sollte jedoch nicht auf unpassende historischen Präzedenzfälle geblickt werden; die Anbieter von heute agieren global und ähneln daher weniger den nationalen Elektrizitäts- oder Eisenbahnmonopolen des 19. und 20. Jahrhunderts. Insofern ist nicht klar, ob mit kartellrechtlichen Regelungen auf nationaler oder europäischer Ebene die Informationsmacht der Anbieter wirkungsvoll zu regeln ist oder ob dies nur auf internationaler Ebene, etwa in Form von Governance-Modellen wie der ICANN – die wiederum eigene Probleme aufweisen – oder durch die Implementierung von Protokollen auf Infrastruktur-Ebene, zu erreichen ist.[94]

93 So nahm der Rechtsstreit einer betroffenen Person gegen ehrverletzende Suchwortergänzungen zum eigenen Namen, die Google als Autocomplete-Funktion im Jahr 2009 eingeführt hatte, mehrere Jahre bis zum BGH-Urteil vom 14. Mai 2013 – VI ZR 269/12 – in Anspruch. Als Reaktion führte Google ein Formular zum Entgegennehmen von Beschwerden ein. Dass die Anbieter von ChatGPT oder anderen Anwendungen das BGH-Urteil in die Gestaltung ihres Angebots einbezogen hätten, ist nicht ersichtlich.

94 *Keyes*, Wired v. 11. Jan. 2022.

7. Ausblick

Es ist daher fraglich, ob im Rahmen der aktuellen Debatte um den Einsatz algorithmischer Systeme eine Lösung erreicht werden kann, die die fundamentalen Probleme dieser Technik ausreichend durch eine Veränderung der ihrer Anwendung zugrundeliegenden Machstrukturen bewirkt. Notwendig wäre es dafür zunächst den Fokus von Einzelnen abzuwenden und stattdessen die bestehenden gesellschaftlichen Machtstrukturen zu analysieren. Eine solche Analyse muss den Blick jedoch über das, was klassischerweise als Datenschutzrecht angesehen wird, hinaus in benachbarte Rechtsgebiete lenken.

Allerdings liefern auch diese Bereiche, wie etwa das Antidiskriminierungsrecht in Bezug auf die hier beschriebenen intersektionalen Diskriminierungen, keine Patentlösungen. Es ist daher eine Erweiterung der Perspektive jenseits des Rechts auch auf Lösungsansätze nötig, die von Angehörigen marginalisierter Gruppen entwickelt wurden. Mit den grundlegenden Prozessen des bestehenden Datenschutzrechtes lassen sich – durch eine solche Perspektiverweiterung – viele der aktuellen Probleme erfassen, bewerten und Abhilfemaßnahmen ableiten.

Wesentlich ist die Erkenntnis, dass die aktuellen Datenpraktiken nicht alle Menschen gleich, sondern marginalisierte Gruppen überproportional treffen. Auch hier muss sich der Fokus von der Industrie und den Anbietern algorithmischer Systeme abwenden. Nur weil jemand ein Problem schafft, heißt es nicht, dass er, mit all seinen wirtschaftlichen Eigeninteressen,[95] auch zur Problemdefinition und -lösung berufen ist.[96] Vielmehr muss die Deutungshoheit von der Industrie hin zu den betroffenen Personen und der Gesellschaft insgesamt gelenkt werden.

Die bestehenden Strukturen, die es Unternehmen ermöglichen und sogar dafür Anreize bieten, mächtige *Large Language Models* bereitzustellen und Risiken auszulagern, müssen grundlegend verändert werden. Erst wenn Anbieter gezwungen sind, Risiken zu bewältigen, bevor sie mit Anwendungen Geld verdienen oder Marktanteile sichern können, ist es realistisch, dass Regelungen, die ihren wirtschaftlichen Interessen derart entgegenlaufen wie der Schutz marginalisierter Gruppen und Datenschutz, umgesetzt werden.

95 Die sich durch den Einsatz von Anwendungen, die auf *Large Language Models* beruhen, zukünftig noch einfacher und womöglich (teil-)automatisiert vertreten lassen, vgl. *Sanders/Schneier*, Technology Review v. 14 März. 2023.

96 *Dencik*, in: Dencik u.a. (Hrsg.): Data Justice 2022, 123 (133 f.).

Je stärker eine Technik Auswirkungen auf die Menschen und die demokratische Gesellschaft haben kann, desto wichtiger ist eine unabhängige Kontrolle bereits vor dem Inverkehrbringen und auch während ihres Einsatzes. Nur so kann Technik dazu beitragen gesellschaftliche Probleme zu lösen und nicht, um die wirtschaftlichen Interessen weniger zu erfüllen, eine Vielzahl von Problemen für die Gesellschaft insgesamt zu verstärken oder zu verursachen.

Danksagung

Diese Arbeit wurde vom Bundesministerium für Bildung und Forschung im Rahmen des Projekts „Privatheit, Demokratie und Selbstbestimmung im Zeitalter von Künstlicher Intelligenz und Globalisierung“ (PRIDS), https://forum-privatheit.de/, gefördert (FKZ 16KIS1376). Wir bedanken uns herzlich bei Jens T. Theilen für die hilfreichen Anmerkungen.

Literatur

Alle Internet-Quellen zuletzt besucht am 08.05.2023

Altman, Sam (24. Feb. 2023): Planning for AGI and beyond. URL: https://openai.com/blog/planning-for-agi-and-beyond

Atleson, Michael (27. Feb. 2023): Keep your AI claims in check. URL: https://www.ftc.gov/business-guidance/blog/2023/02/keep-your-ai-claims-check

Bender, Emily M.; Gebru, Timnit; McMillan-Major, Angelina und Shmitchell, Shmargaret (2021): On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? In: *FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*. S. 610-623. URL: https://doi.org/10.1145/3442188.3445922

Bender, Emily M. (2022): Human-like programs abuse our empathy – even Google engineers aren't immune. *The Guardian* vom 14. Jun. 2022. URL: https://www.theguardian.com/commentisfree/2022/jun/14/human-like-programs-abuse-our-empathy-even-google-engineers-arent-immune

Biddle, Sam (2022): The Internet's New Favorite AI Proposes Torturing Iranians and Surveilling Mosques. *The Intercept* vom 8. Dez. 2022. URL: https://theintercept.com/2022/12/08/openai-chatgpt-ai-bias-ethics/

Bieker, Felix (2022): *The Right to Data Protection: Individual and Structural Dimensions of Data Protection in EU Law*. The Hague: T.M.C. Asser Press. URL: https://doi.org/10.1007/978-94-6265-503-4

Bieker, Felix (2018): Die Risikoanalyse nach dem neuen EU-Datenschutzrecht und dem Standard-Datenschutzmodell. *Datenschutz und Datensicherheit (DuD)*, 42(1), S. 27-31.

Bieker, Felix; Hansen, Marit; Friedewald, Michael (2016): Die grundrechtskonforme Ausgestaltung der Datenschutz-Folgenabschätzung. *Recht der Datenverarbeitung (RDV)*, 32(4), S. 188-197.

Browne, Simone (2015): *Dark Matters*. Durham: Duke University Press.

Bruegger, Bud P. (2021): Towards a Better Understanding of Identification, Pseudonymization, and Anonymization. ULD. https://uld-sh.de/PseudoAnon

Bubeck, Sébastien; Chandrasekaran, Varun; Eldan, Ronen; Gehrke, Johannes; Horvitz, Eric; Kamar, Ece; Lee, Peter; Lee, Yin Tat; Li, Yuanzhi; Lundberg, Scott; Nori, Harsha; Palangi, Hamid; Ribereiro, Marco Tulio; Zhang, Yi (2023): Sparks of Artificial General Intelligence: Early experiments with GPT-4. URL: https://arxiv.org/abs/2303.12712

Buolamwini, Joy; Gebru, Timnit (2018): Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: *Proceedings of Machine Learning Research 81*, S. 1-15. URL: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Carlini, Nicholas; Tramèr, Florian; Wallace, Eric; Jagielski, Matthew; Herbert-Voss, Ariel; Lee, Katherine; Roberts, Adam; Brown, Tom; Song, Dawn; Erlingsson, Úlfar; Oprea, Alina; Raffel, Colin (2021): Extracting Training Data from Large Language Models. In: *Proceedings of 30th USENIX Security Symposium*, S. 2633-2650. https://www.usenix.org/conference/usenixsecurity21/presentation/carlini-extracting

Clarke, Arthur C. (1973): Profiles of the Future: An Inquiry into the Limits of the Possible. 2. Aufl. Harper & Row.

Constantaras, Eva; Geiger, Gabriel; Braun, Justin-Casimir; Mehrotra, Dhruv; Aung, Htet (2023): Inside the Suspicion Machine. *Wired* vom 6. Mar. 2023. URL: https://www.wired.com/story/welfare-state-algorithms/

Crenshaw, Kimberle (1989): Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics. *The University of Chicago Legal Forum*, 168, 139-167.

de Conca, Silvia; Bratu, Ioana; Leiser, Mark; Cooper, Zac (14. Nov. 2022): May Cause Liability – Use Care When Using the Internet of Things. URL: https://alti.amsterdam/may-cause-liability-part-1/

Dencik, Lina (2022): Data and Social Justice. In: Dencik, Lina; Hintz, Arne; Redden, Joanna; Treré, Emiliano (Hrsg.): *Data Justice*. Los Angeles: Sage. S. 123-137.

Draude, Claude; Hornung, Gerrit, Klumbytė, Goda (2022): Mapping Data Justice as a Multidimensional Concept Through Feminist and Legal Perspectives. In: Hepp, Andreas; Jarke, Juliane; Kramp, Leif (Hrsg.): *New Perspectives in Critical Data Studies*. Cham: Palgrave Macmillan. S. 187-216.

Eubanks, Virginia (2018): The Digital Poorhouse. *Harper's Magazine* von Jan. 2018. URL: https://harpers.org/archive/2018/01/the-digital-poorhouse/

Elish, Madeleine Clare (17. Jan. 2018). Don't Call AI "Magic". URL: https://points.datasociety.net/dont-call-ai-magic-142da16db408

Fredrikson, Matt; Jha, Somesh; Ristenpart, Thomas: Model inversion attacks that exploit confidence information and basic countermeasures. *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS '15)*. S. 1322-1333. https://doi.org/10.1145/2810103.2813677

Freeman, Alan David (1978): Legitimizing racial discrimination through antidiscrimination law: A critical review of Supreme Court doctrine. *Minnesota Law Review*, 62, S. 1049-1120.

Friedewald, Michael; Bieker, Felix; Obersteller, Hannah; Nebel, Maxi; Martin, Nicholas; Rost, Martin; Hansen, Marit (2019): White Paper Datenschutz-Folgenabschätzung. Karlsruhe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. URL: https://www.forum-privatheit.de/download/datenschutz-folgenabschaetzung-3-auflage-2017/

Friedewald, Michael; Székely, Iván; Karaboga, Murat; Runge, Greta; Ebbers, Frank (2023, i.E.): Access to Archives: Implementation of Recommendation No. R(2000)13 on a European policy on access to archives. Study commissioned by the Council of Europe. Karlsruhe: Fraunhofer ISI.

Friedman, Batya (1996): Value-Sensitive Design. *Interactions*, 3(6), S. 17-23. URL: https://dl.acm.org/doi/pdf/10.1145/242485.242493

Friedman, Baty; Kahn, Peter H.; Borning, Alan (2008): Value Sensitive Design and Information Systems. In: Himma, Kenneth Einar; Tavani, Herman T. (Hrsg.): *The Handbook of Information and Computer Ethics*. Hoboken: John Wiley & Sons. URL: https://onlinelibrary.wiley.com/doi/10.1002/9780470281819.ch4

Gal, Uri (2023). ChatGPT is a data privacy nightmare. If you've ever posted online, you ought to be concerned. *The Conversation* vom 8. Feb. 2023. URL: https://theconversation.com/chatgpt-is-a-data-privacy-nightmare-if-youve-ever-posted-online-you-ought-to-be-concerned-199283

Gilliard, Chris; Culik, Hugh (24. Mai 2016): Digital Redlining, Access, and Privacy. URL: https://www.commonsense.org/education/articles/digital-redlining-access-and-privacy

Goland, Joshua A. (2023): Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as The FTC's Newest Enforcement Tool for Bad Data. *Richmond Journal of Law & Technology*, 29(2).

González Hauck, Sué (2022): *Weiße* Deutungshoheit statt Objektivität: Der ‚objektive Dritte' und die systematische Abwertung rassismuserfahrener Perspektiven. *Zeitschrift für Rechtssoziologie*, 42(2), S. 153-175.

Gray, Mary L.; Suri, Siddarth (2019): *Ghost Work*, Boston: Houghton Miffin Harcourt.

Guijarro Santos, Victoria (2023): Nicht besser als nichts, ein Kommentar zum KI-Verordnungsentwurf. *Zeitschrift für Digitalisierung und Recht*, 3, S. 23-42.

Hansen, Marit; Bieker, Felix; Bremert, Benjamin (2022): Datenschutz und Privatheitsschutz durch Gestaltung der Systeme. In: Roßnagel, Alexander; Friedewald, Michael (Hrsg.): *Die Zukunft von Privatheit und Selbstbestimmung*, Wiesbaden: Springer Vieweg. S. 259-300. https://doi.org/10.1007/978-3-658-35263-9_8

Hansen, Marit; Krasemann, Henry (2022): Datenherausgabe und Informationsfreiheit by Design – Was (nicht nur behördliche) Datenschutzbeauftragte wissen sollten. *BvD-News* 2/2022, S. 34-38.

Hasters, Alice (2020): Was weiße Menschen nicht über Rassismus hören wollen aber wissen sollten. München: Hanserblau.

Heidelberger, Natali; Diakopoulos, Nicholas (2023): ChatGPT and the AI Act. *Internet Policy Review*, 12(1). URL: https://policyreview.info/essay/chatgpt-and-ai-act

Hicks, Mar (2019): Hacking the Cis-tem. *IEEE Annals of the History of Computing* 2019, S. 20-33.

Hicks, Mar (2021): When Did the Fire Start? In: Mullaney, Thomas S.; Peters, Benjamin; Hicks, Mar; Philip, Kavita (Hrsg.): *Your Computer is On Fire*. Cambridge, MA: MIT Press. S. 11-26.

Hill Collins, Patricia; Bilge, Sirma (2020): *Intersectionality*. 2. Aufl. Cambridge: Polity.

Hintz, Arne (2022): Data and Policy. In: Dencik, Lina; Hintz, Arne; Redden, Joanna; Treré, Emiliano (Hrsg.): *Data Justice*. Los Angeles: Sage. S. 89-104.

Hoffmann, Anna Lauren (2019): Where fairness fails: data, algorithms, and the limits of antidiscrimination discourse. *Information, Communication & Society* 22(7), S. 900-915.

Johnson, Khari (2022): DALL-E 2 Creates Incredible Images—and Biased Ones You Don't See. *Wired* vom 5. Mai 2022. URL: https://www.wired.com/story/dall-e-2-ai-text-image-bias-social-media/

Jones, Phil (2021): *Work without the Worker, Labour in the Age of Platform Capitalism*. London: Verso.

Eggers, Maureen Maisha; Kilomba, Grada; Piesche, Peggy; Arndt, Susan (2020): Mythen, Masken und Subjekte – Kritische Weißseinsforschung in Deutschland. 4. Aufl. Münster: Unrast-Verlag.

Kaminski, Margot (2022): The Case for Data Privacy Rights (or "Please, a little Optimism"), *Notre Dame Law Review Reflection*, 97(5), S. 385-399.

Keyes, Os (2022): It Doesn't Make Sense to Treat Facebook Like a Public Utility. *Wired* vom 11. Jan. 2022. URL: https://www.wired.com/story/facebook-public-utility-regulation/

Liebscher, Doris (2021): *Rasse im Recht – Recht gegen Rassismus*. Berlin: Suhrkamp.

Luccioni, Alexandra Sasha; Akiki, Christopher; Mitchell, Margaret; Jernite, Yacinde (2023): Stable Bias: Analyzing Societal Representations in Diffusion Models. URL: https://arxiv.org/abs/2303.11408

Mac, Ryan (2021): Facebook Apologizes after A.I. Puts 'Primates' Label on Video of Black Men, *New York Times* vom 3. Sep. 2021. URL: https://www.nytimes.com/2021/09/03/technology/facebook-ai-race-primates.html

Matzner, Tobias, Masur, Philipp K., Ochs, Carsten, von Pape, Thilo (2016): Do-It-Yourself Data Protection—Empowerment or Burden? In: Gutwirth, Serge, Leenes, Ronald, De Hert, Paul (Hrsg.): *Data Protection on the Move*. Law, Governance and Technology Series. Dordrecht: Springer. https://doi.org/10.1007/978-94-017-7376-8_11

Nguyen, Thanh Tam; Huynh, Thanh Trung; Nguyen, Phi-Le; Liew, Alan Wee-Chung; Yin, Hongzhi; Nguyen, Quoc Viet Hung (2022): A Survey of Machine Unlearning. https://arxiv.org/abs/2209.02299. Siehe auch https://github.com/tamlhp/awesome-machine-unlearning

Perrigo, Billy (2022): AI Chatbots Are Getting Better. But an Interview With ChatGPT Reveals Their Limits. *Time* vom 5. Dez. 2022. URL: https://time.com/6238781/chatbot-chatgpt-ai-interview/

Powles, Julia; Nissenbaum, Helen (2018): The Seductive Diversion of 'Solving' Bias in Artificial Intelligence. *Medium* vom 7. Dez. 2018. URL https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53

Raji, Inioluwa Deborah; Bender, Emily M.; Paullada, Amandalynne; Denton, Emily; Hanna, Alex (2021). in: *Proceedings of the Neural Information Processing Systems Track on Datasets and Benchmarks 1 (NeurIPS Datasets and Benchmarks 2021)*. URL: https://datasets-benchmarks-proceedings.neurips.cc/paper_files/paper/2021/file/084b6fbb10729ed4da8c3d3f5a3ae7c9-Paper-round2.pdf

Raji, Inioluwa Deborah; Kumar, I. Elizabeth; Horowitz, Aaron; Selbst, Andrew D. (2022): The Fallacy of AI Functionality. In: *FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*. URL: https://facctconference.org/static/pdfs_2022/facct22-78.pdf

Roberts, Sarah T. (2021): Your AI is a Human. In: Mullaney, Thomas S. u.a. (Hrsg.): *Your Computer is on Fire*. Cambridge, Mass. und London: MIT Press, S. 51-70.

Roose, Kevin (2023): A Conversation with Bing's Chatbot Left Me Deeply Unsettled. *New York Times* vom 16. Feb. 2023. URL: https://www.nytimes.com/2023/02/16/technology/bing-chatbot-microsoft-chatgpt.html

Rouvroy, Antoinette und Poullet, Yves (2009): The Right to Informational Self-Determination and the Value of Self-Development, Reassessing the Importance of Privacy for Democracy. In: Gutwirth, Serge; Poullet, Yves; De Hert, Paul; de Terwangne, Cécile; Nouwt, Sjaak (Hrsg.): *Reinventing Data Protection?* Dordrecht: Springer, S. 45-76.

Sanders, Nathan E.; Schneier, Bruce (2023): How AI could write our laws. *Technology Review* vom 14 Mar. 2023. URL: https://www.technologyreview.com/2023/03/14/1069717/how-ai-could-write-our-laws/

Schräer, Frank (2023): Google Bard: Fehlerhafte Antwort der KI lässt Experten und Anleger zweifeln, *Heise Online* vom 09. Feb. 2023; abrufbar unter: https://www.heise.de/news/Google-Bard-Fehlerhafte-Antwort-der-KI-laesst-Experten-und-Anleger-zweifeln-7489896.html

Schwartz, Oscar (2018): 'The discourse is unhinged': how the media gets AI alarmingly wrong. *The Guardian* vom 25. Jul. 2018. URL: https://www.theguardian.com/technology/2018/jul/25/ai-artificial-intelligence-social-media-bots-wrong

Shanklin, Will (2023): Snapchat adds OpenAI-powered chatbot and proactively apologizes for what it might say. *Engadget* vom 27. Feb. 2023. URL: https://www.engadget.com/snapchat-adds-openai-powered-chatbot-and-proactively-apologizes-for-what-it-might-say-180507261.html

Shokri, Reza; Stronati, Marco; Song, Congzheng; Shmatikov, Vitaly (2017): Membership Inference Attacks Against Machine Learning Models. *Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP '17)*. S. 3-18. https://doi.org/10.1109/SP.2017.41

Taylor, Luke (2023): Colombian Judge says he used ChatGPT in ruling. *The Guardian* vom 3. Feb. 2023. URL: https://www.theguardian.com/technology/2023/feb/03/colombia-judge-chatgpt-ruling

Theilen, Jens T.; Baur, Andreas; Bieker, Felix; Ammicht Quinn, Regina; Hansen, Marit; González Fuster, Gloria (2021): Feminist Data Protection: An Introduction. *Internet Policy Review*, 10(4). URL: https://policyreview.info/pdf/policyreview-2021-4-1609.pdf

Tramèr, Florian; Shokri, Reza; San Joaquin, Ayrton; Le, Hoang; Jagielski, Matthew; Hong, Sanghyun; Carlini, Nicholas (2022): Truth Serum: Poisoning Machine Learning Models to Reveal Their Secrets. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*. S. 2779-2792, https://doi.org/10.1145/3548606.3560554

Veale, Michael; Silberman, Michael; Binns, Reuben (2023): Fortifying the algorithmic management provision in the proposed Platform Work Directive. *European Labour Law Journal*, 14(2). S. 308-322, https://doi.org/10.1177/20319525231167983

Volpicelli, Gian (2023): ChatGPT broke the EU plan to regulate AI. *Politico* vom 3. März 2023. URL: https://www.politico.eu/article/eu-plan-regulate-chatgpt-openai-artificial-intelligence-act/

Wagner, Lukas (2023): Ethischer Umgang mit der Technik: Wie KI in Zukunft reguliert werden soll. *ZDFheute* vom 30. Apr 2023. URL: https://www.zdf.de/nachrichten/politik/ki-regeln-gesetz-ai-act-eu-ethik-experten-100.html

Xiang, Chloe (2022): AI Is Probably Using Your Images and It's Not Easy to Opt Out, *Vice*, 26.09.2022, https://www.vice.com/en/article/3ad58k/ai-is-probably-using-your-images-and-its-not-easy-to-opt-out

Ye, Jiayuan; Maddi, Aadyaa; Murakonda, Sasi Kumar; Bindschaedler, Vincent; Shokri, Reza (2022): Enhanced Membership Inference Attacks against Machine Learning Models. In: *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*. S. 3093-3106. https://doi.org/10.1145/3548606.3560675

Yeom, Samuel; Giacomelli, Irene; Menaged, Alan; Fredrikson, Matt; Jha, Somesh (2020): Overfitting, Robustness, and Malicious Algorithms: A Study of Potential Causes of Privacy Risk in Machine Learning. *Journal of Computer Security* 28(1), S. 35-70. https://doi.org/10.3233/JCS-191362

Yu, Weichen; Pang, Tianyu; Liu, Qian; Du, Chao; Kang, Bingyi; Huang, Yan; Lin, Min; Yan, Shuicheng (2023): Bag of Tricks for Training Data Extraction from Language Models. https://arxiv.org/pdf/2302.04460.pdf

Beteiligung von Betroffenen in der Abwägung und Adressierung von Datenschutzrisiken: Grundrechte schützen durch partizipative Technikgestaltung

Daniel Guagnin, Fabian Dantscher und Antonios Hazim

Zusammenfassung

Für die Wahrung der Grundrechte der Betroffenen im Rahmen der Verarbeitung ihrer Daten ist es an einigen Stellen der Datenschutz-Grundverordnung (DSGVO) gefordert, die Risiken der Datenverarbeitung abzuwägen. Eine Reihe von Datenverarbeitungen erfordern zudem eine Datenschutz-Folgenabschätzung. Eine Konsultation der potentiell Betroffenen selbst ist nach DSGVO nicht obligatorisch, erscheint jedoch äußerst sinnvoll.

Im Projekt „KIDD – KI im Dienste der Diversität"[1] erproben wir einen Ansatz zur partizipativen Ausgestaltung und Einführung von KI-Anwendungen und algorithmischen Entscheidungssystemen in Betrieben, bei dem die Berücksichtigung der Diskriminierungsfreiheit im Fokus steht. Die frühzeitige Einbindung unterschiedlicher Perspektiven ermöglicht es, Werte wie Datenschutz und Diskriminierungsfreiheit im Sinne eines Value-Sensitive-Designs von Anfang an zusammenzudenken und so zu einer datenschutzfreundlichen Gestaltung zu gelangen. Auf diese Weise wird auch die DSGVO-Anforderung eines Datenschutz-by-Design Ansatzes adressiert. Der Beitrag diskutiert das entwickelte partizipative Verfahren und die praktischen Herausforderungen vor dem Hintergrund der Anforderungen an Datenschutz-Folgenabschätzungen und des Ansatzes des Value-Sensitive-Designs.

1. Einleitung

Digitalisierungsprozesse haben einen stetig wachsenden Einfluss auf vielfältige Lebensbereiche. Im KIDD-Projekt, aus dem dieses Paper entstanden ist, fokussieren wir auf die Arbeitswelt. Insbesondere die Einführung von

1 Das KIDD-Projekt wurde gefördert vom Bundesministerium für Arbeit und Soziales. Mehr Infos zum Projekt: kidd-prozess.de (letzter Aufruf 20.04.2023).

algorithmischen Entscheidungssystemen (AES), die personenbezogene Daten automatisiert erfassen, analysieren und auf Basis der Ergebnisse eine Entscheidung(-sempfehlung) ableiten, birgt für Unternehmen Chancen und Risiken. Um strukturelle Benachteiligungen Einzelner und Einschränkungen von Grundrechten in der Anwendung von AES zu minimieren, müssen mögliche Auswirkungen solcher Anwendungen schon während des Design-Prozesses reflektiert, Risiken abgewogen und angemessene technische Lösungen entworfen werden. Um sicherzustellen, dass die Werte, auf denen unsere Grundrechte beruhen, bei der Entwicklung von Softwaresystemen berücksichtigt werden, zeichnet sich Value-Sensitive-Design (VSD) als ein theoretisch fundierter Ansatz aus, der darauf abzielt, gesellschaftliche Werte während des gesamten Gestaltungsprozesses zu berücksichtigen (Friedman u. a. 2013).

Schon lange vor dem Inkrafttreten der Datenschutz-Grundverordnung wurde Datenschutz und das Grundrecht auf Privatsphäre in verschiedenen Ansätzen von Impact-Assessments, oder zu deutsch: Folgenabschätzungen, diskutiert und erprobt (z. B. Wright und de Hert 2012), und eine datenschutzfreundliche Entwicklung durch Privacy-by-Design gefordert. Seit 2018 sind aber sowohl Datenschutz-by-Design also auch eine Datenschutz-Folgenabschätzung (DSFA) in bestimmten Fällen rechtlich geboten.

Im Projekt „KIDD – KI im Dienste der Diversität“[2] (KIDD) wird ein standardisierter Prozess entwickelt, mithilfe dessen Unternehmen befähigt werden sollen, „gerechte, transparente und verständliche“ IT- und KI-Systeme zu entwickeln oder einzukaufen und einzuführen. Im Folgenden stellen wir diesen Prozess als einen Ansatz vor, um durch die Beteiligung von Mitarbeitenden und Betroffenen ihre Perspektive bei Entwicklungs- und Einführungsprozessen in Unternehmen einzubinden und somit insbesondere Grundrechtsrisiken zu vermindern und im Prozess der Technikgestaltung zu berücksichtigen („by-Design“) und damit eine datenschutzkonforme Entwicklung zu unterstützen. Abschließend geben wir Einblick in die damit verbundenen Herausforderungen der Umsetzung. Der Prozess bildet folglich einen Ansatzpunkt, Datenschutz-by-Design und DSFA gemeinsam zu denken, und so den Schutz der Grundrechte bei der Entwicklung und Einführung von Software ernst zu nehmen.

2 Der Fokus liegt auf den Konzepten der französischen und britischen Datenschutz-Aufsichtsbehörden Commission Nationale de l’Informatique et des Libertés (CNIL) und Information Commissioner’s Office (ICO), des deutschen Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom), und des wissenschaftlichen Konsortiums Forum Privatheit.

2. Datenschutz-Folgenabschätzungen ohne Betroffene?

Eine wichtige Methode des Datenschutzes für die Abwägung der Risiken der Datenverarbeitung für die Grundrechte der Betroffenen und die Wahl entsprechender Abhilfemaßnahmen ist die DSFA (Art. 35 Abs. 7 DSGVO). Sorgfältig durchgeführt, ermöglichen DSFA eine systematische Identifikation von Risiken und bieten somit eine wertvolle Basis für die strategische Weiterentwicklung und Verbesserung von Produkten und Dienstleistungen (Friedewald u.a. 2022, S. 439). Die DSFA beschränkt sich nicht nur auf die Risiken für Datenschutz und Privatheit, sondern umfasst nach Art. 35 Abs. 1 DSGVO allgemein „die Rechte und Freiheiten natürlicher Personen". Bei algorithmischen Systemen bezieht sich dies insbesondere auf Fragen von Gleichheit und Diskriminierungsfreiheit.

In Art. 35 Abs. 9 DSGVO ist gefordert, *gegebenenfalls* „den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung" einzuholen. Die Einbeziehung der Perspektive der Betroffenen leuchtet unmittelbar ein, allerdings wird diese nicht explizit vorgeschrieben und auch nicht ausgeführt, wie diese „Vertretung" konkret aussehen soll. Insgesamt wird für die DSFA in der DSGVO nur ein weiter Rahmen definiert, den die Datenverarbeitenden selbst ausfüllen müssen. Verschiedene Präzisierungen und methodische Frameworks werden aber von Datenschutzbehörden, Wissenschaftler:innen und Verbänden diskutiert. Die Auswahl der Methode und ihre Umsetzung obliegt aber der datenverarbeitenden Organisation (Friedewald et al. 2022, S. 425).

Martin u. a. (2020) analysieren unterschiedliche DSFA-Konzepte[3] und arbeiten unter anderem die verschiedenen Priorisierungen von Konsultationen heraus. Die formulierten Anforderungen reichen von geringen Vorgaben hinsichtlich der Einbindung „interessierter" Gruppen bis hin zu der Anforderung, Konsultationen von Betroffenen oder ihren Vertreter:innen grundsätzlich durchzuführen und nur in *begründeten Ausnahmefällen* auszulassen. Die Einbindung von Betroffenen bringt dabei verschiedene Herausforderungen mit sich, da diese sowohl technisch als auch juristisch und hinsichtlich der sozialen Implikationen keine Expert:innen sind, son-

3 Im referenzierten Artikel wurden DSFA-Verfahren der französischen und britischen Datenschutz-Aufsichtsbehörden Commission Nationale de l'Informatique et des Libertés (CNIL) und Information Commissioner's Office (ICO), des deutschen Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom), und eine aus dem wissenschaftlichen Konsortium Forum Privatheit heraus entwickelte Methode miteinander verglichen.

dern für die qualifizierte Bewertung von Risiken befähigt werden müssen (Friedewald u. a. 2022). Zudem bestehen häufig Interessenskonflikte, bspw. wenn Mitarbeiter:innen zwischen ihren Bedürfnissen und den Anforderungen ihrer Arbeitgeber:in abwägen müssen. Eine sorgfältige Auswahl der Konsultierten, und unter Umständen die Moderation durch externe Expert:innen erscheinen daher dringlich angeraten (vgl. Friedewald u. a. 2022, S. 440). Im Rahmen des KIDD-Projekts haben wir einen Prozess entwickelt, der aufzeigt, wie die Einbindung von Betroffenen in der Abwägung und Adressierung von Datenschutzrisiken ausgestaltet und moderiert werden kann. Im Folgenden wird dieser Prozess näher ausgeführt.

3. Privacy, Datenschutz und andere: Werte „by-Design"

Im KIDD-Projekt haben wir einen Prozess entwickelt, der - über eine reine Folgenabschätzung hinausgehend - ein Value-Sensitive-Design (VSD) ermöglicht und Betroffene partizipativ in die Technikentwicklung einbezieht. VSD zielt darauf ab, dass Menschen, egal ob sie als Individuen, Organisationen oder Gesellschaften agieren, die Werkzeuge und Technologien, die sie nutzen und mit denen sie interagieren, möglichst selbstbestimmt formen; so wie umgekehrt diese Werkzeuge und Technologien die menschliche Erfahrung und Gesellschaft formen (Davis und Nathan 2014). Dies gilt umso mehr bei der Gestaltung von Systemen, die versuchen, die Interaktion zwischen Mensch und Computer weiterzuentwickeln, und innovative Methoden wie lernende Algorithmen einsetzen. Demnach gehört zu unserem Verständnis eines Value-Sensitive-Design, Konsultationen nicht nur möglichst früh vor der tatsächlichen Einführung oder Fertigstellung einer Software durchzuführen, sondern die Software so weit wie möglich in ihrer Ausrichtung und Anwendung den Bedürfnissen der Betroffenen anzupassen.

Aus einer Vielzahl von methodischen VSD-Ansätzen (vgl. Friedman and Hendry 2019), die in verschiedenen Stadien eines Designprozesses angewendet werden können, sind für uns drei Komponenten als Säulen der methodologischen Überlegungen zentral (vgl. Friedman u. a. 2013):

1. *Interaktion*: Welche Menschen sind von dem zu entwickelnden System betroffen und welche Werte vertreten sie? Interagieren Stakeholder direkt oder sind sie indirekt vom System betroffen?
2. *Werte-Spannungen*: Unterschiedliche Werte können konsensual oder widerstrebend sein. Zudem sind menschliche Werte keine statischen Gebil-

de, sondern ändern sich dynamisch im Laufe der Zeit. Wichtig ist daher ein offener und konstruktiver Umgang mit den entstehenden Spannungen.

3. *Koevolution von Technologie und Sozialstruktur*: Mensch-Computer-Interaktion auf Systemebene ist keine Einbahnstraße. Der technische Gestaltungsraum kann nicht losgelöst von den sozialen Strukturen, in denen er entsteht, betrachtet werden. Damit wird deutlich, dass ein Gestaltungsprozess dieser Interaktion nicht nur in einem der beiden Gestaltungsräume stattfinden kann, sondern technische *und* soziale Systembestandteile je für sich und in ihrem Zusammenspiel betrachtet werden müssen.

Während VSD in der Praxis noch nicht für die Entwicklung von KI-Systemen eingesetzt oder moduliert wurde (Umbrello und Bellis 2018), finden sich im hier vorgestellten KIDD-Prozess, der die partizipative Einführung von KI-Systemen adressiert, die beschriebenen Merkmale des VSD-Ansatzes wieder. VSD ist jedoch keineswegs der einzige Ansatz zur Integration ethischer Werte in Entwicklungsprozessen. Wie Umbrello und Bellis haben wir uns für VSD entschieden, weil es - im Vergleich zu parallel oder früher entwickelten Ansätzen wie z. B. Values in Design (Nissenbaum 2001), Worth-Centered Design (Cockton 2009) oder Design for Values (Van den Hoven 2015) - in verschiedenen Anwendungsbereichen erfolgreich angewandt wurde, während einige neuere Ansätze wie z. B. IEEE Std 7000-2021 (IEEE 2021) zwar vielversprechend sind, aber noch keine breitere Anwendung und Erprobung erfahren haben.

4. KIDD: Ein holistischer Ansatz zur partizipativen Technikgestaltung

Ziel des KIDD-Prozesses ist es, Unternehmen und ihre Beschäftigten zu befähigen, die Ausgestaltung und Einführung von KI-Anwendungen und AES wirksam mitzugestalten und dabei sicherzustellen, dass neu eingeführte Systeme gemeinsam ausgehandelten ethischen Anforderungen entsprechen. Der KIDD-Prozess beruht dabei auf der Annahme, dass die Entwicklung von Softwareanwendungen, die weitreichende Implikationen für Unternehmen und Beschäftige haben, nicht alleine in der Hand von Entwickler:innen oder unternehmensinternen Entscheidungsträger:innen liegen soll, sondern die Nutzer:innen und Betroffenen selbst bei der Ausgestaltung des digitalen Systems umfänglich einzubinden sind.

Diese Einbindung wird im KIDD-Prozess durch die Einrichtung und Arbeit eines Gremiums ermöglicht, das im Projekt als „Panel der Vielfalt" (PdV) bezeichnet wird. Das PdV ist ein primär innerbetriebliches Gremium, das in seiner Zusammensetzung ein möglichst breites Spektrum an Perspektiven abbildet und frühzeitig und kontinuierlich im Software-Entwicklungs- und -Einführungsprozess beteiligt wird. Im Sinne der DSGVO kann das PdV als Gremium verstanden werden, in dem die Standpunkte und Perspektiven der Betroffenen bzw. ihrer „Vertreter:innen" zur Ausgestaltung der Software bzw. der beabsichtigten Verarbeitung der personenbezogenen Daten eingeholt werden (siehe Art. 35 Abs. 9 DSGVO). Im gesamten KIDD-Prozess finden sich eine Reihe an Elementen aus dem Value-Sensitive-Design wieder. Zu Beginn des Prozesses findet eine Stakeholder-Analyse statt, in der für das Projekt relevante Akteur:innen sowie deren Ziele und Einstellungen identifiziert werden, um sie adäquat im KIDD-Prozess und ggf. im PdV einbeziehen zu können. Zu einem frühen Zeitpunkt im Prozess der Softwareentwicklung bzw. -anschaffung unternimmt das PdV eine Folgenabschätzung, in der die Mitglieder des Gremiums auf Basis von persönlichen und technisch-organisationalen Erfahrungen und Werten „Hoffnungen und Befürchtungen" bezüglich der Einführung der Software-Anwendung formulieren. Die Folgenabschätzung im KIDD-Prozess ist dabei weniger formalisiert, zugleich aber inhaltlich breiter konzipiert als die DSFA, die als Nachweis-Instrument im Kontext der DSGVO vorgesehen ist. Die Mitglieder des PdV sammeln und diskutieren in diesem Schritt Chancen und Risiken, die sie mit der Einführung der Anwendung sowohl für die Organisation als auch für sie als individuell Betroffene assoziieren. Durch eine diverse Zusammensetzung des Gremiums soll sichergestellt werden, dass eine möglichst große Bandbreite an Verzerrungen und Diskriminierungspotenzialen in der Anwendung bereits im Vorfeld der Entwicklung und Einführung identifiziert und minimiert werden.

Aufbauend auf den Ergebnissen der Folgenabschätzung formuliert das PdV anschließend erste allgemeine Anforderungen, wie die Software ausgestaltet sein soll und welche organisationalen und strategischen Aspekte bei der Einführung der Anwendung berücksichtigt werden müssen. Im Rahmen des Adaptions- bzw. Entwicklungsprozesses der Anwendung tritt das PdV in einem nächsten Schritt in einen Aushandlungsprozess mit den Softwareentwickelnden hinsichtlich der ethischen und diskriminierungssensiblen Gestaltungsoptionen der Software und formuliert konkrete soft-

warebezogene Empfehlungen. Grundlage dafür ist die transparente und verständliche Darstellung dieser Gestaltungsoptionen durch die Softwareexpert:innen. Da eine fundierte Schulung des gesamten PdV in technischen Spezialfragen nicht möglich ist, bedarf es im Aushandlungsprozess mit den Softwareentwickelnden und bei der Formulierung konkreter Empfehlungen einer geschulten KIDD-Moderator:in, die den KIDD-Prozess operativ durchführt und moderiert. Hierbei sieht der KIDD-Ansatz jedoch nicht notwendigerweise den Einsatz eines externen Facilitators vor. Vielmehr wird davon ausgegangen, dass interne Mitarbeitende befähigt werden, den Prozess zu moderieren.[4] In diesem Aspekt weist der KIDD-Prozess Parallelen zum Ansatz des Collaboration Engineering auf, in dem ebenfalls Anwender:innen ermächtigt werden, wiederholbare Kollaborationsprozesse zum Beispiel im Kontext der Gestaltung von Datenschutzprozessen eigenständig durchzuführen (siehe Hornung et al. 2022). Im KIDD-Prozess kann darüber hinaus jedoch die Unterstützung durch eine KI-Expert:in sinnvoll sein, die technisch komplexe Sachverhalte für das PdV allgemeinverständlich darstellen und bei der Formulierung softwarebezogener Empfehlungen unterstützen, aber auch kritische Nachfragen hinsichtlich der Gestaltung der Software stellen kann.

Die Praxis zeigt, dass bei der Formulierung der Anforderungen oft sehr unterschiedliche Werte und Vorstellungen gegeneinander abgewogen werden müssen. Diese Diskussions- und Entscheidungsprozesse müssen dokumentiert und im Unternehmen transparent kommuniziert werden, um einen konstruktiven und für alle nachvollziehbaren Diskurs zu ermöglichen. Schließlich wird vor Inbetriebnahme der Anwendung gemeinsam mit dem PdV abgestimmt, auf welche Weise die kontinuierliche Einhaltung der ethischen und diskriminierungssensiblen Anforderungen sichergestellt werden kann, und es werden die dafür nötigen Monitoringmaßnahmen definiert.

Um sicherzustellen, dass der KIDD-Prozess in Unternehmen von den relevanten Akteur:innen reibungslos umgesetzt werden kann und eine hohe Erfolgsaussicht auf Anerkennung hat, wurden im KIDD-Prozess konkrete Anknüpfungspunkte und Schnittstellen zu etablierten Entwicklungs- und Einführungsprozessen von IT-Anwendungen herausgearbeitet. Der gemeinsame Austausch zwischen Entwickler:innen und Betroffenen ist herausfordernd, da die verschiedenen Perspektiven einander verständlich

4 Eine entsprechende Schulung wurde ebenfalls im KIDD-Projekt entwickelt.

gemacht werden müssen, bringt aber einen konstruktiven Diskurs zutage, der die Software verbessern kann, und gleichzeitig Akzeptanz stiftet. Generell kann man feststellen, dass die Betroffenen sehr schnell die essentiellen Fragen für eine grundrechtssensible, datenschutzfreundliche und damit akzeptanzfähige Softwaregestaltung stellen, und dabei auch den Nutzen der Software für Mitarbeitende und Unternehmen mitdenken.[5]

5. Fazit

In der Praxis verläuft die Verknüpfung von Software-Einführungsprozess und die Beteiligung der verschiedenen Stakeholder und der von der Datenverarbeitung direkt Betroffenen nicht immer reibungslos. Hier sind noch Anpassungsschritte des KIDD-Prozessmodells notwendig, die in der praktischen Auseinandersetzung und Anwendung erarbeitet werden. Die Erfahrungen aus den Experimentierräumen, in denen der KIDD-Prozess in enger Zusammenarbeit mit Unternehmen entwickelt und angewandt wurde, macht bereits deutlich, dass die gute Vorbereitung und präzise Planung des Beteiligungsprozesses im Unternehmen unerlässlich sind, um einen für alle Beteiligten nutzbringenden Austausch zu etablieren: in diesem Fall zwischen dem Panel der Vielfalt als Betroffenengremium, der Managementebene und den Software-Entwickelnden. Die erfolgreiche Umsetzung des KIDD-Prozesses bedarf der Definierung klarer Zielsetzungen, Rahmenbedingungen und Aufgabenstellungen, welche offen und transparent kommuniziert werden müssen.

Partizipative Technikgestaltung als Methode zur Verwirklichung eines Value-Sensitive-Design ist also kein Selbstläufer, sondern erfordert ernsthafte und sorgfältig organisierte Auseinandersetzungen auf verschiedenen Unternehmensebenen. Essentiell ist dabei, vorab auf den verschiedenen Ebenen das Problembewusstsein zu stärken und die Diskussionen an den entscheidenden Stellen sensibel zu moderieren. Richtig angewendet, kann der skizzierte Beteiligungsprozess sowohl eine aussagekräftige DSFA unterstützen, als auch ein Datenschutz-by-Design-Prozess in der Entwicklung etablieren. Einerseits wird im entwickelten Prozess lange vor der tatsächlichen Einführung einer Software ein Raum geschaffen, in dem Betroffene Nutzen und Risiken kritisch reflektieren können; das gegründete Panel

5 Ausführliche Berichte über die verschiedenen Fallstudien finden sich in Kürze auf der Website des Projekts: kidd-prozess.de.

der Vielfalt begleitet den Einführungsprozess von Anfang an. Die Gestaltung der Software (Auswahl, Konfiguration, Entwicklung) wird somit im Sinne eines Datenschutz-by-Design von Anfang an auch im Sinne der Nicht-Diskriminierung und dem Schutz der Grundrechte der Betroffenen gestaltet. Andererseits findet in dieser begleitenden kritischen Diskussion ein sorgfältiger Abwägungsprozess statt, der die „Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten" (Art. 35, Abs. 1, DSGVO) beinhaltet, und durch entsprechende Dokumentation belegt werden kann. Der beschriebene KIDD-Prozess stellt einen empirisch erarbeiteten und aus der organisationalen Praxis heraus entwickelten Ansatz dar, um künftig Unternehmen dabei zu unterstützen, Risiken für die Grundrechte abzumildern und Transparenz und Mitbestimmung für die Betroffenen zu fördern.

Literatur

Cockton, Gilbert (2009): Getting there: six meta-principles and interaction design. In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09). Association for Computing Machinery*. https://doi.org/10.1145/1518701.1519041

Davis, Janet und Lisa P. Nathan (2013): Value Sensitive Design: Applications, Adaptations, and Critiques. In: Jeroen van den Hoven, Pieter E. Vermaas und Ibo van de Poel (Hrsg.): *Handbook of Ethics, Values, and Technological Design*. Dordrecht: Springer, S. 1–26. doi: 10.1007/978-94-007-6970-0_3

Friedewald, Michael, Felix Bieker, Hannah Obersteller, Maxi Nebel, Nicholas Martin und Marit Hansen (2018): Datenschutz-Folgenabschätzung. Ein Werkzeug für einen besseren Datenschutz. White Paper. Karlsruhe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt.

Friedewald, Michael, Ina Schiering, Nicholas Martin und Dara Hallinan (2022): Data Protection Impact Assessments in Practice. In: *Computer Security. ESORICS 2021 International Workshops*. Lecture Notes in Computer Science, Bd. 13106. Cham: Springer International Publishing, S. 424–43. doi: 10.1007/978-3-030-95484-0_25

Friedman, Batya und David G. Hendry (2019): *Value Sensitive Design: Shaping Technology with Moral Imagination*. The MIT Press.

Friedman, Batya, Peter H. Kahn, Alan Borning und Alina Huldtgren (2013): Value Sensitive Design and Information Systems. In: Neelke Doorn, Daan Schuurbiers, Ibo van de Poel, und Michael E. Gorman (Hrsg.): *Early Engagement and New Technologies: Opening up the Laboratory*. Dordrecht: Springer Netherlands, S. 55–95. doi: 10.1007/978-94-007-7844-3_4

Hornung, Gerrit, Matthias Söllner, Jan-Phillip Stroscher und Eva-Maria Zahn (2022). Kollaboration im Datenschutz: Collaboration Engineering als Instrument zur partizipativen und nachhaltigen Gestaltung von Datenschutzprozessen. *Datenschutz und Datensicherheit (DuD)*, 46(6), 384-389. doi: 10.1007/s11623-022-1625-4

IEEE (2021): IEEE Standard Model Process for Addressing Ethical Concerns during System Design. IEEE Std 7000-2021. doi: 10.1109/IEEESTD.2021.9536679.

Martin, Nicholas, Ina Schiering und Michael Friedewald (2020): Methoden der Datenschutz-Folgenabschätzung: Welche Unterschiede weisen die verschiedenen methodischen Ansätze auf? *Datenschutz und Datensicherheit (DuD)*, 44(3), S. 154–60. doi: 10.1007/s11623-020-1242-z

Nissenbaum, Helen (2001): How computer systems embody values, *IEEE Computer*, 34(3), S. 120-119. doi: 10.1109/2.910905.

Van den Hoven, Jeroen, Pieter E. Vermaas und Ibo van de Poel (2015): *Handbook of Ethics, Values, and Technological Design: Sources, Theory, Values and Application Domains*. Dordrecht: Springer. https://doi.org/10.1007/978-94-007-6970-0_40

Wright, David und Paul de Hert (Hrsg.) (2012): *Privacy Impact Assessment*. Dordrecht: Springer.

Teil II: Fairer Wettbewerb in der Datenökonomie

Datenschutz, Wettbewerbsrecht und Verbraucherschutz: Zur Notwendigkeit der Lösung von Marktversagensproblemen

Wolfgang Kerber und Louisa Specht-Riemenschneider

1. Einleitung

Der Beitrag beruht auf den folgenden drei Grundthesen, die in den folgenden Abschnitten kurz genauer erklärt und begründet werden:

(1) Das Individuum kann aufgrund diverser Marktversagensprobleme auf Datenmärkten nicht selbstbestimmt in Bezug auf den Umgang mit personenbezogenen Daten entscheiden.
(2) Für die Funktionsfähigkeit des Datenschutzrechts müssen diese Marktversagensprobleme miteinbezogen werden. Insofern muss das Datenschutzrecht auch neu gedacht werden.
(3) Datenschutzrecht kann alleine diese Probleme nicht lösen. Insofern ist eine enge Koordinierung mit anderen Politiken wie insbesondere dem Wettbewerbsrecht und Verbraucherschutzrecht notwendig.

2. Marktversagen auf Datenmärkten

Durch die Möglichkeit, im Rahmen der Privatautonomie in die private Nutzung personenbezogener Daten einzuwilligen, entstehen Datenmärkte. Allerdings leiden diese Märkte unter gravierenden Marktversagensproblemen, die dazu führen, dass oft nur eine formelle Privatautonomie existiert, aber eine echte Selbstbestimmung (materiale Privatautonomie) nicht gewährleistet ist. Die ökonomische Marktversagenstheorie, die eine Anzahl verschiedener Arten des Marktversagens unterscheidet, kann wesentlich bei der Analyse dieser Probleme mangelnder Selbstbestimmung auf Märkten für personenbezogene Daten helfen.

1.1 Informationsasymmetrien, Transaktionskosten und Rationalitätsprobleme

Betroffene Personen können oft die Vorteile und (Privatheits-)Risiken der Weitergabe von personenbezogenen Daten nicht einschätzen. Zentrale Ursachen sind zu hohe Informationskosten, nicht ausreichende Informationspflichten im Datenschutzrecht sowie der oft gleichzeitig auftretende „information overload", mit der Folge eines Abbruchs der Informationsverarbeitung bei den Datensubjekten.[1] Aus der Verhaltensökonomie ist auch bekannt, dass Menschen oft systematische Entscheidungsfehler durch „behavioral biases" machen. Diese Schwächen können zunehmend von digitalen Plattformen zur Verhaltensmanipulation bei der Einwilligung in die Nutzung von personenbezogenen Daten über das Design von Benutzeroberflächen („dark pattern") ausgenutzt werden.[2] Da alle Individuen in diesem Sinne vulnerabel in der digitalen Welt sind, führen Informations(asymmetrie)probleme, zu hohe Transaktionskosten und Rationalitätsprobleme auch aus ökonomischer Sicht zu einem gravierenden Versagen von Märkten für personenbezogene Daten. Ein möglicher Ansatz zu ihrer Lösung stellen Personal Information Management Systems (PIMS) dar, für die aber ein weitreichender ermöglichender Rechtsrahmen erforderlich ist.[3]

1.2 Wettbewerbsprobleme

Digitale Plattformen der großen Tech-Firmen (Google, Meta, Amazon etc.) verfügen über sehr große Marktmacht, die ihnen auch die Sammlung sehr großer Mengen personenbezogener Daten ermöglicht. Hiermit können sehr detaillierte Verbraucher:innen-Profile für zielgerichtete Werbung entwickelt werden, die sich negativ auf die Privatsphäre der Datensubjekte auswirken können. Aus ökonomischer Sicht kann das Fehlen von wirksamen Wettbewerb durch diese Marktmacht zu einer exzessiven Sammlung von personenbezogenen Daten führen, da die Datensubjekte oft keine realisti-

1 *Martinek*, in: Grundmann (Hrsg.), Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts, 2000, 511 (524); vgl. dazu auch; *Specht*, Diktat der Technik, 2019, 168.

2 Auch wenn die Anzahl solcher Designelemente bisher empirisch nur schwer nachvollzogen werden kann, vgl. *Weinzierl*, NVwZ-Extra 2020, 1 (3) m. w. N.; sowie *Rieger/Sinders*, Dark Patterns, Mai 2020, 22 m. w. N.

3 *Specht-Riemenschneider/Kerber*, Datentreuhänder, 2021, 33 f.

schen Ausweichmöglichkeiten bezüglich der Dienstleistungen solcher Plattformen haben und insofern die Bedingungen dieser Plattformen akzeptieren müssen. Das Bundeskartellamt hat mit seinem Facebook-Fall (2019) die Bündelung der Einwilligung zur Nutzung personenbezogener Daten aus verschiedenen Quellen als missbräuchliches Verhalten eines marktbeherrschenden Unternehmen verboten.[4] Es handelt sich dabei weltweit um den ersten Fall, in dem Datenschutzrecht von einer Wettbewerbsbehörde explizit in einem Fall von Marktmachtmissbrauch bei der Anwendung von Wettbewerbsrecht einbezogen worden ist.

1.3 Negative und positive Datenexternalitäten

Marktversagensprobleme treten auch auf, wenn Auswirkungen eines Verhaltens auf andere bei Entscheidungen nicht einbezogen werden. Dieses Problem ist vor allem bei sogenannten Umweltexternalitäten bekannt, wenn die negativen Wirkungen von umweltschädlichen Produkten von den Verursachern nicht ausreichend berücksichtigt werden und folglich Märkte zu einem zu hohen Niveau von Umweltschäden führen.[5] Da sich auch die Weitergabe von personenbezogenen Daten einer Person A negativ auf die Privatsphäre einer anderen Person B auswirken kann (bspw. durch ähnlichkeitsbasierte Inferenz[6]), kann es in vergleichbarer Form zu sogenannten negativen Datenexternalitäten kommen, weil solche Wirkungen normalerweise nicht von der Person A bei ihrer Einwilligung berücksichtigt werden.[7] Solche negativen Datenexternalitäten können sich negativ auf das Datenschutzniveau auswirken, auch weil sie die Anreize der Datensubjekte, ihre eigenen Daten zu schützen, reduzieren. Dies ist auch direkt von ökonomischer Forschung bestätigt worden.[8]

Umgekehrt aber ist es auch wohlbekannt, dass die Nutzung personenbezogener Daten einer Person sich auch positiv auf den Nutzen anderer Personen oder der gesamten Gesellschaft auswirken kann (wie bspw. bei

4 *Bundeskartellamt*, B6-22/16 vom 6.2.2019; vgl. dazu *Podzun*, GRUR 2020, 1268; *Mackenrodt/ Wiedemann*, ZUM 2021, 89; *Kerber/ Zolna*, Eur. J. Law Econ., 2022, 217.

5 *Fritsch*, Marktversagen und Wirtschaftspolitik, 2018, 84 ff.

6 *Hacker*, Datenprivatrecht, 2020, 67 m.w.N.; *Palka*, Buffalo Law Review 2020, 559.

7 So etwa *Roßnagel* et al., Modernisierung des Datenschutzrechts, 2001, 37 f.

8 *Choi* et al., Journal of Public Economics 2019, 113; vgl. in diesem Zusammenhang auch die Arbeit von *Acemoglu et al*, American Economic Journal 2022, 218; dies erklärt womöglich das sog. "privacy paradoxon", vgl. *Martens et al*., Business-to-Business data sharing 2020, 17 f.

der Nutzung von Patientendaten für die medizinische Forschung[9]). Ökonomisch handelt es sich um positive Datenexternalitäten, bei denen dann jedoch das Problem entsteht, dass die Datensubjekte bei ihrem individuellen Kosten-Nutzen-Kalkül in Bezug auf ihre datenschutzrechtliche Einwilligung solche positiven Wirkungen auf Dritte oft nicht ausreichend miteinbeziehen. Dies führt dazu, dass aus einer gesamtgesellschaftlichen Sicht zu wenige Daten verfügbar gemacht werden, was sich negativ auf Forschung und Innovation auswirken kann. Staatliche Datensammlungen wie z. B. Medizindatenregister sind ein Teil der Lösung des Problems, sind allein aber nicht ausreichend.

Aus ökonomischer Sicht werfen sowohl negative als auch positive Datenexternalitäten erhebliche Grundsatzfragen auf, da sie das Prinzip individueller Selbstbestimmung bzgl. der Nutzung der eigenen personenbezogenen Daten in Frage stellen. Beim Vorhandensein von Datenexternalitäten können individuelle Entscheidungen zu falschen Lösungen aus gesamtgesellschaftlicher Sicht führen. Mögliche Lösungen sind:

1. Zur Verringerung von negativen Datenexternalitäten können zahlreiche datenschutzrechtliche Vorschriften zwingend ausgestaltet werden und absolute Verbote besonders gefährlicher Datenverarbeitungen normiert werden. Auch eine Beschränkung der Einwilligungsmöglichkeit in bestimmten Fällen fällt hierunter.[10]
2. Umgekehrt können für eine bessere Berücksichtigung positiver Datenexternalitäten unter spezifischen Voraussetzungen (bspw. in einer Datentreuhand) auch allgemeine Erlaubnistatbestände für bestimmte Datenverarbeitungen eingeführt werden (bspw. für Forschungszwecke).

3. Zusammenspiel zwischen Datenschutz, Wettbewerbsrecht und Verbraucherschutz

Im letzten Abschnitt haben wir gesehen, dass durch die Privatautonomie bei datenschutzrechtlichen Einwilligungen Datenmärkte entstehen, auf denen gleichzeitig mehrere unterschiedliche Marktversagensprobleme auftreten können. Aus ökonomischer Sicht gibt es üblicherweise eine Arbeitsteilung zwischen verschiedenen Politiken (oder Rechtsgebieten), um solche

9 *Specht-Riemenschneider/Radbruch*, Deutsches Ärzteblatt 2021, A 1358.

10 Zu letzterem Aspekt vgl. *Roßnagel/Geminn*, Datenschutz-Grundverordnung verbessern, 2020.

Marktversagensprobleme zu lösen oder zumindest ihre negativen Auswirkungen zu vermindern. Während die Wettbewerbspolitik die Aufgabe hat, sich um die Lösung von Problemen wettbewerbsbeeinträchtigenden Verhaltens einzelner Marktakteure–zu kümmern, ist es die Aufgabe der Verbraucherpolitik, sich um die Lösung von Informations(asymmetrie)problemen und Rationalitätsproblemen zu bemühen. Auch wenn das Datenschutzrecht hier nicht so eindeutig zugeordnet werden kann, so hat es doch starke Züge eines Verbraucherschutzrechts in Bezug auf personenbezogene Daten von Individuen.

In unserer Studie "Synergies between data protection law and competition law" (Kerber/Specht-Riemenschneider 2021) für den Verbraucherzentrale Bundesverband (vzbv) haben wir uns vertieft mit der Beziehung zwischen Datenschutzrecht und Wettbewerbsrecht in Bezug auf die Macht der großen Tech-Firmen auf digitalen Plattformen beschäftigt. Hier tritt das Problem auf, dass gleichzeitig ein sehr großes Marktmachtproblem vorliegt und erhebliche Informations- und Rationalitätsprobleme in Bezug auf die Sammlung und Verarbeitung personenbezogener Daten auftreten. Dies bedeutet, dass eine Kombination von Marktmacht und Informations-(und Manipulations-)Macht besteht, die zu der sehr umfangreichen Sammlung von personenbezogenen Daten durch diese Tech-Firmen führt. Dies kann zu stark negativen Wirkungen sowohl auf den Wettbewerb als auch auf die Privatsphäre führen. Insofern ist diese Macht der Tech-Firmen sowohl für die Wettbewerbspolitik als auch für das Datenschutzrecht von zentraler Bedeutung.

Die gleichzeitige Existenz dieser beiden Arten von Marktversagen in Bezug auf personenbezogene Daten führt aus ökonomischer Sicht dazu, dass sich Wettbewerbspolitik gegenüber diesen Tech-Firmen nicht nur auf den Wettbewerb auswirkt, sondern auch auf den Datenschutz, ebenso wie umgekehrt die Anwendung des Datenschutzrechts auf die Sammlung solcher Daten auch Auswirkungen auf den Wettbewerb haben kann. Wettbewerbspolitik und Datenschutzrecht stehen damit in einer komplexen Beziehung zueinander, mit vielfältigen Interaktionseffekten zwischen beiden Politiken. Durch die zentrale Rolle von personenbezogenen Daten auf digitalen Plattformmärkten können Wettbewerbsrecht und Datenschutzrecht nicht mehr als zwei getrennte Rechtsgebiete angesehen werden, die unabhängig voneinander angewendet werden sollten. Vielmehr müssen auch die Interaktionen und die Wirkungen des kombinierten Einsatzes beider Rechtsgebiete berücksichtigt werden, zumindest in Bezug auf die Gefahren, die von den großen digitalen Plattformen auf Wettbewerb und den Schutz der Privat-

sphäre ausgehen. Insofern war es eine zentrale Aufgabe dieser vzbv-Studie, solche Interaktionseffekte genauer zu untersuchen und dadurch einerseits mögliche Konflikte, andererseits aber auch die Möglichkeiten von Synergien zwischen Datenschutzrecht und Wettbewerbsrecht herauszuarbeiten. Dies impliziert vor allem auch die Frage, wie in Bezug auf die großen digitalen Plattformen gleichzeitig sowohl mehr Datenschutz als auch mehr Wettbewerb erreicht werden können.

Von zentraler Bedeutung sind hierfür vor allem auch konzeptionelle Weiterentwicklungen im Wettbewerbsrecht und im Datenschutzrecht. Ein wichtiges Problem ist, dass das Datenschutzrecht nicht über die Expertise und die Instrumente verfügt, um gegen negative Wirkungen auf die Privatsphäre vorzugehen, die durch Wettbewerbsprobleme verursacht werden. Zwar gibt es eine zunehmende Diskussion im Datenschutzrecht, ob durch das Machtungleichgewicht, das durch eine marktbeherrschende Stellung (wie im Facebook-Fall des Bundeskartellamts) entsteht, noch die „Freiwilligkeit der Einwilligung" gegeben ist. Auch wenn der risikobasierte Ansatz des Datenschutzrechts im Prinzip Möglichkeiten eröffnet, Marktmacht als Kriterium im Datenschutzrecht einzubeziehen, so steht diese Diskussion noch ganz am Anfang und ist noch weit von der aktuellen Datenschutzpraxis entfernt, die zumindest im Grundsatz gerade nicht zwischen verschiedenen Gruppen von Unternehmen unterscheiden möchte.

Insofern wird es notwendig sein, dass das Wettbewerbsrecht helfen muss, die negativen Effekte von Wettbewerbsproblemen, sei es durch marktbeherrschende Stellungen oder durch Fusionen, auf den Datenschutz zu bekämpfen. Der Facebook-Fall des Bundeskartellamts hat hier einen großen Beitrag geleistet. Allerdings sollte man auch klar die Probleme und Grenzen sehen, die das Wettbewerbsrecht hat, um Wirkungen auf die Privatsphäre in ihre konkrete Anwendungspraxis einzubeziehen. So wurde innerhalb der wettbewerbsrechtlichen Diskussion vehement kritisiert, dass das Wettbewerbsrecht den Wettbewerb schützen soll und nicht die Privatsphäre. Allerdings ist der Schutz der Privatsphäre aus ökonomischer Sicht durchaus auch mit dem Ziel der Konsumentenwohlfahrt kompatibel. Zumindest in der internationalen wettbewerbsrechtlichen Diskussion ist inzwischen eine größere Offenheit darüber entstanden, wie man Privatsphäre und Datenschutz besser bei der Anwendung des Wettbewerbsrechts einbeziehen könnte. Eine stärkere konkrete Praxis muss sich aber erst entwickeln. Hier müssen auch methodisch neue Wege beschritten werden.

In der EU wurde durch die Verabschiedung des „Digital Markets Act" (DMA) als zusätzliche Ex-ante-Regulierung von Gatekeeper-Plattformen

ein großer innovativer Schritt gemacht, um besser die Marktmacht von digitalen Plattformen der großen Tech-Konzerne zu bekämpfen, als dies mit der traditionellen Missbrauchsaufsicht marktbeherrschender Unternehmen (Art. 102 TFEU) möglich war. Schützt der DMA auch besser die Privatsphäre von Datensubjekten gegenüber solchen Gatekeepern? Dies ist leider sehr zweifelhaft, da der DMA nach weitverbreiteter Meinung doch primär nur wettbewerbspolitisch verstanden wird. Zwar enthält er mit der Verpflichtung in Art. 5(2) DMA eine Vorschrift, die auf der Grundidee des Verbots einer Kombination von personenbezogenen Daten aus verschiedenen Quellen (wie im Facebook-Fall des Bundeskartellamts) aufbaut. Allerdings kann dies auch hier durch das Herbeiführen einer expliziten Einwilligung wieder umgangen werden, ohne dass klar ist, ob die Marktversagensprobleme ausreichend gelöst werden. In unserer vzbv-Studie haben wir deshalb gefordert, dass der DMA auf der Basis seines „Fairness"-Ziels wesentlich expliziter auch datenschutzrechtliche und verbraucherpolitische Zielsetzungen verfolgen sollte, d.h. dass die asymmetrische Regulierung in Bezug auf Gatekeeper sich nicht nur auf den Wettbewerb, sondern auch auf den Daten- und Verbraucherschutz beziehen sollte.

In seiner „Preliminary opinion" hat der European Data Protection Supervisor bereits 2014 die Notwendigkeit einer Analyse des Zusammenspiels zwischen Datenschutzrecht, Wettbewerbsrecht und Verbraucherschutz klar herausgearbeitet und einen stärker integrativen Ansatz zwischen allen drei Politiken gefordert. Weder das Datenschutzrecht, das Wettbewerbsrecht, oder das Verbraucherrecht sind alleine in der Lage, die Herausforderungen durch die gravierenden Marktversagensprobleme auf Märkten für personenbezogene Daten zu lösen. Insofern ist – auch aus ökonomischer Perspektive – eine stärkere Koordinierung und Zusammenarbeit zwischen diesen Politiken und damit eine Überwindung des traditionellen Denkens in getrennten „Politik-Silos" erforderlich.

Literatur

Acemoglu, Daron; Ali Makhdoumi; Azarakhsh Malekian und Asu Ozdaglar (2022): Too Much Data: Prices and Inefficiencies in Data Markets. *American Economic Journal: Microeconomics*, 14 (4), S. 218-56. doi: 10.1257/mic.20200200.

Bundeskartellamt (6.3.2019): Beschluss B6-22/16. URL: https://www.bundeskartellamt.de/SharedDocs/Entscheidung/DE/Entscheidungen/Missbrauchsaufsicht/2019/B6-22-16.pdf;jsessionid=FD8C3A4FF87608C4DFB15F99E5AB7BF0.1_cid390?__blob=publicationFile&v=8 (besucht am 03. 04. 2023).

Choi, Jay P.; Jeon, Doh S. und Kim, Byung C. (2019): Privacy and personal data collection with information externalities. *Journal of Public Economics*, 173, S. 113-124. doi: 10.1016/j.jpubeco.2019.02.001.

Frisch, Michael (2018): *Marktversagen und Wirtschaftspolitik: Mikroökonomische Grundlagen staatlichen Handelns*. 10. Auflage. München: Vahlen.

Hacker, Philipp (2020): *Datenprivatrecht: Neue Technologien im Spannungsfeld von Datenschutzrecht und BGB*. Tübingen: Mohr Siebeck.

Kerber, Wolfgang (2022): Taming Tech Giants: The Neglected Interplay Between Competition Law and Data Protection (Privacy) Law. *The Antitrust Bulletin* 67(2), S. 280-301. doi 10.1177/0003603X221084145.

Kerber, Wolfgang; Specht-Riemenschneider, Louisa (2021): Synergies Between Data Protection Law and Competition Law. Studie für Verbraucherzentrale Bundesverband (vzbv). Berlin: vzbv. URL: https://www.vzbv.de/sites/default/files/2021-11/21-11-10_Kerber_Specht-Riemenschneider_Study_Synergies_Betwen_Data%20protection_and_Competition_Law.pdf (besucht am 03. 04. 2023).

Kerber, Wolfgang und Zolna, Karsten (2022): The German Facebook Case: The Law and Economics of the Relationship between Competition and Data Protection Law. *European Journal of Law and Economics* 54(2), S. 217-250. DOI: 10.1007/s10657-022-09727-8.

Mackenrodt, Mark-Oliver und Wiedemann, Klaus (2021): Zur kartellrechtlichen Bewertung der Datenverarbeitung durch Facebook und ihrer normativen Kohärenz. *Zeitschrift für Urheber- und Medienrecht ZUM*, S. 89-103.

Martens, Bertin; de Streel, Alexandre; Graef, Inge; Tombal, Thomas und Duch-Brown, Néstor (2020): *Business-to-Business data sharing: An economic and legal analysis*. JRC Technical Report JRC121336. Seville: European Commission. URL: https://ec.europa.eu/jrc/sites/default/files/jrc121336.pdt (besucht am 03. 04. 2023).

Martinek, Michael (2000): Unsystematische Überregulierung und kontraintentionale Effekte im europäischen Verbraucherschutzrecht, oder: Weniger wäre mehr. In: Grundmann, Stefan (Hrsg.): *Systembildung und Systemlücken in Kerngebieten des Europäischen Privatrechts: Gesellschaftsrecht, Arbeitsrecht, Schuldvertragsrecht*. Tübingen: Mohr Siebeck, S. 511 – 557.

Pałka, Przemysław (2020): Data Management Law for the 2020s: The Lost Origins and the New Needs. *Buffalo Law Review*, 68(2), S. 559-640

Podszun, Rupprecht (2020): Der Verbraucher als Marktakteur: Kartellrecht und Datenschutz in der „Facebook"-Entscheidung des BGH. *Gewerblicher Rechtsschutz und Urheberrecht GRUR*, 122(12), S. 1268-1276.

Rieger, Sebastian und Sinders, Caroline (2020): *Dark Patterns: Design mit gesellschaftlichen Nebenwirkungen: Wie Regierungen und Regulierungsbehörden auf die Verbreitung problematischer Benutzeroberflächen reagieren können*. Berlin: Stiftung Neue Verantwortung. URL: https://www.stiftung-nv.de/sites/default/files/dark.patterns.pdf (besucht am 03. 04. 2023).

Roßnagel, Alexander und Geminn, Christian (2020): *Datenschutz-Grundverordnung verbessern: Änderungsvorschläge aus Verbrauchersicht*. Baden-Baden: Nomos.

Roßnagel, Alexander; Pfitzmann, Andreas und Garstka, Hansjürgen (2001). *Modernisierung des Datenschutzrechts*. Gutachten im Auftrag des Bundesministeriums des Innern. Berlin.

Specht-Riemenschneider, Louisa (2023): Datenschutzrecht als Verbraucherschutzrecht – Zum Erfordernis der Behebung vielfältiger Marktversagen auf Datenmärkten durch Anpassungen des materiellen Datenschutzrechts. In: Buchner, Benedikt und Petri, Thomas (Hrsg.) *Informationelle Menschenrechte und digitale Gesellschaft*. Tübingen: Mohr Siebeck, S. 77-98.

Specht-Riemenschneider, Louisa und Radbruch, Alexander (2021): Datennutzung und -schutz in der Medizin: Forschung braucht Daten. *Deutsches Ärzteblatt*, 118(27-28), S. A-1358.

Specht-Riemenschneider, Louisa und Kerber, Wolfgang (2021). *Datentreuhänder – Ein problemlösungorientierter Ansatz*. Berlin: Konrad-Adenauer-Stiftung. URL: https://www.kas.de/documents/252038/16166715/Designing+ Data+Trustees+-+A+Purpose-Based+Approach.pdf/ffadcb36-1377-4511-6e3c-0e32tc727a4d (besucht am 03. 04. 2023).

Specht, Louisa (2019): *Diktat der Technik: Regulierungskonzepte technischer Vertragsinhaltsgestaltung am Beispiel von Bürgerlichem Recht und Urheberrecht*. Baden-Baden: Nomos.

Weinzierl, Quirin (2020): Dark Patterns als Herausforderung für das Recht: Rechtlicher Schutz vor der Ausnutzung von Verhaltensanomalien. *Neue Zeitschrift für Verwaltungsrecht NVwZ*, 39(15).

Targeting Reputation – Publication of Compliance as a Regulatory Concept in Comparative Data Protection Law

Sebastian J. Kasper and Timo Hoffmann

Abstract

In addition to direct sanctions, for example, in the form of levying fines, indirect measures like reputation-related measures might have a deterrent effect on companies. Particularly in data-driven industries, trust and having a good reputation seem to be important to acquire new customers and prevail over competitors. Therefore, it is not surprising that States may target companies' reputations to incentivise or compel them to comply with regulatory standards. This comparative paper shows that reputation-related measures are a common phenomenon across various data privacy legislations. However, this paper also demonstrates that the theory underlying reputation-related measures reveals many uncertainties when assessing the efficacy of those measures. By combining reputational literature, findings from the field of behavioural economics, and a comparative analysis, we further introduce structural elements for a typology to allow for future comparative assessments of regulatory concepts that target reputation.

1. Introduction

Legislation on data protection and informational privacy has become a global phenomenon,[1] with 157 countries having data privacy laws on their books as of mid-2022.[2] While laws aiming to protect individuals' personal information have existed for quite some time, data protection has steadily become more prominent. Particularly, the high fines that may be imposed under data protection laws, such as the European Union's (EU's) General

1 See Moritz Hennemann, 'Wettbewerb der Datenschutzrechtsordnungen' (2020) 84(4) RabelsZ 864.

2 Graham Greenleaf, 'Now 157 countries: Twelve data privacy laws in 2021/22' [2022] PrivL&BusIntlR 3.

Data Protection Regulation (GDPR)[3] or the Brazilian General Personal Data Protection Law (LGPD)[4] have attracted attention.[5] However, many companies processing personal data fear not only (severe) monetary sanctions, but also the adverse effect on their reputation should the public become aware that they have violated data protection law[6].

We aim to identify and categorise regulatory instruments that impact companies' reputations directly or indirectly, in the context of data protection and informational privacy.

In an effort to account for the discussion and advancement in decolonial approaches to comparative law,[7] we attempt to reduce bias[8] by applying three strategies: Firstly, we employ a broad understanding of reputation-related measures in light of the concept of legal pluralism.[9] Secondly, we build our categorisation on an abstract typology which is derived from behavioural economics. Thirdly, we understand the various jurisdictions of our comparison as starting points to learn about different approaches to regulation, without being able to apply an all-encompassing comparison in this paper.[10]

Consequently, this article is structured as follows: We outline a theory of reputation (2), based on which we develop a typology for reputation-related measures (3). Thereafter, we compile a collection of regulatory

3 Article 83(4) and (5) Regulation (EU) 2016/679, OJ 2016 L 119/1.

4 Article 52(2) Lei Geral de Proteção de Dados Pessoais (*transl. General Law for the Protection of Personal Data*), Law No. 13.709 of 14 August 2018.

5 As an example, see BBC News, 'Three years of GDPR: the biggest fines so far' *BBC News* (24 May 2021) <https://www.bbc.com/news/technology-57011639> accessed 4 August 2023.

6 For a comprehensive analysis of reputational effects and countermeasures in the context of data breaches, see Kholekile L Gwebu, Jing Wang and Li Wang, 'The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management' (2018) 35(2) JMIS 683.

7 See only Lena Salaymeh and Ralf Michaels, 'Decolonial Comparative Law: A Conceptual Beginning' (2022) 86(1) RabelsZ 166.

8 Günter Frankenberg, 'Critical Comparisons: Re-thinking Comparative Law New Directions in International Law' (1985) 26(2) HarvIntlLJ 411.

9 For an introduction to the concept, see John Griffiths, 'What is Legal Pluralism?' (1986) 18(24) JLegPlurUnoffL, 1. Further, see Keebet von Benda-Beckmann and Bertram Turner, in: The Oxford Handbook of Global Legal Pluralism, 2020.

10 The 'traditional' structure of comparative legal research consists of the identification and comprehension of relevant legal rules in different jurisdictions followed by a comparative evaluation. See only Uwe Kischel, *Rechtsvergleichung* (C.H. Beck 2015) 109–111; Salaymeh and Michaels (n 7), passim.

concepts (4) and conclude with observations and a concept-oriented comparison (5).

2. Theory of Reputation

In this section, we outline what we understand under the concept of reputation. We therefore start by providing a working definition (2.1), before we demonstrate the mechanism of how reputation can or ought to influence human – and subsequently institutional – behaviour (2.2). Thereafter, we combine these mechanisms with various aspects stemming from the field of behavioural economics (2.3). We follow this approach to establish not only under which conditions the targeting of reputation as a regulatory concept could – ideally – work, but also where pitfalls might lie.

2.1 Notion and Structural Elements

When researching for a unified notion of reputation, the researcher quickly realises that such a notion does not exist.[11] The reason for this gap might be that various fields of research (e.g., psychology, economics, sociology, law) work with their own perceptions of reputation as a concept.

Coming from the field of law and economics, we build our arguments in this paper on a working definition that understands reputation as a "[…] set of beliefs that stakeholders hold regarding the company's quality."[12] This definition entails three main aspects: a group of stakeholders comprising more than one stakeholder, beliefs instead of knowledge, and perceived quality of the company in question, which usually includes the quality of the company's products or services. We apply these elements of a definition to the field of comparative data protection law.

In addition, if a company's reputation changes, it can influence at least two groups of parties. This links our understanding to the mechanisms described below.

11 Carolin Hümmer, *Die Reputation interner Dienstleister in Konzernen* (Business-to-Business-Marketing 2015) 39–49; John F Mahon, 'Corporate Reputation' (2002) 41(4) Bus&Soc'y 415, 438; Manfred Schwaiger and Sascha Raithel, 'Reputation und Unternehmenserfolg' (2014) 64(4) MRQ 225, 228–230; Kent Walker, 'A Systematic Review of the Corporate Reputation Literature: Definition, Measurement, and Theory' (2010) 12(4) CorpReputRev 357, 379.

12 Roy Shapira, *Law and Reputation* (Cambridge University Press 2020) 21.

Group of Stakeholders. It is important to notice that a company's reputation is made up of the sum of various stakeholders' perceptions.[13] Consequently, it is not a matter of altering only one person's experience with or beliefs in a company or its products to effectively affect the company's reputation. Considering the pace in which positive and, more importantly, negative information disseminates on social media,[14] it is likely that the necessary group size of individuals who have personally experienced an incident shrinks.[15]

Aggregate of Beliefs. Stakeholders' perceptions consist of their beliefs about a company's past actions and situations[16], with the likelihood that the above-mentioned beliefs can be influenced by but are often distinct from actual knowledge. More importantly, the stakeholders' perceptions, their attitudes towards an industry or sector, their (factual) experiences with a company, and the media coverage[17] constitute important influences.

With a focus on data protection, stakeholders can experience a company's attitude towards data protection, for example, when they are (properly or improperly) confronted by cookie banners, when their access to certain webpages is (not) restricted by paywalls, or when they are burdened with extensive (or concise) data protection consent forms. Furthermore, stakeholders' attitude towards an industry might result from personal (factual) experience with data leakage or similar incidents. However, most of the time it is media coverage that is likely to influence stakeholders' attitude towards the data industry. Media coverage can validate but also invalidate previous perceptions. Furthermore, it can also verify, question, or falsify personal (factual) experience.[18]

Similarly, the stakeholders' perceptions of a company can be influenced by reputation management mechanisms. Therefore, it is not surprising that

13 Charles J Fombrun, 'The Buidling Blocks of Corporate Reputation: Definitions, Antecedents, Consequences' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012) 102; Thomas Noe, 'A Survey of the Economic Theory of Reputation: Its Logic and Limits' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012) 116.

14 See only Tina McCorkindale and Marcia W Distaso, 'The Power of Social Media and Its Influence on Corporate Reputation' in Craig E Carroll (ed), *The Handbook of Communication and Corporate Reputation* (Blackwell Publishing Ltd 2013) 497–500.

15 Shapira (n 12) 26.

16 See only Mahon (n 11), 439.

17 This might also extend to non-traditional media, such as customer reviews on customer review platforms or social media.

18 See also Schwaiger and Raithel (n 11), 235–237, 251–252.

approximately 9.5 billion US dollars worldwide were spent on reputation management in the year 2019 alone.[19]

Focus on (Perceived) Quality of Company and Product. The third aspect pertains to the (perceived) quality of a company or product. When focusing on data protection, individual stakeholders can only assess the recency and frequency of a company's data leakages or data protection incidents. Apart from that, stakeholders can only trust in a company's fair, reasonable, and legal processing of their data, as described above.[20] Although it is possible to link trust to a company's prominence on the market and although an excellent reputation management highly influences trust,[21] we cannot focus on such a 'celebrity status' in our assessment of reputation in data protection laws.

Overall, trust in data-driven companies' handling of data, companies' attitude towards data protection, and the absence of data leakages become increasingly important for stakeholders to assess a company's quality, real or perceived, and integrity. Since the handling of data needs to be classified as a credence good or service instead of an experience good or service,[22] it is nearly impossible for stakeholders to factually assess such quality which is why believing in the handling of data becomes increasingly relevant. Owing to these information asymmetries, it can become even more pressing to have not only legal rules requiring companies to inform their customers about data leakages and other data protection incidents, but also media coverage.[23] Depending on a State's regulatory approach, also trust in data protection agencies, their efficacy, the companies' subsequent compliance, and transparency about the agencies' work can have their effects.[24]

Second and Third Parties. Should a State measure (e.g., mandatory information about a data leakage, acquiring a public or private certificate)

19 CHEQ and University of Baltimore, 'The Economic Cost of Bad Actors on the Internet: Fake News 2019' (November 2019), 11–13 <https://de.statista.com/statistik/daten/studie/1074000/umfrage/jaehrliche-kosten-durch-die-auswirkungen-von-fake-news/> accessed 4 August 2023.

20 Certifying companies' data processing might increase trust but highly depends on the frequency of or generally on continuous review mechanisms. Whether the triennial periodic review, outlined in Article 42 GDPR, is sufficient, will be seen.

21 Charles Fombrun and Mark Shanley, 'What's in a Name? Reputation Building and Corporate Strategy' (1990) 33(2) AMJ 233, 252–254.

22 Daniel Feser and Till Proeger, 'Knowledge-Intensive Business Services as Credence Goods—a Demand-Side Approach' (2018) 9(1) JKnowlEcon 62, 74.

23 See also below in section 4.2.

24 See also below in sections 4.3, 4.8, and 4.9.

target a company's reputation, we can identify two groups of parties on whom such reputation-related measures seem to have significantly different effects.

Firstly, there is the group of purported second parties. The second parties are customers, suppliers, investors, and other subjects that are directly dependent on a company.[25] Secondly, there is the group of third parties, which comprises the public, indirectly affected individuals, and other market players.

Armour et al. were able to demonstrate that reputation-related measures have up to nine times greater effect on the group of second parties than they have on the group of third parties.[26] Although their findings were limited to the capital market in the United Kingdom, some structural elements of financial markets and the markets for data-driven companies are comparable: Both fields are highly dependent on trust and their stakeholders' perception, both can be highly volatile depending on the current market situation; both build in large parts on reputation and information asymmetries. Consequently, the findings are at least in part transferable.

2.2 Mechanism

After having established what we understand by the term reputation and how it is built, we outline the (theoretical) mechanism that links reputation-related measures with intended effects. As *Figure 1* outlines, reputation-related measures (e.g., implemented by a State) are supposed to influence a company's behaviour preventively (before any incident might occur) or at least for the future (after an incident occurred).

25 Jonathan M Karpoff, 'Does Reputation Work to Discipline Corporate Misconduct?' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012) 372.

26 John Armour, Colin Mayer and Andrea Polo, 'Regulatory Sanctions and Reputational Damage in Financial Markets' (2017) 52(4) JFinancQuantAnal 1429.

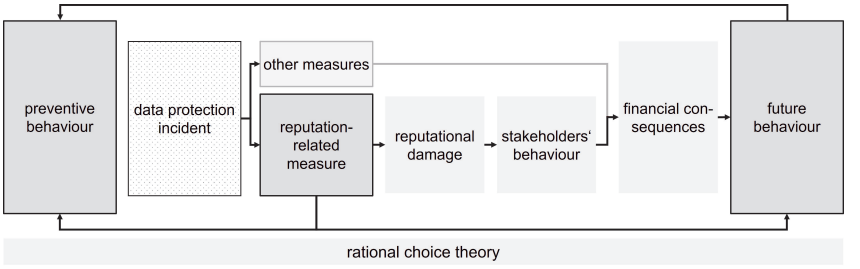

Figure 1 Structured Mechanism of Reputation and its Effects on Behaviour

Ideally, the mere threat of reputation-related measures alters a company's behaviour, because it adapts to avoid the measures' indirect[27] effects. This is because (effective) reputation-related measures that follow a data protection incident will lead to reputational damage. Consequently, the reputational damage alters the stakeholders' perception of a company, which, in turn, affects the company's returns negatively.[28] To avoid such financial repercussions, a company will – so goes the theory – do as much as economically possible and feasible to steer clear of reputational damage.

However, even if a company did not avoid a data incident, it will alter its conduct for the future to avoid further (reputational) losses. Sometimes, the company might also plan to demonstrate to the market and its shareholders that it has changed its behaviour. Such conduct signals market goodwill on the company's part and might restore some, if not all, of its reputational losses.[29]

Reputation-related measures rely on the market to evaluate the data incident and to react accordingly. This already indicates a fundamental obstacle of reputation-related measures: The market needs to be correctly, timely, and comprehensibly informed.[30] Consequently, when evaluating whether reputation-related measures might be effective, it is necessary to

27 In contrast, pecuniary fines can have a more direct, yet sometimes less damaging effect. See only ibid.

28 ibid 1440, 1442.

29 Mobin Fatma and others, 'Building company reputation and brand equity through CSR: the mediating role of trust' (2015) 33(6) IJBM 840, 850.

30 Mona N Lintvedt, 'Putting a price on data protection infringement' (2022) 12(1) IDataPrivL 1, 14.

consider findings relating to the risk of exposure.[31] In parallel, asymmetrical information might entail aspects of market failure, such as adverse selection and moral hazard.[32]

Additionally, the described mechanism of reputation-related measures is directly linked to the theory of (fully) rational behaviour. A fully rational and calculating individual would assess the risk of exposure and multiply it by the expected direct and indirect financial losses. If the calculated sum is higher than the costs of compliance, it will initiate the relevant changes, and vice versa.

2.3 Behavioural Economics and Reputation

However, it is well established that individuals do not behave fully rationally.[33] Instead, their behaviour is subject to heuristics (shortcuts), limited by their computational capacity, and prone to biases.[34] Consequently, it might well be that a company's representative does not act upon the introduction or enactment of reputation-related measures. At the same time, these measures build on the assumption and expectation that a broad audience[35] notices, (correctly) assesses, decides to act, and acts upon a data incident (e.g., a data leakage).[36] However, cognitive biases might interfere with each of these four steps (notice, assess, decide, act).

Noticing. Firstly, stakeholders need to become aware of the relevant pieces of information (e.g., about a data leakage). This is easier assumed than proven, since the mere magnitude of information stimuli to which stakeholders are exposed impedes noticing all relevant information. Especially when stakeholders are not directly informed about a data incident,

31 See Annika Selzer and others, 'Practitioners' Corner – An Economic Analysis of Appropriateness under Article 32 GDPR' (2021) 7(3) EDPL 456, 461.

32 See chapter by Kerber/Specht-Riemenschneider in this volume.

33 Gerd Gigerenzer and Reinhard Selten, 'Rethinking rationality' in Gerd Gigerenzer and Reinhard Selten (eds), *Bounded Rationality* (Dahlem Workshop Reports, MIT Press 2001) 1, 2–6.

34 See only the findings by Daniel Kahneman, *Attention and effort* (Prentice Hall series in experimental psychology, Prentice Hall 1973); Daniel Kahneman and Amos Tversky, 'Prospect Theory: An Analysis of Decision under Risk' (1979) 47(2) Econometrica 263; Amos Tversky and Daniel Kahneman, 'Judgment under Uncertainty: Heuristics and Biases' (1974) 185(4157) Science 1124.

35 See section 2.1 above.

36 Michael L Barnett, 'Why Stakeholders Ignore Firm Misconduct' (2014) 40(3) JManage 676, 683 et passim.

they often only learn of such a situation if an intermediary (e.g., the media) reports about it. In those cases, however, the link between an incident and a stakeholder noticing it is indirect and therefore unsure. Consequently, not every piece of information will reach the individual stakeholder and the market with the same intensity.

Furthermore, such information needs to be salient[37] enough to stand out from the magnitude of information that surrounds stakeholders every day. Especially, the level of harm (caused by a data incident), the stakeholders' personal or professional[38] interests in noticing a piece of information, their motivation to learn about (types of) information, and heuristics (e.g., availability heuristic) will determine whether they notice such information.[39]

Assessing. Secondly, stakeholders who have noticed a piece or pieces of information also need to assess it correctly. At this stage, primarily the way in which information is presented (e.g., framing effects[40]) determines how stakeholders will assess information. Moreover, there are a variety of heuristics and biases that originate from within a stakeholder (e.g., confirmation bias,[41] ambiguity aversion,[42] status quo bias[43]) and influence the way and likelihood to assess a (piece of) information correctly.

Deciding. Thirdly, and assuming that a stakeholder has noticed a piece or pieces of information and assessed it correctly, the stakeholder must decide whether to act on the information. At that stage, the market's status quo is as important as biases that originate from the stakeholder itself. Only if a market allows for equally suitable alternatives (e.g., alternative messenger services that at least most of a stakeholder's regular contacts use or might

37 Salience generally refers to the degree to which a particular attribute or piece of information is prominent or noticeable in the decision-making process of an individual or group, see Pedro Bordalo and others, 'Salience and Consumer Choice' (2013) 121(5) JPoliticalEcon 803, 3, 40.

38 An example might be system administrators who become aware of risks stemming form certain programmes, etc.

39 Barnett (n 36), 683 et passim.

40 Alan M Rubin, 'An Examination of Television Viewing Motivations' (1981) 8(2) Communication Research 141, 158.

41 Barnett (n 36), 688.

42 Daniel Ellsberg, 'Risk, Ambiguity, and the Savage Axioms' (1961) 75(4) QJEcon 643, 668.

43 William Samuelson and Richard Zeckhauser, 'Status quo bias in decision making' (1988) 1 JRiskUncertain 7, 47.

likely use) and only if the opportunity costs[44] that are incurred when switching to the alternative service are not prohibitive, is a stakeholder faced with a reasonable opportunity to switch service providers.[45]

Moreover, stakeholders are again subject to diverse biases (e.g., status quo bias, sunk costs fallacy[46], home bias[47]), which might prevent them from acting. Furthermore, stakeholders need to be motivated to switch services or service providers. The perception of how they personally assess the immaterial costs of changing current and practiced behaviour will influence their calculation of opportunity costs.

Acting. Fourthly, even if individuals noticed an incident that harms a company's reputation, assess the situation fully and correctly, and decide to take action, there remain three ways in which they can act: do nothing, voice their irritation, or exit the market or company's service.[48]

To sum up, the prima facie link between introducing a reputation-related measure and the aforesaid measure taking effect is all but straight and clear. Instead, there are multiple hurdles and obstacles that such measures need to overcome before becoming effective.

3. Structural Elements for a Typology

The following structural elements for a typology are meant to support a future comparison of regulatory measures. The elements are influenced by the above-described mechanism of reputation and are drawn from our comparison of eight data protection legal systems.[49] They lead towards

44 Opportunity cost is the value of the next best alternative forgone as a result of making a decision, see Nicholas G Mankiw, *Principles of macroeconomics* (Cengage Learning 2021) 4.

45 At this stage, competition laws came into play, see also Kerber/Specht-Riemenschneider in this volume.

46 Samuelson und Zeckhauser 1988, S. 35.

47 Bong-Chan Kho and others, 'Financial Globalization, Governance, and the Evolution of the Home Bias' (2009) 47(2) JAccountRes 597, 600.

48 For the purpose of assessing the (immediate) effects of reputation-related measures, future re-entries into the market can be ignored at this stage.

49 For a summary of our research project's legal comparison, see Timo Hoffmann, 'The Laws of Data Disclosure: Examining the Regulation of Individuals' Personal Data Disclosure in Brazil, China, the European Union, Ghana, Japan, Russia, Switzerland and the United States of America' in Moritz Hennemann and others (eds), *Data disclosure: Global developments and perspectives* (Global and Comparative Data Law Volume 2, De Gruyter 2023), 1.

the concept-oriented comparison (5). In this paper, we wish to describe eight such elements, knowing that this list can only be a starting point for future research.[50] With these elements, we attempt to categorise the reputation-related measures below (4).

3.1 Mode of Regulation

A first element pertains to the mode of regulation. Some reputation-related measures are the result of self-regulatory advances. Those self-regulatory measures might be developed by industry associations or companies themselves to signal compliance with high levels of data protection. Other measures are circumscribed by legislation, whereas the details are left to companies or industry associations to determine (i.e., regulated self-regulation). Then again, other measures are completely prescribed by law.

3.2 Actors

A second element focuses on the actors that are obligated under such regulation. Generally, this is either a private corporation or a State organ. However, there might be specific alternatives to or forms of such dichotomy. For example, industry associations – which can be State-owned, publicly organised, or founded as a privately owned association – might be required to act upon legislation.

3.3 Effects

A third element concerns the effects of a measure. When it comes to reputation-related measures, these effects can range on a continuum from very concrete effects (e.g., direct shaming) to rather diffuse effects (e.g., naming). Undoubtedly, the particular formulation, reach, and distribution of those measures will influence how a particular measure is assessed in terms of its effects.

50 For a link between these elements and the collection of concepts, see the concept-oriented comparison in and at 5 below.

3.4 Impact as a Sanction

A fourth element has to do with whether the reputation-related measure has an impact as a sanction. Again, this element should be understood as a continuum, ranging from no sanction intended through to measures that are structured to only have secondary sanctioning effects or measures that involve intended sanction. In practice, most measures could be argued to have at least secondary sanctioning effects.

3.5 Starting Point

A fifth element is the starting point of a reputation-related measure. Whereas some measures are meant to have preventive effects, others are designed to operate repressively. Particularly, measures that operate based on information requirements can have both effects. Following such information, market participants might refrain from using a company's products or they might take measures to protect their data.

3.6 Reach

A sixth element has to do with a measure's reach. When it becomes necessary to inform aggrieved parties directly about, for example, a data leakage, the measure focuses on a definable group of individual subjects. However, if a measure is meant to inform the general public, it reaches an undefinable group and can be described as collective.

3.7 Point in Time

A seventh element pertains to the timeline or point in time when a measure is meant to take place. Particularly, measures that should have preventive effects usually also need to be conducted before a data incident occurs. Other measures function (primarily) repressively and have to be implemented in the aftermath of a data incident. Then again, there are measures that need to be activated during a data incident. Nonetheless, some measures might take effect at various points in time.

3.8 Reception

An eighth and last element has to do with the reception. Whereas some measures are meant to be noticed directly by market participants, others are aimed at intermediaries. In the latter case, it is left for such intermediaries (e.g., general press, news media outlets, academic literature, private website hosts, blogs) to further distribute the effects of a measure. Often, intermediaries such as the press or the media exercise discretion in whether and how they disseminate information. Aggravated individuals or the public might therefore not be the primary recipient.

4. Collection of Concepts

The following sections outline a total of ten concepts of reputation-related measures we identified in various legal systems.

4.1 Codes of Conduct

A common reputation-related measure pertains to a (standardised) code of conduct about processing personal data. Typically, industry associations prepare these codes for their members, and the codes are meant to guide how to protect personal data for industry-specific or area-specific acts of processing. Usually, companies add a reference that they comply with these codes.

Data protection legislation can reference such codes of conduct, giving incentives for subscription to such a code[51] or allowing for review by the regulatory authority.[52] Within legislation, codes of conduct may be linked to modes of certification.[53]

51 Under Article 52 § 1 IX of the Brazilian *Lei Geral de Proteção de Dados Pessoais* (LGPD), the regulator can positively consider the adoption of a code of conduct in the form of a 'good practices and governance policy' in the event of the imposition of a sanction. See Timo Hoffmann and Pietro L Pietrobon de Moraes Vargas, 'LGPD Et Al.: Report on the Law of Data Disclosure in Brazil' (2022) 22(6) University of Passau IRDG Research Paper Series, 45.

52 Article 40 GDPR.

53 See section 4.2 below.

Article 53 of the Japanese data protection law, the Act on the Protection of Personal Information (APPI),[54] provides for the implementation of codes of conduct via the development of guidelines by 'accredited personal information protection organizations'. These guidelines must be forwarded to the Personal Information Protection Commission (PPC), which then publishes the guidelines.[55] The accredited organisation must then 'take action' towards the implementation of the act.[56] Accredited organizations like those referred to above are usually industry associations.[57] In addition, the PPC lists the companies covered by such organisations on their website.[58]

The mere existence or non-existence of codes of conduct can have signalling effects for market participants.[59] Particularly, if an industry standard has been developed and the public is familiar with it, companies that do not reference such a code of conduct or that do not comply with it might be subject to reputational effects.

4.2 Certification Mechanisms

To obtain certification, a party intending to process personal data must submit itself (as an organisation), certain procedures, or provided services to a review by a regulator or specialised agency. Upon positive review, the party processing personal data may then advertise itself as certified or alike.[60] This allows those parties to signal their compliance with data protection legislation to the public.

54 Act on the Protection of Personal Information, amended version, effective 1 April 2022. English translation available at Personal Information Protection Commission Japan, 'Laws and Policies' (2023) <https://www.ppc.go.jp/en/legal/> accessed 4 August 2023.

55 Article 53(2) and (3) APPI.

56 Article 53(4) APPI.

57 Personal Information Protection Commission Japan, 'List of Authorized Personal Information Protection Organizations (transl.)' (8 February 2023) <https://www.ppc.go.jp/personalinfo/nintei/list/> accessed 8 February 2023.

58 ibid.

59 Stephen Brammer and Gregory Jackson, 'How Regulatory Institutions Influence Corporate Reputations: A Cross-Country Comparative Approach' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012) 310.

60 Regarding Article 42(5) GDPR and the 'European Data Protection Seal', see also Hornung/Kohpeiß in this volume.

An example of such certification by recognised independent certification bodies can be found in Article 11 of the Swiss Data Protection Act (DSG)[61]. Upon positive evaluation, companies acquire a 'Data Protection Quality Seal'[62]. In practice, this specific certification mechanism has not proven particularly popular.[63] Under the revised version of the DSG[64], set to enter into force in September 2023, the certification of services will be possible (Article 13) too, while the overall certification system remains unchanged.[65]

Certifications can have a signalling effect for market participants, if they (can) trust the certifying institution. Once a certification has become well established in the market, the stakeholders will also notice the absence of a certificate for a product, service, or company, which then leads to reputational effects.

4.3 Public Data (Protection) Register

In Ghana, Section 27 of the Data Protection Act 2012 (DPA)[66] includes a wide-ranging obligation for all parties processing personal data to register with the Data Protection Commission (DPC), that is the Ghanaian regulator. Those covered by the DPA are required, *inter alia*, to provide comprehensive information on their data processing activities, contact information, and a 'general description of measures to be taken to secure the data'.[67] The DPC then checks the application and registers the applicant.[68]

61 Bundesgesetz über den Datenschutz (transl. *Data Protection Act*), enacted 19 June 1992 as amended 1 March 2019, SR 235.1. Not to be confused with the revised DSG set to enter into force on 1 September 2023, which will also be referred to hereafter.

62 Translated from German: '*Datenschutz-Qualitätszeichen*'.

63 The Swiss regulator has already spoken of 'difficulties' with certification in 2010: Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, 'Stand der Produkt- und Dienstleistungszertifizierung' (2011) <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/datenschutzzertifizierung/stand-der-produkt--und-dienstleistungszertifizierung.html> accessed 8 February 2023.

64 Bundesgesetz über den Datenschutz (transl. *Data Protection Act*), enacted 25 September 2020, BBl 2020, 7639.

65 See further Peer Sonnenberg and Timo Hoffmann, 'Data Protection Revisited: Report on the Law of Data Disclosure in Switzerland' (2022) 22(17) University of Passau IRDG Research Paper Series, 45.

66 Data Protection Act, 2012 (Act 843).

67 Section 47(1) DPA 2012.

68 Section 49 DPA 2012.

Registration and the registration's biennial renewal are subject to a fee,[69] which is the major source of financing for the DPC.[70]

The DPC makes the register accessible to the public,[71] which, in practice, is done via a searchable webpage.[72] Anyone interested in a particular party's data processing activities may check whether it is properly registered. Non-registration or expired registration is easily identifiable, clearly indicating non-compliance with this obligation. In practice, however, only a minority of obligated parties are registered,[73] leading to a temporary amnesty in an effort to increase registration numbers,[74] followed by the announcement of enforcement measures.[75]

Public data (protection) registers can improve public credence and allow for public easy-access information. Depending on the information these registers collect and on the level of review by the responsible authority, stakeholders can trust the validity of certain information or believe that their data is processed in compliance with the law.

4.4 Violation in Plain View

Another reputational effect of data protection may occur when a data protection law is violated in a manner that is clearly visible to a stakeholder. An example may be found in the non-fulfilment of information requirements under the GDPR.[76] The GDPR requires parties processing personal data to provide the data subject with information such as, *inter alia*, the purpose of

69 Section 59 DPA 2012.

70 See further Timo Hoffmann, 'Data Protection Act(ion): Report on the Law of Data Disclosure in Ghana' (2022) 22(1) University of Passau IRDG Research Paper Series, 15.

71 Section 54 DPA 2012.

72 Data Protection Commission Ghana, 'Data Protection Register – Entities Search' (2019) <http://app.dataprotection.org.gh/en/entities/search/> accessed 4 August 2023.

73 Ghanaian German Economic Association, 'Data controllers granted 6-month relief to regularize their operations' *Ghanaian German Economic Association* (12 October 2020) <http://ggea.net/news/data-controllers-granted-6-month-relief-to-regularize-their-operations/> accessed 4 August 2023.

74 Data Protection Commission Ghana, 'Amnesty' (2020) <https://dataprotection.org.gh/amnesty> accessed 4 August 2023.

75 Juliet Akyaa Safo, 'Register with Data Protection Commission or face prosecution – Adusei-Poku' *Graphic Online* (31 March 2022) <https://www.graphic.com.gh/news/general-news/register-with-data-protection-commission-or-face-prosecution-adusei-poku.html> accessed 4 August 2023.

76 Regulation (EU) 2016/679 of 2016, OJ L (2016) 119/1.

processing, categories of personal data processed, and the contact details of a data protection officer.[77] Data subjects who are aware of this requirement may notice non-compliance with the GDPR if asked to provide personal data. Failure to comply with such informational requirements may thus negatively affect the way in which the data subject witnessing this violation of the GDPR views the party processing personal data.

Depending on the stakeholders' data privacy literacy[78], they might be aware of missing information, the absence of cookie banners, or illegal dependencies between a company's request for personal data and access to its digital products. Consequently, the better the stakeholders know the relevant legal regime, the more severe the reputational loss suffered by non-compliant companies will be.

4.5 Notification Obligations after Data Breach

Obligations to report to the public are very common in the case of data leaks or data breaches. Where personal data is subjected to an incident such as hacking, data loss, or the like, the above-mentioned notification obligations require, with some variation, that the party informs the regulator, the data subjects affected, the public, or a combination of the former.

In the case of a 'personal data breach', for example, the GDPR requires notification of the relevant regulatory authority within 72 hours of awareness of the situation.[79] In severe cases,[80] the party affected by the breach is additionally required to inform the data subjects of the breach 'without undue delay',[81] alongside further information like the nature of the data breach, its consequences, and measures taken.[82] In cases where a great

77 Article 13 GDPR.

78 Data privacy literacy refers to the level of knowledge and understanding that stakeholders have about their data privacy rights, the risks associated with data collection and processing, and the measures they can take to protect their personal information, see Trepte and others, 'Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale"' in Serge Gutwirth and others (eds), *Reforming European Data Protection Law* (Springer Netherlands 2015) 333, 339.

79 Article 33(1) GDPR.

80 Article 34(1) GDPR.

81 Article 34(1) GDPR.

82 Article 34(3) GDPR.

number of individuals are involved, this may equate to a *de facto* publication requirement via media reception.[83]

Consequently, notification obligations are meant to allow data subjects not only to take appropriate measures to protect themselves from any harm (if feasible, e.g., changing of passwords), but also to allow them to take the data leakage into account when assessing whether a competitor might be better suited to protect their data. Since aggrieved subjects must often be personally informed, there is a very high probability that they at least notice the data incident, particularly when the responsible controller has taken further noticeable action to mitigate the impact of the breach.

4.6 Violation-Oriented Shaming as an Explicit Sanction

The explicit use of shaming as a sanction for violations of data protection laws is rare amongst data protection legislation, despite shaming being a widespread instrument in other areas of the law,[84] such as capital markets regulation, in the form of 'naming and shaming'.[85]

An exception can be found in the Brazilian LGPD.[86] In its catalogue of sanctions, the Brazilian data protection authority (ANPD)[87] may 'publicise the infraction after its accurate assessment and confirmation of its occurrence'.[88]

The ANPD has not yet published the guidelines for the application of sanctions. However, the comments on the sanction of publication in

83 Cédric Burton, *Article 34 Communication of a personal data breach to the data subject* (2020) 660.

84 Judith van Erp, '30 – Shaming and Compliance' in Daniel D Sokol and Benjamin van Rooij (eds), *The Cambridge Handbook of Compliance* (Cambridge University Press 2021) 439; Cullen S Hendrix and Wendy H Wong, 'When Is the Pen Truly Mighty? Regime Type and the Efficacy of Naming and Shaming in Curbing Human Rights Abuses' (2013) 43(3) BritJPolitSci 651, 671.

85 Judith van Erp, 'Naming and Shaming of Corporate Offenders' in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of criminology and criminal justice* (Springer Reference 2014) 3209, 3210; Edward F Greene and Joshua L Boehm, 'The Limits of "Name-and-Shame" in International Financial Regulation' (2012) 97(5) CornellLRev 1083, 1086.

86 Lei Geral de Proteção de Dados Pessoais (*transl. General Law for the Protection of Personal Data*), Law No. 13.709 of 14 August 2018.

87 Autoridade Nacional de Proteção de Dados (*transl. National Authority for the Protection of Personal Data*).

88 Article 52(4) LGPD.

the regulatory impact assessment concerning sanctions, which compares the sanction catalogue to other national and international legislation and comments on its operationalisation, implies that publication is to occur in the news media, such as in newspapers.[89] The offender is likely to also bear the costs of publication.[90]

Evidently, such shaming in the media has the potential of heavy reputational losses.[91] However, the specific effects will depend on details of the publication: the type and reach of the medium, whether publication occurs repeatedly, the size and presence of the publication, etc. In contrast to the previously described individual notification requirements, public shaming is less targeted at current customers but focuses on the public as a whole and potential future customers.

4.7 (Voluntary) Public Apology

In certain contexts, normative effects with regard to reputation in data protection contexts may arise not only from State law, but from societal expectations. Where there is strong social pressure, these expectations can constitute a form of law.[92] In data protection practice, a Japanese social 'obligation' may require a company to publicly apologise.[93] Such an apology may lead to more widespread awareness of a violation of law, but it may perhaps also soften the reputational blow as a countermeasure to negative public opinion. In Japan, public apologies are primarily made out of fear for the reputational impacts.[94]

In one case, this fear for the reputational impacts has extended to the granting of (low-value) vouchers to affected individuals.[95] This practice

89 Autoridade Nacional de Proteção de Dados, *Relatório de Análise de Impacto Regulatório: Construção do Modelo Regulatório Previsto Na LGPD com Relação à Aplicação de Sanções Administrativas e às Metodologias de Cálculo do Valor-Base das Sanções de Multa* (2022) 107–108.

90 This presumably relates to fees for advertisement space/time in such media.

91 See only Armour, Mayer and Polo (n 26); Sharon Yadin, 'Regulatory Shaming' (2019) 49(2) EnvtlL 407–451, 417.

92 For more detail on non-state normative ordering, refer to Griffiths (n 9), 1.

93 Flora Wang, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement' (2020) HarvJL&Tech 661, 679–681.

94 Regarding willingness to disclose data, see Daniela Wawra and others, 'Cultural Influences on Personal Data Disclosure Decisions – Japanese Perspectives' [2022] SSRN Journal <https://ssrn.com/abstract=4079634> accessed 4 August 2023.

95 Wang (n 93), 680.

must be understood in the context of the generally observed aversion to litigation[96] and hard enforcement[97] in Japan[98] in favour of a focus on cooperation and communal reputation.

Public apologies can be out of the reputation management playbook.[99] Often, such apologies do not only disclose that a data breach has occurred, but also include information about the steps a company has already taken and is about to take to prevent future leaks. The additional information is meant to mitigate reputational losses. Consequently, apologies are open to exploit framing effects. At the same time, the fear of having to apologise to the public after a leakage can incentivise companies to take precautionary steps.

4.8 Public Relations Work by Supervisory Authorities

In some cases, supervisory authorities' publications and public relations work can have reputational effects. Often, such activities are required to enhance governmental transparency and are not necessarily considered a sanction from a legal perspective.

An example is the United Kingdom Information Commissioner's Office (ICO). The ICO makes its actions public – extensively – on its website, naming individual companies that have been fined, going as far as offering an 'action we've taken e-newsletter'.[100] In its press releases, the ICO, apart from naming the companies, even provides testimonials by victims, thereby making use of emotional responses to violations.[101]

96 Giorgio F Colombo and Hiroshi Shimizu, 'Litigation or Litigiousness? Explaining Japan's "Litigation Bubble" (2006-2010)' [2016] Oxford University Comparative Law Forum <https://ouclf.law.ox.ac.uk/litigation-or-litigiousness-explaining-japans-litigation-bubble-2006-2010/> accessed 4 August 2023.

97 Wang (n 93), 680.

98 See further Timo Hoffmann, 'Data Protection by Definition: Report on the Law of Data Disclosure in Japan' (2022) 22(3) University of Passau IRDG Research Paper Series.

99 Tulika M Varma, 'Responsible Leadership and Reputation Management During a Crisis: The Cases of Delta and United Airlines' (2021) 173(1) JBusEthics 29, 40.

100 UK Information Commissioner's Office, 'Action we've taken' (2023) <https://ico.org.uk/action-weve-taken/> accessed 4 August 2023.

101 UK Information Commissioner's Office, 'Five businesses fined a total of £435,000 for making nearly half a million unlawful marketing calls' (7 December 2022) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/12/five-busin

In a blog post, a law firm makes reference not only to the ICO's practice of 'naming and shaming', stating the importance of publicity as a concern of involved companies, but also to the 'lack [of] a clear appeals mechanism once a reprimand has been imposed'. The latter aspect is particularly problematic because such informational action by the ICO cannot, as opposed to other sanctions, be appealed to the relevant tribunal.[102] This hints at the high practical relevance of such public relations work by authorities and demonstrates the reputation effects companies fear.

4.9 Transparency in the Judicial or Administrative Process

Another notable reputation-related measure can come as a side effect of judicial or administrative transparency. By allowing for a high degree of transparency in judicial or administrative proceedings, the public can gain insight into alleged or actual breaches of data protection or privacy legislation. Such publications might include information on how (effectively) the situation was handled.

Where the United States' Federal Trade Commission enforces privacy laws in the US, documents regarding enforcement are made public, and thus transparent, to a great degree.[103] Comprehensive publication of case documents takes place, which allows for easily accessible insights into wrongdoing. This subjects the party processing personal data, conditional on enforcement action, to the 'court' of public opinion[104] alongside other applied sanctions.

The effect of such judicial or administrative transparency highly depends on the reception by major media outlets and the relevant public. Reputational effects are therefore usually rather indirect and dependent on the

---

esses-fined-a-total-of-435-000-for-making-nearly-half-a-million-unlawful-marketing-calls/> accessed 4 August 2023.

102 Giles Pratt and others, 'Naming and shaming? The UK ICO is now naming most organisations it investigates' (31 January 2023) <https://technologyquotient.freshfields.com/post/102i6m7/naming-and-shaming-the-uk-ico-is-now-naming-most-organisations-it-investigates> accessed 4 August 2023.

103 Federal Trade Commission, 'Privacy and Security Enforcement' 107–108 <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> accessed 4 August 2023.

104 See, for example, media reporting: Frank Bajak, 'FTC fines GoodRx for unauthorized sharing of health data' *CBS News* (1 February 2023) < https://www.cbsnews.com/sacramento/news/goodrx-unauthorized-sharing-of-health-data/> accessed 4 August 2023.

distribution by intermediaries should the judicial or administrative organ not enhance publication themselves.

4.10 Governmental Warnings

In certain situations, supervisory authorities may warn the public of certain companies or products that are considered harmful. While the sanctioning effect is not the primary goal, being subject to such a warning can have significant reputational impact.

In Germany, the Federal Office for Information Security (BSI)[105] may warn the public or affected groups in the event of a loss of or unauthorised access to data.[106] Although related to a slightly different context,[107] such a warning by the BSI was recently subject to much debate after it issued a warning against a Russian antivirus software provider[108] following the Russian invasion of Ukraine[109].[110]

In particular, if a government or its individual institutions are (highly) trusted by the citizens, a governmental or administrative warning can have detrimental effects on a company's reputation, presuming that such warnings are used rarely and as a measure of last resort. In such a case, it is likely not only that the warning itself is received, but also that the media will report about the warning to make it commonly known. Apart from that, the reputation effects resemble those described with regard to notification obligations (4.5 above), but furnished with a seal of a public warning.

105 Bundesamt für Sicherheit in der Informationstechnik (*transl. Federal Office for Security in Information Technology)*.

106 § 7(1)(1)(c) of the Act on the Federal Office for Information Security (BSIG).

107 This incident concerned security concerns and was based on § 7(1)(1)(a) BSIG.

108 Bundesamt für Sicherheit in der Informationstechnik, 'Warnung vor Kaspersky-Virenschutzsoftware nach § 7 BSIG' (30 September 2022) <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/Archiv/FAQ-Kaspersky/faq_node.html> accessed 4 August 2023.

109 UNGA, *Aggression against Ukraine* (01.03.2022) UN Doc A/ES-11/L.1; UNGA, *Principles of the Charter of the United Nations underlying a comprehensive, just and lasting peace in Ukraine* (16.02.2023) UN Doc A/ES-11/L.7.

110 For a comprehensive overview, see Tilmann Dittrich, 'Die "Akte Kaspersky": kritische Betrachtungen zur Warnung vor einer Virenschutzsoftware' (2022) NJW 2971.

5. Concluding Observations with Concept-Oriented Comparison

Table 1 below merges the above-described structural elements for a typology (3 above) with the collection of concepts described immediately above (4 above). In this last section, we therefore share some concluding observations that follow a concept-oriented comparison.

regulatory instruments	mode of regulation	actors	effects	Impact as a sanction	starting point	reach	point in time	reception
codes of conduct	(regulated) self-regulation	private	diffuse	none	preventive	collective	before incident	direct
certification mechanisms	(regulated) self-regulation	private/ public	diffuse	none	preventive	individual/ collective	before incident	direct/ indirect
public data (protection) register	statutory regulation	public	diffuse	secondary effect	preventive	collective	before incident	direct/ indirect
violation in plain view	statutory regulation	private	concrete	secondary effect	preventive/ repressive	individual	during incident	direct
notification obligations after data breach	statutory regulation	private/ public	concrete	secondary effect	preventive/ repressive	individual/ collective	after incident	direct
violation-oriented shaming as an explicit sanction	statutory regulation	public	concrete	intended	preventive/ repressive	collective	after incident	indirect
(voluntary) public apology	self-regulation	private	concrete	intended	(preventive/) repressive	collective	after incident	indirect
public relations work by supervisory authorities	statutory regulation	public	concrete/ diffuse	secondary effect/intended	preventive/ repressive	collective	after incident	indirect
transparency in the judicial or administrative process	statutory regulation	public	diffuse	secondary effect/none	preventive/ repressive	individual/ collective	after incident	(direct/) indirect
governmental warnings	statutory regulation	public	concrete/ diffuse	secondary effect/intended	Preventive (/repressive)	collective	during incident	direct/ indirect

Table 1 Reputation-related Measures Assessed by Elements of Typology

When assessing the efficacy of reputation-related measures, a common determinant is that the relevant public first needs to notice and process the given information before there is a chance that such information leads to reputational losses. Even if the relevant public notices and processes such information, reputation-related measures can only have an effect if there is sufficient relevant competition that allows stakeholders to switch, for example, service providers.[111]

The link between a reputation-related measure and its effects is rather indirect and often requires intermediaries to play their role. Furthermore, dissemination of information via the media will reach second and third parties alike.[112] Therefore, it will be difficult to evaluate such measures' effects precisely. Consequently, the preventive effects of reputation-related measures are equally uncertain.

From a comparative point of view, we realise that several measures are not primarily meant to have reputation-related effects. However, many

111 See Kerber/Specht-Riemenschneider in this volume.
112 See above following n 24.

accept such reputation-related effects as side effects. Thus far, we could also not identify reputation-related measures with which supervisory authorities explicitly address second parties.

Apart from informational obligations that are often required to obtain consent from data subjects for processing their data, most reputation-related measures are repressive by nature. Furthermore, most measures build on disseminating information in one way or another and can be identified as descriptive by nature. Consequently, stakeholders need to be sufficiently knowledgeable to assess the risk based on such factual and descriptive information. However, such assessment requires a high level of data protection literacy.

Overall, reputation-related measures are common to all reviewed jurisdictions, be it either as direct and intended measures or as indirect side effects.

Acknowledgement

The presented research is part of an interdisciplinary research project 'Vectors of Data Disclosure – A comparative study on the disclosure of personal data from the perspectives of legal, cultural studies, and business information systems research', https://www.bidt.digital/en/vectors-data-disclosure, supported by the Bavarian Research Institute for Digital Transformation (an Institute of the Bavarian Academy of Sciences and Humanities). We would like to thank the participants of the Jahrestagung Forum Privatheit 2022 in Berlin for their feedback and many discussions. Furthermore, we would like to thank the student research assistant Nico Göbel for supporting us with finalising this paper.

References

Akyaa Safo J, 'Register with Data Protection Commission or face prosecution - Adusei-Poku' *Graphic Online* (31 March 2022) <https://www.graphic.com.gh/news/general-news/register-with-data-protection-commission-or-face-prosecution-adusei-poku.html> accessed 4 August 2023.

Armour J, Mayer C and Polo A, 'Regulatory Sanctions and Reputational Damage in Financial Markets' (2017) 52(4) JFinancQuantAnal 1429.

Autoridade Nacional de Proteção de Dados, *Relatório de Análise de Impacto Regulatório: Construção do Modelo Regulatório Previsto Na LGPD com Relação à Aplicação de Sanções Administrativas e às Metodologias de Cálculo do Valor-Base das Sanções de Multa* (2022).

Bajak F, 'FTC fines GoodRx for unauthorized sharing of health data' *CBS News* (1 February 2023) <https://www.cbsnews.com/sacramento/news/goodrx-unauthorized-sharing-of-health-data/> accessed 4 August 2023.

Barnett ML, 'Why Stakeholders Ignore Firm Misconduct' (2014) 40(3) JManage 676.

BBC News, 'Three years of GDPR: the biggest fines so far' *BBC News* (24 May 2021) <https://www.bbc.com/news/technology-57011639> accessed 4 August 2023.

von Benda-Beckmann K, Turner B, 'Anthropological Roots of Global Legal Pluralism' in Paul Schiff Berman (ed), *The Oxford Handbook of Global Legal Pluralism* (1st edn, Oxford Univ Press 2020).

Bordalo P, Gennaioli N and Shleifer A, 'Salience and Consumer Choice' (2013) 121(5) JPoliticalEcon 803.

Brammer S and Jackson G, 'How Regulatory Institutions Influence Corporate Reputations: A Cross-Country Comparative Approach' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012).

Bundesamt für Sicherheit in der Informationstechnik, 'Warnung vor Kaspersky-Virenschutzsoftware nach § 7 BSIG' (30 September 2022) <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/Archiv/FAQ-Kaspersky/faq_node.html> accessed 4 August 2023.

Burton C, *Article 34 Communication of a personal data breach to the data subject* (2020).

CHEQ and University of Baltimore, 'The Economic Cost of Bad Actors on the Internet: Fake News 2019' (November 2019) <https://de.statista.com/statistik/daten/studie/1074000/umfrage/jaehrliche-kosten-durch-die-auswirkungen-von-fake-news/> accessed 4 August 2023.

Colombo GF and Shimizu H, 'Litigation or Litigiousness? Explaining Japan's "Litigation Bubble" (2006-2010)' [2016] <https://ouclf.law.ox.ac.uk/litigation-or-litigiousness-explaining-japans-litigation-bubble-2006-2010/> accessed 4 August 2023.

Data Protection Commission Ghana, 'Data Protection Register – Entities Search' (2019) <http://app.dataprotection.org.gh/en/entities/search/> accessed 4 August 2023.

— 'Amnesty' (2020) <https://dataprotection.org.gh/amnesty> accessed 4 August 2023.

Dittrich T, 'Die "Akte Kaspersky": kritische Betrachtungen zur Warnung vor einer Virenschutzsoftware' [2022] 2971.

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter, 'Stand der Produkt- und Dienstleistungszertifizierung' (2011) <https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/datenschutzzertifizierung/stand-der-produkt--und-dienstleistungszertifizierung.html> accessed 8 February 2023.

Ellsberg D, 'Risk, Ambiguity, and the Savage Axioms' (1961) 75(4) QJEcon 643.

van Erp J, 'Naming and Shaming of Corporate Offenders' in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of criminology and criminal justice* (Springer Reference 2014).

— '30 – Shaming and Compliance' in Daniel D Sokol and Benjamin van Rooij (eds), *The Cambridge Handbook of Compliance* (Cambridge University Press 2021).

Fatma M, Rahman Z and Khan I, 'Building company reputation and brand equity through CSR: the mediating role of trust' (2015) 33(6) IJBM 840.

Federal Trade Commission, 'Privacy and Security Enforcement' (2018) <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> accessed 4 August 2023.

Feser D and Proeger T, 'Knowledge-Intensive Business Services as Credence Goods—a Demand-Side Approach' (2018) 9(1) JKnowlEcon 62.

Fombrun C and Shanley M, 'What's in a Name? Reputation Building and Corporate Strategy' (1990) 33(2) AMJ 233.

Fombrun CJ, 'The Buidling Blocks of Corporate Reputation: Definitions, Antecedents, Consequences' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012).

Frankenberg G, 'Critical Comparisons: Re-thinking Comparative Law New Directions in International Law' (1985) 26(2) HarvIntlLJ 411.

Ghanaian German Economic Association, 'Data controllers granted 6-month relief to regularize their operations' *Ghanaian German Economic Association* (12 October 2020) <http://ggea.net/news/data-controllers-granted-6-month-relief-to-regularize-their-operations/> accessed 4 August 2023.

Gigerenzer G and Selten R, 'Rethinking rationality' in Gerd Gigerenzer and Reinhard Selten (eds), *Bounded Rationality* (Dahlem Workshop Reports, MIT Press 2001).

Greene EF and Boehm JL, 'The Limits of "Name-and-Shame" in International Financial Regulation' (2012) 97(5) CornellLRev 1083.

Greenleaf G, 'Now 157 countries: Twelve data privacy laws in 2021/22' [2022] 3.

Griffiths J, 'What is Legal Pluralism?' (1986) 18(24) JLegPlurUnoffL 1.

Gwebu KL, Wang J and Wang L, 'The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management' (2018) 35(2) JMIS 683.

Hendrix CS and Wong WH, 'When Is the Pen Truly Mighty? Regime Type and the Efficacy of Naming and Shaming in Curbing Human Rights Abuses' (2013) 43(3) BritJPolitSci 651.

Hennemann M, 'Wettbewerb der Datenschutzrechtsordnungen' (2020) 84(4) RabelsZ 864.

Hoffmann T, 'Data Protection Act(ion): Report on the Law of Data Disclosure in Ghana' (2022) 22(1) University of Passau IRDG Research Paper Series.

— 'Data Protection by Definition: Report on the Law of Data Disclosure in Japan' (2022) 22(3) University of Passau IRDG Research Paper Series.

— 'The Laws of Data Disclosure: Examining the Regulation of Individuals' Personal Data Disclosure in Brazil, China, the European Union, Ghana, Japan, Russia, Switzerland and the United States of America' in Moritz Hennemann and others (eds), *Data disclosure: Global developments and perspectives* (Global and Comparative Data Law Volume 2, De Gruyter 2023).

Hoffmann T and Pietrobon de Moraes Vargas PL, 'LGPD Et Al.: Report on the Law of Data Disclosure in Brazil' (2022) 22(6) University of Passau IRDG Research Paper Series.

Hümmer C, *Die Reputation interner Dienstleister in Konzernen* (Business-to-Business-Marketing, 2015).

Kahneman D, *Attention and effort* (Prentice Hall series in experimental psychology, Prentice Hall 1973).

Kahneman D and Tversky A, 'Prospect Theory: An Analysis of Decision under Risk' (1979) 47(2) Econometrica 263.

Karpoff JM, 'Does Reputation Work to Discipline Corporate Misconduct?' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012).

Kho B-C, Stulz RM and Warnock FE, 'Financial Globalization, Governance, and the Evolution of the Home Bias' (2009) 47(2) JAccountRes 597.

Kischel U, *Rechtsvergleichung* (C.H. Beck 2015).

Lintvedt MN, 'Putting a price on data protection infringement' (2022) 12(1) IDataPrivL 1.

Mahon JF, 'Corporate Reputation' (2002) 41(4) Bus&Soc'y 415.

Mankiw NG, *Principles of macroeconomics* (Cengage Learning 2021).

McCorkindale T and Distaso MW, 'The Power of Social Media and Its Influence on Corporate Reputation' in Craig E Carroll (ed), *The Handbook of Communication and Corporate Reputation* (Blackwell Publishing Ltd 2013).

Noe T, 'A Survey of the Economic Theory of Reputation: Its Logic and Limits' in Michael L Barnett (ed), *The Oxford handbook of corporate reputation* (1st edn, Oxford Univ Press 2012).

Personal Information Protection Commission Japan, 'Laws and Policies' (2023) <https://www.ppc.go.jp/en/legal/> accessed 4 August 2023.

— 'List of Authorized Personal Information Protection Organizations (transl.)' (8 February 2023) <https://www.ppc.go.jp/personalinfo/nintei/list/> accessed 8 February 2023.

Pratt G, Annear R and Gillert A, 'Naming and shaming? The UK ICO is now naming most organisations it investigates' (31 January 2023) <https://technologyquotient.freshfields.com/post/102i6m7/naming-and-shaming-the-uk-ico-is-now-naming-most-organisations-it-investigates> accessed 4 August 2023.

Rubin AM, 'An Examination of Television Viewing Motivations' (1981) 8(2) Communication Research 141.

Salaymeh L and Michaels R, 'Decolonial Comparative Law: A Conceptual Beginning' (2022) 86(1) RabelsZ 166.

Samuelson W and Zeckhauser R, 'Status quo bias in decision making' (1988) 1 JRiskUncertain 7.

Schwaiger M and Raithel S, 'Reputation und Unternehmenserfolg' (2014) 64(4) MRQ 225.

Selzer A, Woods D and Böhme R, 'Practitioners' Corner – An Economic Analysis of Appropriateness under Article 32 GDPR' (2021) 7(3) EDPL 456.

Shapira R, *Law and Reputation* (Cambridge University Press 2020).

Sonnenberg P and Hoffmann T, 'Data Protection Revisited: Report on the Law of Data Disclosure in Switzerland' (2022) 22(17) University of Passau IRDG Research Paper Series.

Trepte S and others, 'Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale"' in Serge Gutwirth and others (eds), *Reforming European Data Protection Law* (Springer Netherlands 2015).

Tversky A and Kahneman D, 'Judgment under Uncertainty: Heuristics and Biases' (1974) 185(4157) Science 1124.

UK Information Commissioner's Office, 'Action we've taken' (2023) <https://ico.org.uk/action-weve-taken/> accessed 4 August 2023.

— 'Five businesses fined a total of £435,000 for making nearly half a million unlawful marketing calls' (7 December 2022) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/12/five-businesses-fined-a-total-of-435-000-for-making-nearly-half-a-million-unlawful-marketing-calls/> accessed 4 August 2023.

United Nations General Assembly (UNGA), *Aggression against Ukraine* (01.03.2022) UN Doc A/ES-11/L.1.

— *Principles of the Charter of the United Nations underlying a comprehensive, just and lasting peace in Ukraine* (16.02.2023) UN Doc A/ES-11/L.7.

Varma TM, 'Responsible Leadership and Reputation Management During a Crisis: The Cases of Delta and United Airlines' (2021) 173(1) JBusEthics 29.

Walker K, 'A Systematic Review of the Corporate Reputation Literature: Definition, Measurement, and Theory' (2010) 12(4) CorpReputRev 357.

Wang F, 'Cooperative Data Privacy: The Japanese Model of Data Privacy and the EU-Japan GDPR Adequacy Agreement' (2020) 33(2) HarvJL&Tech 661.

Wawra D and others, 'Cultural Influences on Personal Data Disclosure Decisions – Japanese Perspectives' [2022] <https://ssrn.com/abstract=4079634> accessed 4 August 2023.

Yadin S, 'Regulatory Shaming' (2019) 49(2) EnvtlL 407–451.

Der Facebook-Beschluss des BGH – Datenschutz durch Wettbewerbsrecht?

Tom Schmidt

Zusammenfassung

Dieser Beitrag betrachtet eine vom BGH in seinem Beschluss vom 23.06.2020 neu entwickelte Fallgruppe des § 19 I GWB und arbeitet dabei insbesondere deren dreigliedriges Prüfungsschema heraus. Gezeigt wird sowohl, wie die Verknüpfung von Wertungen des Datenschutzrechts und Instrumenten des Kartellrechts gelingt, als auch wie der BGH vermeidet, auf die Feststellung eines außerkartellrechtlichen Verstoßes gegen rein datenschutzrechtliche Normen, wie die DSGVO, angewiesen zu sein. Schlussendlich wird das Potential und der Bedarf einer solchen Verbindung zwischen Datenschutz und Wettbewerbsrecht diskutiert und darauf hingewiesen, dass einige zentrale Fragen der neuen Fallgruppe, insbesondere mit Blick auf das angemessene Alternativszenario im funktionierenden Wettbewerb, offen bleiben. In diesem letzten Punkt wird jedoch der weitere Verfahrensverlauf vermutlich Klärung bringen können.

1. Einleitung

Ein in den letzten Jahren immer wichtiger werdender Schnittpunkt zwischen Datenschutz- und Wettbewerbsrecht ist die Überlegung, dass die von der datenschutzrechtlichen Ordnung geforderte „substantielle […] Entscheidungsbefugnis des Betroffenen über die Verwendung seiner personenbezogenen Daten“[1] durch die erdrückende Marktmacht einzelner Plattformanbieter (sowie die damit potentiell einhergehenden Netzwerkeffekte) effektiv stark reduziert wird. Zusätzlich besteht bei Geschäftsmodellen, die sich durch die Monetarisierung ihrer Nutzerdaten finanzieren (“Daten gegen Leistung”), der Anreiz, dieses Machtungleichgewicht auch zur

1 BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 104, 106; Diese Formulierung geht auf den Wortlaut des Volkszählungsurteils zurück vgl. BVerfGE 65, 1 Rn. 147.

Durchsetzung einer einseitig definierten, möglichst weitreichenden Datensammlung und -verarbeitung zu nutzen.

Während sich diese Problematik auf datenschutzrechtlicher Seite in Fragen rund um die Freiwilligkeit der Einwilligung in die Verarbeitung personenbezogener Daten i.S.d. Art. 4 Nr. 11 DSGVO und des damit verbundenen EG 43 DSGVO kristallisiert hat (bei den oben bereits erwähnten Geschäftsmodellen flankiert von Streitigkeiten um das sogenannte "Kopplungsverbot" des Art. 7 IV DSGVO),[2] wurde die komplementäre Frage nach einer wettbewerbsrechtlichen Regulierung spätestens 2019 auf die Tagesordnung gesetzt, als das Bundeskartellamt (BKartA) ein Verfahren in dieser Hinsicht gegen Meta Platforms (Meta)[3] eröffnete.

Der vorläufige Höhepunkt in diesem Verfahren ist ein am 23.06.2020 im Eilverfahren vom Bundesgerichtshof (BGH) getroffener Beschluss, welcher auch darüber hinaus weitreichende Auswirkungen auf die zukünftige Regulierung von Marktmachteffekten in Aussicht stellt.[4] Denn während das BKartA sich noch auf die in den „Gegenwert"-Entscheidungen des BGH 2013 und 2017 entwickelte Konstruktion einer „qualitativen Konditionenkontrolle" stützte, und somit auf die inzidente Prüfung und Feststellung eines Verstoßes gegen die DSGVO angewiesen war,[5] weicht der BGH nunmehr von der Argumentation des BKartA ab und entwickelt unter Verwendung des Begriffs der „aufgedrängten Leistungserweiterung" eine neue Fallgruppe des § 19 I GWB,[6] mit welcher er in der Lage ist, datenschutzrechtlichen Wertungen auch ohne inzidente Prüfung und Feststellung eines DSGVO-Verstoßes Rechnung zu tragen. Die Missbrauchskontrolle des § 19 I GWB wird damit als eigenständiges und zum Datenschutzrecht (nicht

2 Vgl. *Kühling* u.a., Datenschutzrecht, 2021 Rn. 376; Zu Beginn wurde das „Kopplungsverbot" teilweise gar als „kaum zu überwindende Hürde" für das Geschäftsmodell betrachtete vgl. *Krohm/Müller-Peltzer*, ZD 2017, 551 (553). Dabei steht insbesondere in Frage, ob der Art. 7 IV DSGVO nur in Fällen greift, in denen „der Verbraucher auf die angebotene Leistung in besonderer Weise angewiesen ist" und über keinen „zumutbaren Zugang" zu einer gleichwertigen Alternative ohne entsprechende Einwilligungserfordernis verfügt vgl. *Klement*, in: Simitis u.a. (Hrsg.), Datenschutzrecht 2019, Art. 7 DSGVO, Rn. 61 oder ob das in Frage stehende Geschäftsmodell in Gänze vom Anwendungsbereich des Art. 7 IV DSGVO ausgenommen ist, da hier die „Datenverarbeitung selbst zum Gegenstand des Vertrags" gemacht wird vgl. *Kühling* u.a., Datenschutzrecht, 2021 Rn. 514 und *Frenzel*, in: Paal/Pauly (Hrsg.) Datenschutzgrundverordnung 2021, Art. 7 DSGVO Rn. 21.

3 Damals hieß der Konzern noch wie das soziale Netzwerk „Facebook".

4 Vgl. *Podzun*, GRUR 2020, 1268 (1268, 1276) und *Körber*, NZKart 2019, 187 (190f.).

5 Vgl. BKartA, Beschluss vom 06.02.2019 – B6-22/16, Rn. 523 und 524.

6 Vgl. *Podzun*, GRUR 2020, 1268 (1270).

jedoch zu dessen Wertungen!) parallellaufendes Instrument in Stellung gebracht.

Um einen genaueren Blick auf dieses Instrument zu ermöglichen, wird im folgenden Beitrag zunächst die prozessuale Entstehungsgeschichte der neue Fallgruppe nachvollzogen (Abschn. 2) bevor ihre Struktur rekonstruiert (Abschn. 3), ihr Verhältnis zur DSGVO untersucht (Abschn. 4) und ein Ausblick zur weiteren Entwicklung gegeben wird (Abschn. 5).

2. Prozessuale Entstehungsgeschichte

Inhaltlich dreht sich das noch laufende Verfahren des BKartA gegen Meta um die Nutzungsbedingungen des sozialen Netzwerks "Facebook", welche dem Nutzer abverlangen, in die kombinierte Verwendung und Verknüpfung von sogenannten „On-" und „Off-Facebook"-Daten einzuwilligen.[7] Während „On-Facebook"-Daten sich nur aus solchen zusammensetzen, welche der Konzern über seine Nutzer erlangt, während diese das soziale Netzwerk als solches nutzen, umfassen "Off-Facebook"-Daten auch solche, die der Konzern über die Nutzer durch den Betrieb seiner anderen Dienste (wie "WhatsApp", "Instagram" oder die "Facebook Business Tools"), sammelt.[8]

Bereits Anfang 2016 eröffnete das BKartA deswegen ein Verfahren, aus welchem am 06.02.2019 eine Untersagungsverfügung hervorging.[9] Darin wurde dem Konzern verboten, Nutzungsbedingungen zu verwenden, welche die Nutzung des sozialen Netzwerks Facebook davon abhängig machen, in die Verwendung und Verknüpfung von „On-" und „Off-Facebook"-Daten einzuwilligen, sowie die entsprechende Datenverarbeitung durchzuführen.[10] Meta legte daraufhin Beschwerde ein und erreichte im einstweiligen Rechtsschutz die Anordnung der aufschiebenden Wirkung der Beschwerde durch das Oberlandesgericht in Düsseldorf am 26.08.2019.[11] Auf Antrag des BKartA hob der BGH am 23.06.2020 den Beschluss des Beschwerdegerichts jedoch unter Entwicklung der hier diskutierten Fall-

7 BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 2-4.
8 Mit einer guten Erklärung zu beiden Begriffen: *Mackenrodt*, ZUM 2021, 89 (90).
9 BKartA, Beschluss vom 06.02.2019 – B6-22/16.
10 BKartA, Beschluss vom 06.02.2019 – B6-22/16, Rn. 916ff.
11 OLG Düsseldorf, Beschluss vom 26.08.2019 – Kart 1/19 (V), Rn. 22.

gruppe wieder auf.[12] In der Hauptsache hat das Beschwerdegericht das Verfahren mittlerweile ausgesetzt (24.03.2021), um dem EuGH einige im Vorhinein zu klärende Fragen vorzulegen.[13] Die entsprechenden Schlussanträge des Generalanwalts der EU wurden am 20.09.2022 veröffentlicht und bekräftigen sowohl das Vorgehen des BKartA als auch des BGH.[14]

3. Neue Fallgruppe des § 19 I GWB

Im konkreten Fall prüft der BGH das Vorliegen einer missbräuchlichen Ausnutzung i.S.d. § 19 GWB in drei Schritten: Zunächst wird festgestellt, dass durch die marktbeherrschende Stellung Facebooks eine Zwangslage für private Nutzer entsteht, aus welcher in Verbindung mit der Verpflichtung, den beanstandeten Konditionen zur Nutzung des Netzwerks zuzustimmen, eine „Leistungserweiterung" resultiert, die nicht mehr durch das Verhalten der Nutzer beeinflussbar und somit „aufgedrängt" ist.[15] Daraufhin bejaht der BGH die „kartellrechtliche Relevanz" der aufgedrängten Leistungserweiterung, da sich aus dieser „wettbewerbsschädliche Wirkungen" ergeben.[16] Abschließend nimmt er eine umfassende Interessenabwägung vor und kommt zu dem Ergebnis, dass die aufgedrängte Leistungserweiterung weiterhin auch missbräuchlich ist.[17] Abstrakt gesprochen wird somit geprüft, (1.) ob ein potentiell schädliches Verhalten vorliegt, welches in einem durch den Wettbewerb nicht hinreichend kontrollierten Handlungsspielraum liegt, (2.) ob dieses Verhalten sich auch als kartellrechtlich relevante Ausnutzung dieses Spielraums erweist und (3.) ob es nach umfassender Abwägung aller betroffenen Interessen überdies als missbräuchlich anzusehen ist. Dieser Prüfungsaufbau bildet den Schutzzweck des § 19 I GWB, die „missbräuchliche Ausnutzung nicht hinreichend vom Wettbewerb kontrollierter Handlungsspielräume" zu unterbinden,[18] genau ab.

Trotzdem wird in der bisherigen Literatur diese Systematik nicht explizit nachvollzogen. Stattdessen werden die Prüfungsschritte bei der Bespre-

12 BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 10.
13 OLG Düsseldorf, Pressemitteilung vom 24.03.2021
14 Generalanwalt beim EuGH, Schlussanträge vom 20.09.2022 – C-252/21, Rn. 22.
15 Vgl. BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 58.
16 Vgl. BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 59 und 64.
17 Vgl. BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 97.
18 BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 74; *Fuchs*, in: Immenga/Mestmäcker (Hrsg.), Wettbewerbsrecht, 2020, § 19 GWB, Rn. 21. AZ

chung des Argumentationsgangs nur vereinzelt thematisiert und dabei teilweise verkannt.[19]

3.1 Potentiell schädliches Verhalten

Hier zeigt der BGH zunächst auf, dass die beanstandeten Konditionen, entgegen der Ansicht des Beschwerdegerichts, einen Kontrollverlust der Nutzer bedeuten und für diese somit eine Zwangslage begründen.[20] Schließlich wird denjenigen, „die auf die Benutzung des sozialen Netzwerks nicht verzichten wollen, die aber auch Wert darauf legen, dass sich die Erhebung und die Verarbeitung von Daten auf [ein Minimum] beschränkt", mit dem „personalisierten Erlebnis" auf Grundlage der „Off-Facebook"-Daten „ein Leistungsinhalt aufgedrängt, den sie möglicherweise nicht wünschen".[21] Dieser aufgrund der erdrückenden Marktmacht des sozialen Netzwerks nicht vorhandenen oder zumindest übermäßig eingeschränkten Kontrolle der Nutzer bei der Vereinbarung zusätzlicher Leistungsinhalte entspricht auf der anderen Seite ein vom Wettbewerb nicht oder nicht hinreichend kontrollierter Handlungsspielraum – hier Metas bei der Festlegung und Vereinbarung dieser Leistungsinhalte durch Definition der Nutzungsbedingungen Facebooks.

19 Auf diese Weise findet sich die Trennung des ersten vom zweiten Prüfungsschritt schon bei *Podzun*, GRUR 2020, 1268 (1270), *Marx,* jurisPR-ITR 21/2020 Anm. 6 und *Walzel,* CR 2020, 660 (675). Verkannt wird diese bei *Mackenrodt*, ZUM 2021, 89 *(*93). Ebenso findet sich die Trennung des zweiten vom dritten Prüfungsschritt bereits bei *Lepsius,* WuW 2020, 566 (567). Verkannt wird sie jedoch bei *Podzun,* GRUR 2020, 1268 (1272) (welcher der Interessenabwägung nur eine Kontrollfunktion neben dem Begriff des ‚Missbrauchs' zumisst). Wie wenig Augenmerk auf eine klare Rekonstruktion der Systematik der neuen Fallgruppe gelegt wurde, demonstriert insbesondere *Lettl*, WRP 2020, 1391: Hier werden alle drei Prüfungsschritte zunächst korrekt erkannt (Rn. 8-9), nur um daraufhin die Trennung zwischen dem zweiten und dritten Schritt wieder zu verwischen (Rn. 10). Dabei ist gerade ein robustes Verständnis des systematischen Aufbaus der neuen Fallgruppe des § 19 I GWB notwendig, um die kontroverse Diskussion über ihre Bedeutung und genaue Ausgestaltung zu ordnen und dadurch fruchtbar zu machen.

20 BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 57.

21 BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 58.

3.2 Wettbewerbsschädliche Auswirkungen

Nachdem der BGH feststellt, dass sowohl vertikale (Ausbeutung) als auch horizontale (Behinderung) wettbewerbsschädliche Auswirkungen in diesem Schritt genügen sollen, bejaht er mit Blick auf die zusätzliche Datenverarbeitung, welche Meta durch die "aufgedrängte Leistungserweiterung" ermöglicht wird, sowohl eine Ausbeutung der Nutzer als auch eine Behinderung des Wettbewerbs.[22] Das zentrale Problem mit Hinsicht auf letztere war im Vorhinein, dass es durch den erdrückenden Marktanteil Facebooks und die damit einhergehenden Netzwerkeffekte stets fast unmöglich sein wird, konkrete Auswirkungen eines vermutlich viel kleineren Faktors nachzuweisen.[23] Der BGH umgeht dieses Problem und lässt die "objektive Eignung" zur „spürbaren Beeinträchtigung der Marktverhältnisse" genügen.[24] Auch die Ausbeutung privater Nutzer war im Vorhinein bezweifelt worden, insbesondere da die Preisgabe ihrer Daten diese nicht wirtschaftlich schwächt.[25] Der BGH hält dem nun entgegen, dass für die kartellrechtliche Beurteilung die Ermöglichung zur Verarbeitung personenbezogener Daten als wirtschaftliche Gegenleistung anzusehen ist, welche bei einer erweiterten Datenverarbeitung erhöht wird.[26]

Nicht klar ausgearbeitet bleibt das Alternativszenario, mit welchem die Datensammlung des Konzerns verglichen wird. Der BGH zieht hier aus Umfrageergebnissen zu den Datenverarbeitungspräferenzen der Facebook-Nutzer den Schluss, dass unter Bedingungen eines „funktionierenden Wettbewerbs" Angebote verfügbar wären, welche den „Nutzerpräferenzen für eine stärkere Autonomie bei der Gestattung des Zugriffs auf Daten" Rechnung tragen würden.[27] Der Argumentationsgang schließt dabei jedoch etwaige „Lock-In-Effekte" im Alternativszenario prinzipiell aus,[28] obwohl solche Wechselhürden auch bereits bei einem deutlich geringeren Marktanteil des sozialen Netzwerks auftreten könnten (wenn auch in abgeschwächter Form). Inwieweit die für den § 19 I GWB ausschlaggebende marktbeherr-

22 BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 64.
23 Deswegen Behinderungswirkungen ablehnend: *Körber*, NZKart 2019, 187 (192).
24 Vgl. BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 83, 93.
25 So etwa: OLG Düsseldorf, Beschluss vom 26.08.2019 – Kart 1/19 (V) I, Rn. 31-33; *Körber*, NZKart 2019, 187 (191).
26 Vgl. BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 62.
27 Vgl. BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 85-86.
28 Vgl. BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 86.

schende Stellung Facebooks für die vermehrte Datenverarbeitung ursächlich ist, bleibt somit fraglich.

3.3 Missbräuchlichkeit der Ausnutzung

Im letzten Schritt nimmt der BGH eine umfassende „Würdigung und Abwägung der betroffenen Interessen" vor, um die Missbräuchlichkeit der durch die vorherigen Schritte bereits belegten Ausnutzung einer marktbeherrschenden Stellung festzustellen.[29] Dabei überwiegt schlussendlich das Interesse der Nutzer, „die Verarbeitung ihrer Daten auf das für die Nutzung des sozialen Netzwerks erforderliche Maß beschränken zu können" das Interesse Facebooks, „sein Leistungsangebot nach eigenen Vorstellungen zu gestalten".[30]

4. Verhältnis zu DSGVO

Der BGH befasst sich erst im Rahmen der umfassenden Interessenabwägung des dritten Prüfungsschritts explizit mit datenschutzrechtlichen Wertungen und Normen. Er prüft folglich auch keinen datenschutzrechtlichen Verstoß.[31] Stattdessen wird die DSGVO nur herangezogen, da durch diese missbilligte Interessen nicht berücksichtigt werden dürfen und die Wertentscheidungen, welche der DSGVO zugrunde liegen, eine Konkretisierung der objektiven Wertordnung durch das Grundrecht auf informationelle Selbstbestimmung darstellen.[32] Unter diesen Gesichtspunkten diskutiert der BGH mehrere Erlaubnistatbestände des Art. 6 I DSGVO. Der Unterschied zur inzidenten Prüfung eines datenschutzrechtlichen Verstoßes tritt dabei besonders in der Behandlung des Art. 6 I a DSGVO zu Tage: Anstatt die Wirksamkeit der Einwilligung in die Nutzungsbedingungen Facebooks zu prüfen, führt der BGH die entscheidenden Normen[33] nur an, um die Bedeutung einer "substantiellen Entscheidungsbefugnis" der privaten Nutzer zu untermauern.[34] Daraus ergeben sich zwei wichtige Konsequenzen: Zum einen werden grundlegende Fragen zum Verhältnis von Marktmacht

29 BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 97-98
30 BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 120-121.
31 Vgl. *Podzun*, GRUR 2020, 1268 (1270 und 1275).
32 Vgl. BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 99 und 106ff.
33 Gemeint sind Art. 4 Nr. 11 DSGVO, Art. 6 I a DSGVO, EG 43 DSGVO.
34 Vgl. BGH, Beschluss vom 23.06.2020 – KVR 69/19, Rn. 106-108.

und Freiwilligkeit der Einwilligung i.S.d. Art. 4 Nr. 11 DSGVO weiterhin offen gehalten. Zum anderen wird deutlich, dass im Rahmen der neu entwickelten Fallgruppe bereits jetzt den Wertungen des Datenschutzrechts Rechnung getragen werden kann, ohne Fragen des Datenschutzrechts im engeren Sinne zu präjudizieren.

5. Fazit und Ausblick

Das zentrale Problem des Facebook-Sachverhalts liegt darin, dass durch die erdrückende Marktmacht des Konzerns und die damit verbundenen, starken Netzwerkeffekte aus Sicht des einzelnen Nutzers eine Zwangslage entsteht, in welcher dessen effektive Entscheidungsbefugnis über die Verarbeitung seiner personenbezogenen Daten stark eingeschränkt wird, zumindest insoweit er auf die angebotene Leistung nicht verzichten kann oder will. Bezüglich der Datenverarbeitung, welche zur technischen Funktion des Netzwerks notwendig ist, mag dies tautologisch klingen und nicht zu verhindern sein. Darüber hinaus kann es jedoch nicht als wünschenswert erachtet werden, dass große Plattformanbieter ihre gesamte Marktmacht zur Durchsetzung einer einseitig festgelegten Datenverarbeitung verwenden können. Dies gilt insbesondere in Anbetracht der hohen finanziellen Anreize datengetriebener Geschäftsmodelle.

Der Ansatz des BGH, datenschutzrechtlichen Wertungen innerhalb des Wettbewerbsrechts auch ohne inzidente Prüfung eines datenschutzrechtlichen Verstoßes Rechnung zu tragen, stellt nun ein neues Instrument in Aussicht, um diese Problematik asymmetrischer Machtverhältnisse zwischen Nutzern und Plattformanbietern zu adressieren. Mit Blick auf die informationelle Selbstbestimmung der Endnutzer ist eine solche Entwicklung nur zu begrüßen, insbesondere da die DSGVO selbst nicht zwischen verschiedenen Unternehmen differenziert und somit Marktmachteffekte nur schwer berücksichtigen kann.[35]

Leider bleibt gerade bei der zentralen Frage des korrekten Alternativszenarios weiterhin ein großes Fragezeichen zurück, sodass die tatsächliche Tragfähigkeit der neuen Fallgruppe vermutlich erst beurteilt werden kann, wenn der BGH auch in der Hauptsache die Chance bekommen hat, seine Ansichten vollständig darzulegen. Hier muss die wegweisende

35 Hierzu ist die Diskussion in *Kerber/Zolna*, European Journal of Law and Economics 2022, 217 (232-234) zu empfehlen.

Entscheidung getroffen werden, ob mit dem Begriff des „funktionierenden Wettbewerbs" nur ein Szenario gemeint ist, in dem der Normadressat keine marktbeherrschende Stellung inne hat, oder ob gar ein Idealzustand ohne Marktunvollkommenheit (wie z.B. Lock-In-Effekte) konstruiert wird.

Literatur

Fuchs, Andreas (2020): § 19 GWB. In: Immenga, Ulrich/Mestmäcker, Ernst-Joachim (akutell hrsgg.v. Körber, Torsten/Schweitzer, Heike/Zimmer, Daniel): Wettbewerbsrecht. München: C. H. Beck.

Frenzel, Eike Michael (2021): DS-GVO Art. 7 Bedingungen für die Einwilligung. In: Paal, Boris P.; Pauly, Daniel A. (Hrsg.): Beck'sche Kompakt Kommentare Datenschutz-Grundverordnung. Bundesdatenschutzgesetz. München: C.H. Beck.

Kerber, Wolfgang und Zolna, Karsten (2022): The German Facebook case: the law and economics of the relationship between competition and data protection law. *European Journal of Law and Economics* 2022, S. 217–250.

Klement, Jan Henrick (2019): Art. 7 Datenschutz-Grundverordnung [Einwilligung]. In: Simitis, Spiros; Hornung, Gerrit und Spieker genannt Döhmann, Indra (Hrsg.): Kommentar Datenschutzrecht (DSGVO mit BDSG). Baden-Baden: Nomos.

Körber, Torsten (2019): Die Facebook-Entscheidung des Bundeskartellamtes – Machtmissbrauch durch Verletzung des Datenschutzrechts?. *Neue Zeitschrift für Kartellrecht (NZKart)* 2019, S. 187-195.

Krohm, Niclas und Müller-Peltzer, Phillip (2017): Auswirkungen des Kopplungsverbots auf die Praxistauglichkeit der Einwilligung – Das Aus für das Modell „Service gegen Daten"?. *Zeitschrift für Datenschutz (ZD)* 2017, S. 551-556.

Kühling, Jürgen; Klar, Manuel; Sackmann, Florian (2021): *Datenschutzrecht.* Heidelberg: C.F. Müller.

Lepsius, Oliver (2020): Der Facebook-Beschluss des BGH aus der Sicht des Verfassungsrechts. *Wirtschaft undWettbewerb (WuW)* 2020, S. 566-569.

Lettl, Tobias (2020): Art. 102 AEUV, § 19 GWB und Rechtsbruch, insbesondere Verstöße gegen AGB-Recht und Datenschutzrecht. *Wettbewerb in Recht und Praxis (WRP)* 2020, S. 1391-1400.

Mackenrodt, Mark-Oliver (2021): Zur kartellrechtlichen Bewertung der Datenverarbeitung durch Facebook und ihrer normativen Kohärenz mit dem Datenschutzrecht und dem Datenschuldrecht. *Zeitschrift für Urheber- und Medienrecht (ZUM)* 2021, S. 89-103.

Marx, Lorenz (2020):Plattformübergreifende Sammlung von nutzerbezogenen Daten: Missbräuchliche Ausnutzung einer marktbeherrschenden Stellung durch Facebook. *juris PraxisReport IT-Recht (jurisPR-ITR)* 21/2020 Anm. 6.

OLG Düsseldorf (24. März 2021) „Facebook gegen Bundeskartellamt: Ergebnisse des Verhandlungstermins", Pressemitteilung. https://www.d-kart.de/wp-content/uploads/2021/03/OLG-Duesseldorf-Pressemitteilung-v.-24.03.2021-Nr.-92021.pdf

Podzun, Rupprecht (2020): Der Verbraucher als Marktakteur: Kartellrecht und Datenschutz in der „Facebook" - Entscheidung des BGH. *Gewerblicher Rechtsschutz und Urheberrecht (GRUR)* 2020, S. 1268-1276.

Walzel, Daisy (2020): Urteilsanmerkung zum Urteil des BGH-Beschluss vom 23.06.2020 – KVR 69/19, *Computer und Recht (CR)* 2020, S. 660-676.

Anforderungen an die automatisierte Protokollierung von Datenverarbeitungstätigkeiten in einem Transaktionsjournal: eine Multi-Stakeholder-Perspektive auf Motivation und Umsetzung

Lars Pfeiffer, Stefanie Astfalk, Lorenz Baum, Björn Hanneke, Christian H. Schunck und Matthias Winterstetter

Zusammenfassung

In der Digitalwirtschaft besteht ein erhebliches Bedürfnis nach sowohl effektiven als auch effizienten Lösungen, um datenbasierte Geschäftsmodelle mit den hohen europäischen Datenschutz-Standards in Einklang zu bringen. Hierbei stellen einerseits die Förderung von Transparenz und Intervenierbarkeit für die betroffenen Personen sowie andererseits der Ressourcenaufwand zur Einhaltung der rechtlichen Vorgaben für – insbesondere kleine und mittlere – Unternehmen wesentliche Herausforderungen dar. Personal Rights Management (PRM)-Systeme können bei der Adressierung dieser Herausforderungen unterstützen, indem sie auf einen vermittelnden Ansatz abzielen, der den Interessen aller Stakeholder gerecht wird. Dieser Beitrag beschreibt aus einer datenschutzrechtlichen, sozioökonomischen und technischen Perspektive die Motivation für und die Multi-Stakeholder-Anforderungen an die Komponente des Transaktionsjournals zur automatisierten Protokollierung von Datenverarbeitungstätigkeiten im Rahmen eines PRM-Systems. Betroffene erhalten durch das Transaktionsjournal eine nachvollziehbare Darstellung dessen, was mit ihren Daten geschieht, was die jeweilige Verarbeitungstätigkeit legitimiert und welche Interventionsmöglichkeiten ihnen zur Verfügung stehen. Unternehmen profitieren von einem besseren Überblick ihrer Datenverarbeitungstätigkeiten und der Förderung ihrer Fähigkeit zum Nachweis der Einhaltung ausgewählter datenschutzrechtlicher Anforderungen.

1. Einführung – Fortbestehende Datenschutzprobleme in der Praxis

In der Digitalwirtschaft besteht ein erhebliches Bedürfnis nach technischen sowie ökonomischen Lösungsansätzen, um die seit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) hohen europäischen Standards zum Privatsphärenschutz mit datengetriebenen Geschäftsmodellen in Einklang zu bringen. Gerade in der Plattformökonomie[1] kann die ressourcenbindende Einhaltung der Vorgaben aus der DSGVO, insbesondere für kleinere Plattformbetreiber,[2] eine Hürde bedeuten. Allerdings sehen sich nicht nur kleine Unternehmen Schwierigkeiten gegenüber – selbst große digitale Plattformen haben Probleme, ihre Datenbestände und deren rechtmäßige Verarbeitung zu kontrollieren, sich der Rechtskonformität ihrer Tätigkeiten zu vergewissern und ihren Dokumentationspflichten nachzukommen.[3] Neben dieser unternehmenszentrierten Perspektive führt die Vielzahl der über eine Plattform interagierenden Akteure zu zahlreichen unterschiedlichen Datenströmen und Möglichkeiten der Datenweitergabe, was aus Sicht der betroffenen Personen die Nachvollziehbarkeit der Datenverarbeitung erschwert. Dabei sind selbst abseits der Plattformökonomie die datenschutzrechtlichen Transparenzprobleme in der Praxis immer noch nicht zufriedenstellend gelöst – beispielsweise werden regelmäßig weder Einwilligungen „in Kenntnis der Sachlage" (ErwGr. 42 DSGVO) erteilt, noch wird die Nachvollziehbarkeit der gesamten Datenverarbeitung gewährleistet, womit es auch an der Voraussetzung für eine effektive Nachprüfbarkeit von deren Rechtmäßigkeit (ErwGr. 63 DSGVO) mangelt.

Um die von den Plattformkunden gewünschten Services anzubieten, können Plattformbetreiber in der Regel nicht auf die Verarbeitung personenbezogener Daten verzichten, weshalb auch die Anwendung des in der Privacy-Forschung besonders intensiv betrachteten Konzepts der Anonymisierung (z.T. auch als Schutzziel der „Unverkettbarkeit[4] bezeichnet) weitgehend impraktikabel ist. Aus diesem Grund hat das vom *Bundesministerium für Bildung und Forschung* (*BMBF*) geförderte Forschungsprojekt

1 Für eine ausführliche Darstellung von Charakteristika, Funktionen und Herausforderungen digitaler Plattformen s. *Engert*, AcP 2018, 304 (304 ff.).

2 In diesem Beitrag wird aus Gründen der Vereinfachung und besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich eingeschlossen.

3 S. exemplarisch zu Facebook *Lang*, Facebook hat keine Kontrolle über seine Daten, Netzpolitik v. 30. Apr. 2022.

4 *Zibuschka u. a.*, in: Roßnagel u. a. (Hrsg.), Open Identity Summit, 2019, 71-82.

PERISCOPE[5] das Ziel, „privatsphärenfreundliche Geschäftsmodelle für die Plattformökonomie“ insbesondere durch die Stärkung von Transparenz und Intervenierbarkeit zu ermöglichen. Dabei wird dieses Problemfeld u. a. durch die Implementierung eines Transaktionsjournals adressiert, das über die Transparenzanforderungen aus der DSGVO hinausgehend eine tatsächliche Informiertheit der betroffenen Personen herstellen und damit die Nachvollziehbarkeit aller relevanten Datenverarbeitungstätigkeiten fördern soll. Durch Anreicherung der dargestellten Verarbeitungsvorgänge mit weiteren Informationen wie Zweck und Rechtsgrundlage der jeweiligen Datenverarbeitung sowie auch der den betroffenen Personen jeweils zustehenden Interventionsmöglichkeiten, wird zugleich auch eine Förderung des Schutzziels der Intervenierbarkeit verfolgt.

In diesem Beitrag stellen wir erste Ergebnisse von Studien zur Motivation für und zu Multi-Stakeholder-Anforderungen an den Einsatz eines solchen Transaktionsjournals vor. Dabei ist der Beitrag folgendermaßen strukturiert: In den Abschnitten 2 und 3 werden wichtige Praxisprobleme bei der Umsetzung der DSGVO – vor allem, aber nicht ausschließlich – in der Plattformökonomie diskutiert. Der Fokus liegt dabei auf Transparenz und Intervenierbarkeit für die betroffene Person und einem potenziell die Wettbewerbsfähigkeit bedrohenden Ressourcenaufwand für kleinere Unternehmen. In Abschnitt 4 gehen wir darauf ein, wie diese Herausforderungen mit Hilfe eines Personal Rights Management (PRM)-Systems, das eine automatische Protokollierung von Verarbeitungstätigkeiten umfasst, angegangen werden können. Die dazu erhobenen Multi-Stakeholder-Anforderungen werden auszugsweise in Abschnitt 5 vorgestellt. Der Beitrag schließt mit einem Fazit und Ausblick.

2. Praxisproblem I: Transparenz und Intervenierbarkeit für die betroffene Person

Gemäß dem „grundrechtlich determinierten“[6] Transparenzgrundsatz aus Art. 5 Abs. 1 lit. a Alt. 3 DSGVO ist die Verarbeitung personenbezogener Daten in einer für die betroffenen Person nachvollziehbaren Weise vorzu-

5 Förderkennzeichen: 16KIS1479K; für mehr Informationen s. https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/periscope.

6 *Greve*, in: Sydow/Marsch (Hrsg.), DSGVO | BDSG, 3. Aufl. 2022, Art. 12 DSGVO Rn. 5.

nehmen. Die Aufnahme des Transparenzgrundsatzes an dieser prominenten Stelle der Verordnung spiegelt damit die Bedeutung, die Transparenz im Allgemeinem zugeschrieben wird. So wird sie etwa als Grundvoraussetzung für das Recht auf informationelle Selbstbestimmung[7] oder sogar als „konstitutiv für das gesamte Datenschutzrecht"[8] angesehen. Wie auch die anderen in Art. 5 DSGVO enthaltenen Grundsätze der Datenverarbeitung entfaltet das Transparenzgebot Wirkung für alle nachfolgenden Vorschriften der DSGVO und ist bei deren Anwendung zu beachten – anderenfalls ist die entsprechende Datenverarbeitung rechtswidrig.[9] Insofern handelt es sich zwar um eine unmittelbar geltende Pflicht für den Datenverarbeiter,[10] zugleich wird allerdings die Konkretisierungsbedürftigkeit des Transparenzgrundsatzes wegen seines hohen Abstraktionsgrades und insofern sein Charakter als „Optimierungsvorgabe"[11] hervorgehoben, der dadurch bedingt ist, dass die Grundsätze mittels Zielvorgaben die Beschreibung eines Idealzustands vornehmen, für dessen Erreichung es keine klar definierten Grenzen gibt.[12]

Gleichwohl findet sich eine Konkretisierungsleistung dieser abstrakten Vorgabe sowohl in den Erwägungsgründen, als auch in zahlreichen weiteren Vorschriften der DSGVO.[13] In erster Linie können hier die allgemeinen Transparenzanforderungen aus Art. 12 DSGVO sowie ErwGr. 39 DSGVO genannt werden, die weiteren Aufschluss darüber geben, was eine transparente Datenverarbeitung gegenüber der betroffenen Person voraussetzt. So findet sich in Art. 12 Abs. 1 DSGVO etwa das Erfordernis, geeignete Maßnahmen zu treffen, um die der betroffenen Person bereitzustellenden Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. In Anbetracht der Menge und des Umfangs der beispielsweise gem. Art. 13 und 14

7 *Husemann/Pittroff,* in: Roßnagel u. a. (Hrsg.), Die Fortentwicklung des Datenschutzes, 2018, 337 (340).

8 *Tribess*, ZD 2020, 440 (441) m. w. N.

9 *Roßnagel*, in: Simitis u. a. (Hrsg.), Datenschutzrecht, 2019, Art. 5 DSGVO Rn. 1; eindeutig auch der *EuGH*, Urt. v. 16.01.2019 – C-496/17, EU:C:2019:26, Rn. 57.

10 *Reimer*, in: Sydow/Marsch (Hrsg.), DSGVO | BDSG, 3. Aufl. 2022, Art. 5 DSGVO Rn. 1; *Roßnagel*, in: Simitis u. a. (Hrsg.), Datenschutzrecht, 2019, Art. 5 DSGVO, Rn. 1.

11 *Roßnagel/Hornung*, MMR 2018, 197 (198).

12 *Roßnagel/Hornung*, MMR 2018, 197 (198); *Roßnagel*, ZD 2018, 339 (342).

13 S. etwa *Roßnagel*, ZD 2018, 339 (340), demzufolge der Grundsatz „seinen Ausdruck in den Rechten der betroffenen Person auf Information und Auskunft und in den korrespondierenden Pflichten des Verantwortlichen" findet.

DSGVO bereitzustellenden Informationen zeigt sich schon am Kriterium der Präzision die sich für den Verantwortlichen ergebende Schwierigkeit, den rechtlichen Anforderungen gerecht zu werden. So sollen die Informationen zwar möglichst knappgehalten, „auf eine einfache Formel gebracht und griffig formuliert"[14] sein, gleichzeitig darf dieses Bestreben nicht zu Lasten der inhaltlichen Richtigkeit und Vollständigkeit der Informationen gehen.[15]

Empirische Studien deuten allerdings darauf hin, dass die geltenden Transparenzanforderungen aus der DSGVO und die derzeitigen Versuche der Verantwortlichen, diesen Anforderungen gerecht zu werden, nicht darin resultieren, dass in der Praxis eine tatsächliche Informiertheit der betroffenen Personen geschaffen wird. So gaben etwa bei einer Umfrage der *Europäischen Kommission* im Jahr 2015 lediglich 20% der Studienteilnehmer an, immer über die Bedingungen der Datenerhebung und die weiteren Verwendungsmöglichkeiten informiert zu werden, wenn sie online darum gebeten werden, persönliche Informationen bereitzustellen.[16] Vier Jahre später und damit bereits nach Inkrafttreten nach der DSGVO hat sich diese Situation nicht verbessert – 2019 gaben lediglich 22 % der Befragten an, immer informiert zu werden.[17] Die Bereitschaft zum vollständigen Lesen von Datenschutzerklärungen (DSE) nahm von 2015 bis 2019 sogar ab. Während 2015 noch 18 % der Befragten angaben, DSE vollständig zu lesen, waren es 2019 nur noch 13 %.[18] Weitere Studien geben Hinweise auf mögliche Gründe dafür: So gaben in einer Studie von *Bitkom Research* im Jahr 2015 90 % der Befragten an, dass sie DSE in der Regel unverständlich finden und 86 % gaben an, dass die Erklärungen schlicht zu lang sind.[19] Diese Ergebnisse decken sich mit denen aus den Umfragen der *Europäischen Kommission*. So gaben im Jahr 2015 67 % der Befragten an, dass sie DSE zu lang finden und 38 % hoben die Unverständlichkeit als Hinderungsgrund hervor,[20] 2019 waren es 66% respektive 31 %.[21] Diese Ergebnisse sind nicht weiter

14 *Artikel-29-Gruppe*, WP 260 rev.01, Rn. 8.
15 *Paal/Hennemann*, in: Paal/Pauly (Hrsg.), DS-GVO BDSG, 3. Aufl. 2021, Art. 12 DSGVO Rn. 28.
16 *European Commission*, Special Eurobarometer 431, 2015, S. 81.
17 *European Commission*, Special Eurobarometer 487a, 2019, S. 15.
18 *European Commission*, Special Eurobarometer 431, 2015, S. 84; *European Commission*, Special Eurobarometer 487a, 2019, S. 16.
19 *Bitkom*, Datenschutz in der digitalen Welt, 2015, S. 11.
20 *European Commission*, Special Eurobarometer 431, 2015, S. 87.
21 *European Commission*, Special Eurobarometer 487a, 2019, S. 17.

verwunderlich, wenn man berücksichtigt, dass die DSE der 50 umsatzstärksten Internethändler in Deutschland im Mittel aus 444,5 Sätzen mit jeweils 17,85 Wörtern bestehen,[22] die Lektüre jeder einzelnen DSE daher im Durchschnitt rund 44 Minuten benötigen würde[23] und die Erklärungen zuletzt nach vier gängigen Lesbarkeitsindizes als schwer verständlich zu bewerten sind.[24] Doch selbst dieser Umfang scheint nicht zwangsläufig zur Vollständigkeit der dargestellten Informationen beizutragen. *Freye* hat Form, Sprache und Inhalte der DSE von Gesundheits-Apps analysiert und auf Rechtskonformität im Einklang mit den Transparenzleitlinien der *Artikel-29-Datenschutzgruppe* (*Art.-29-Gruppe*),[25] die vom *Europäischen Datenschutzausschuss* (*EDSA*) ausdrücklich angenommen wurden,[26] überprüft.[27] Dabei ist sie zu dem Ergebnis gekommen, dass keine der zehn untersuchten DSE vollumfänglich überzeugt. Beispielsweise bestehen erhebliche Kritikpunkte hinsichtlich der korrekten Angabe der Rechtsgrundlage der Datenverarbeitung und der korrekten Information über die Betroffenenrechte.[28]

Im Unterschied zur Transparenz hat der Begriff der Intervenierbarkeit keinen expliziten Einzug in die DSGVO erhalten, insbesondere nicht als Datenschutzgrundsatz gem. Art. 5 DSGVO.[29] Dennoch ergibt sich auch dieses Schutz- bzw. Gewährleistungsziel[30] aus den Vorschriften der DSGVO[31] und wird dort in zahlreichen Normen konkretisiert – in erster Linie in den Betroffenenrechten in Art. 15-22 DSGVO.[32] Gleichwohl umfasst das Schutzziel der Intervenierbarkeit nicht lediglich die individuelle Fähigkeit zur Geltendmachung von Betroffenenrechten, sondern deckt

22 S. dazu die Studie von *Gerpott/Mikolas*, MMR 2021, 936 (938).
23 *Gerpott/Mikolas*, MMR 2021, 936 (938).
24 *Gerpott/Mikolas*, MMR 2021, 936 (940).
25 *Artikel-29-Gruppe*, WP 260 rev.01.
26 *EDSA*, Endorsement 01/2018.
27 *Freye*, DuD 2022, 762.
28 *Freye*, DuD 2022, 762 (765 f.).
29 Dies als Versäumnis bezeichnend *Roßnagel*, ZD 2018, 339 (341).
30 Die sechs Schutzziele der Transparenz, Intervenierbarkeit, Nichtverkettbarkeit, Verfügbarkeit, Integrität und Vertraulichkeit dienen der systematische Konkretisierung der abstrakten datenschutzrechtlichen Anforderungen in technische und organisatorische Maßnahmen. S. dazu u. a. *Rost/Pfitzmann*, DuD 2009, 353; *Bock/Meissner*, DuD 2012, 425; ebenso – allerdings unter Rückgriff auf den Begriff der Gewährleistungsziele und erweiternd um das Ziel der Datenminimierung – *DSK*, Standard-Datenschutzmodell, Version 2.0b, 2020, S. 9 f.
31 So auch *Roßnagel*, in: Roßnagel (Hrsg.), HDSIG, 2021, Einleitung, Rn. 65.
32 S. dazu die Ausführungen der *DSK*, Standard-Datenschutzmodell, Version 2.0b, 2020, S. 28.

auch weitere Perspektiven ab.[33] Hier sind u. a. die Möglichkeit der Aufsichtsbehörden zur Kontrolle der Rechtmäßigkeit der Datenverarbeitung durch die Verantwortlichen,[34] die Möglichkeit der Verantwortlichen zur Einwirkung auf bestehende Systeme, etwa indem die Option zur Deaktivierung einzelner Funktionalitäten ohne negative Auswirkungen auf die Funktionalität des Gesamtsystems gegeben ist,[35] sowie auch die Fähigkeit der Verantwortlichen einer Datenverarbeitung, auf ihre Weisungen hin agierende Auftragsdatenverarbeiter kontrollieren zu können,[36] zu nennen. Für diesen Beitrag und auch für die Aktivitäten im PERISCOPE-Forschungsprojekt liegt der Fokus jedoch auf der Fähigkeit der betroffenen Personen zur Wahrnehmung der ihnen gem. DSGVO zustehenden Interventionsmöglichkeiten – in erster Linie die Betroffenenrechte aus den Art. 15-22 DSGVO sowie das Recht auf Widerruf der Einwilligung gem. Art. 7 Abs. 3 DSGVO.

Diese Fähigkeit zur Intervention ist eng verknüpft mit der Funktion der Transparenzanforderungen aus der DSGVO. Denn erst durch die Einhaltung der Transparenzanforderungen wird die betroffene Person in die Lage versetzt, die Verarbeitung der sie betreffenden personenbezogenen Daten nachzuvollziehen, den Verantwortlichen dadurch gegebenenfalls zur Rechenschaft ziehen zu können sowie informiert in bestimmte Datenverarbeitungen einzuwilligen oder aber auch ihre Einwilligung zu widerrufen.[37] Diese enge Verbindung zeigt sich auch am Auskunftsrecht der betroffenen Person aus Art. 15 DSGVO, dessen unmittelbarer Zweck die Schaffung von Informiertheit ist: Die betroffene Person soll erkennen können, was mit den sie betreffenden personenbezogenen Daten geschieht und dadurch die Rechtmäßigkeit der Datenverarbeitung bewerten können.[38] Mittelbar hängt jedoch die Fähigkeit zur Wahrnehmung (nahezu) aller anderen Be-

33 S. a. *Rost*, Das Standard-Datenschutzmodell, 2022, S. 85, der Intervenierbarkeit einerseits als auf die Fähigkeit der Verantwortlichen, Änderungsbedarfen nachzukommen, abzielend versteht, andererseits auf die Fähigkeit der betroffenen Personen, ihre Rechte wahrzunehmen und durchzusetzen.

34 *Conrad*, in: Auer-Reinsdorff/Conrad (Hrsg.), HdB IT- und Datenschutzrecht, 3. Aufl. 2019, § 34 Rn. 557.

35 *Conrad*, in: Auer-Reinsdorff/Conrad (Hrsg.), HdB IT- und Datenschutzrecht, 3. Aufl. 2019, § 34 Rn. 557; *Scheja u. a.,* in: Leupold u. a. (Hrsg.), IT-Recht, 4. Aufl. 2021, Teil 6.6, Rn. 324.

36 So etwa die *ENISA*, Privacy and Data Protection by Design – from policy to engineering, 2014, S. 7.

37 Vgl. auch *Artikel-29-Gruppe*, WP 260 rev.01, Rn. 4.

38 *Dix*, in: Simitis u. a. (Hrsg.), Datenschutzrecht, 2019, Art. 15 DSGVO Rn. 1.

troffenenrechte vom Auskunftsrecht ab,[39] weshalb es regelmäßig als „das zentrale subjektive Datenschutzrecht“[40] eingeordnet wird. Ein weiteres Beispiel für die enge Verbindung von Transparenz und Intervenierbarkeit zeigt sich auch darin, dass den Betroffenen keine falsche Interventionsmöglichkeit suggeriert werden darf, indem beispielsweise eine Datenverarbeitung aus Absicherungsgründen sowohl auf die Einwilligung gem. Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO als auch auf die Erforderlichkeit zur Vertragserfüllung gem. Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO gestützt wird. In diesem Fall würde der betroffenen Person ansonsten fälschlicherweise die Möglichkeit zur Intervention durch Ausübung des Widerrufsrechts aus Art. 7 Abs. 3 DSGVO suggeriert werden.[41]

Wenngleich empirisch weniger umfangreich belegt als die unverändert bestehenden Transparenzprobleme des Datenschutzrechts, so zeigt sich doch auch hinsichtlich der Fähigkeit zur Wahrnehmung von Betroffenenrechten ein Problem in der Praxis. So zeigen etwa *Kozyreva u. a.* in einer Studie, dass sich zwar 82% der Deutschen hinsichtlich ihrer Privatsphäre besorgt zeigen, zugleich jedoch nur 37% ihre Privatsphären- und Werbeeinstellungen auf Online-Plattformen ändern.[42] Diese Ergebnisse werden durch eine im Rahmen des PERISCOPE-Projekts durchgeführten quantitativen Online-Umfrage grundsätzlich bestätigt. Hierbei gaben 81% der Befragten an, im vergangenen Jahr über eine Veränderung ihre Privatsphäreeinstellungen nachgedacht zu haben, wobei als häufigster Grund dafür die „Angst/Sorge vor unbefugtem Zugriff auf persönliche Daten“ genannt wurde. Insofern ist es auch nicht verwunderlich, dass Transparenz bei den Befragten grundsätzlich einen hohen bis sehr hohen Stellenwert einnimmt und sich dabei 71% der Befragten fragen, wer Zugriff auf ihre persönlichen Daten hatte und 60%, auf welcher Rechtsgrundlage ihre Daten verarbeitet werden. Im Missverhältnis dazu steht mit 64% allerdings der Anteil der Befragten, die tatsächlich aktiv ihre Privatsphäreeinstellungen verändert haben. Als wesentliche Hinderungsgründe wurden Angst vor Servicever-

39 *Bienemann*, in: Sydow/Marsch (Hrsg.), DS-GVO | BDSG, 3. Aufl. 2022, Art. 15 DGSVO Rn. 1 f.; *Dix*, in: Simitis u. a. (Hrsg.), Datenschutzrecht, 2019, Art. 15 DSGVO Rn. 1; *Franck*, in: Gola/Heckmann (Hrsg.), DS-GVO BDSG, 3. Aufl. 2022, Art. 15 DSGVO Rn. 1.

40 *Dix*, in: Simitis u. a. (Hrsg.), Datenschutzrecht, 2019, Art. 15 DSGVO Rn. 1; ähnlich *Bienemann*, in: Sydow/Marsch (Hrsg.), DS-GVO | BDSG, 3. Aufl. 2022, Art. 15 DGSVO Rn. 1.

41 *Engeler*, ZD 2018, 55 (58).

42 *Kozyreva u. a.*, Artificial Intelligence in Online Environments, 2020, S. 12.

schlechterung (45 %), Komplexität bzw. Unwissenheit (32 %) und Zeitaufwand (30 %) genannt (jeweils % der Befragten, Mehrfachauswahl zulässig). Insbesondere für vulnerable Gruppen, etwa ältere Menschen sowie Bevölkerungsgruppen mit geringerer Bildung, fällt dabei eine mangelnde Fähigkeit zur Intervention auf: Viele Befragten dieser Gruppen haben ihre Privatsphäreeinstellungen noch nie geändert. Darüber hinaus gaben 49% der Befragten an, dass sie sich über ihre Betroffenenrechte aus der DSGVO bewusst sind, wobei sich lediglich 42 % der Befragten in der Lage sehen, diese auch in Anspruch zu nehmen.

Insgesamt weisen empirische Erkenntnisse daher darauf hin, dass die Betroffenen in der Praxis weder ausreichend informiert noch ausreichend dazu befähigt sind, die ihnen zustehenden Rechte wahrzunehmen und dadurch auf die Datenverarbeitung Einfluss zu nehmen.

3. Praxisproblem II: Ressourcenaufwand als Bedrohung für die Wettbewerbsfähigkeit kleinerer Unternehmen

Praxisprobleme des Datenschutzes bestehen nicht nur auf der Seite der betroffenen Personen, sondern auch auf Seiten der für die Datenverarbeitung Verantwortlichen. Schon seit dem Inkrafttreten der DSGVO wurden sie von Wirtschaft und Politik in erster Linie als Innovationshindernis gesehen.[43] Wenngleich diese „typische Datenschutz-Ausrede" nicht immer der tatsächlichen Sachlage entspricht,[44] weisen zumindest die Selbsteinschätzungen der Unternehmen auf einen wahren Kern dieser Aussage hin: So gaben beispielsweise 2019 in einer Umfrage von *Bitkom Research* rund 14 % der Befragten an, dass in ihren eigenen Unternehmen bereits innovative Projekte wegen der DSGVO gescheitert seien und 29 % der Befragten betonten darüber hinaus, dass durch die DSGVO Innovationen innerhalb der EU verhindert würden.[45] 2020 bejahten bereits 56 % der befragten Unternehmen das Scheitern neuer, innovativer Projekte aufgrund der DSGVO[46]

43 Anschaulich und leicht polemisch dazu *Pettinger*, Datenschutz als Spaßbremse? Weniger Fakt als Ausrede.

44 Exemplarisch statt vieler *Kelber*, Digitalisierung und Datenschutz - Schluss mit Ausreden!, Netzpolitik v. 04. Feb. 2023.

45 *Bitkom*, DS-GVO, ePrivacy, Brexit – Datenschutz und die Wirtschaft, 2019, S. 6-8.

46 *Bitkom*, DS-GVO und Corona – Datenschutzherausforderungen für die Wirtschaft, 2020, S. 5.

und 2022 berichteten gar 98 % der Studienteilnehmer „von mindestens einem gescheiterten Innovationsprojekt."[47]

Größerer Konsens herrscht hingegen bezüglich der Feststellung, dass es sich bei der DSGVO um ein „Bürokratiemonster"[48] handle. Dies ist in Anbetracht dessen, dass die DSGVO – je nach Zählweise – rund 46 Pflichten für die Verantwortlichen bereithält und die Verantwortlichen daher nachweisen können müssen, „welche mindestens 46 Maßnahmen [sie] zur Erfüllung dieser 46 Pflichten ergriffen [haben]",[49] wenig überraschend. So bestätigten 2019 rund 95 % der im Rahmen einer Studie befragten Unternehmen einen eher hohen bis sehr hohen personellen Aufwand und 94 % einen eher hohen bis sehr hohen finanziellen Aufwand, der mit der Umsetzung der DSGVO-Pflichten einhergehe.[50] Als wesentlichste Gründe werden dabei mit jeweils 97 % die Erfüllung von Informationspflichten sowie die Erfüllung von Dokumentationspflichten ausgemacht.[51] Diese hohen Umsetzungsaufwände werden auch von anderen Studienergebnissen gestützt. So gingen beispielsweise bei 36 % der im Rahmen einer Studie von *Capgemini Research* befragten deutschen Unternehmen im ersten Geltungsjahr der DSGVO über 1.000 Betroffenenanfragen ein[52] und der Anteil an Unternehmen, die zur Einhaltung der Datenschutzvorgaben mehr als 1.000.000 Euro in den Bereichen „legal fees", „consulting fees" und „technology upgrade costs" ausgegeben haben, stieg von 2019 auf 2020 deutlich an (Steigerungen von jeweils 8 %, 3 % und 8 %).[53]

Insbesondere kleine und mittelständische Unternehmen haben oft nicht die notwendigen Ressourcen und Expertise, um die regulatorischen Anforderungen korrekt und vollumfänglich umzusetzen.[54] Zusätzlich haben *Chen u. a.* gezeigt, dass die negativen Auswirkungen der DSGVO auf den Gewinn der Unternehmen, die in den Anwendungsbereich der Verordnung

47 *Bitkom*, Datenschutz in der deutschen Wirtschaft: DS-GVO & internationale Datentransfers, 2022, S. 8; s. dazu *Jakobs*, ZD-Aktuell 2022, 01404; vgl. auch *Karaboga u. a.,* in: Friedewald/Roßnagel (Hrsg.), Die Zukunft von Privatheit und Selbstbestimmung, 2022, S. 49 (50 f.).

48 Diese Frage aufwerfend etwa *Heidrich/Maekeler*, Bürokratiemonster EU-Datenschutz?, c't Magazin 19/2018, S. 162.

49 *Veil*, ZD 2018, 9 (9).

50 *Bitkom*, DS-GVO, ePrivacy, Brexit – Datenschutz und die Wirtschaft, 2019, S. 4.

51 *Bitkom*, DS-GVO, ePrivacy, Brexit – Datenschutz und die Wirtschaft, 2019, S. 5.

52 *Capgemini Research*, Championing Data Protection and Privacy, 2019, S. 15.

53 *Capgemini Research*, Championing Data Protection and Privacy, 2019, S. 12.

54 S. beispielhaft die Studie von *Freitas/Mira da Silva*, J Inform Systems Eng 3(4), Article No: 30.

fallen, abhängig von Unternehmensgröße und Branche zu sein scheinen. So fallen die negativen Auswirkungen auf den Gewinn bei kleinen Unternehmen aus dem IT-Sektor doppelt so stark aus, wie der durchschnittliche negative Effekt auf die Gesamtuntersuchungsmenge. Bei großen IT-Unternehmen konnten hingegen keine wesentlichen Auswirkungen festgestellt werden.[55]

Die Ergebnisse deuten darauf hin, dass zumindest das Potenzial für Markteintrittsbarrieren von KMUs bestehen. Dieser Befund ist aus zwei Gründen gerade in der Plattformökonomie nachteilig. Zum einen besteht aufgrund ihrer ökonomischen Charakteristika ohnehin bereits die Tendenz zur Monopolbildung, was sich – etwas verkürzt dargestellt – aus dem Zusammenspiel aus Netzwerkeffekten, Lock-In-Effekten infolge hoher Wechselkosten sowie auch den sog. „Datennetzwerkeffekten" ergibt.[56] Zum anderen wird gerade in der Plattformökonomie der Erfüllungsaufwand zur Gewährleistung eines (nicht nur datenschutz-)rechtskonformen Geschäftsbetriebs weiterhin zunehmen. Als Reaktion auf die zunehmende Bedeutung digitaler Plattformen für die Gesamtwirtschaft hat die *Europäische Kommission* in den vergangenen Jahren insbesondere die bedenkliche Marktmacht digitaler Plattformen, „vor allem die der mächtigsten […], denen andere Marktteilnehmer kaum noch ausweichen können"[57], herausgestellt und dabei betont, dass ein „bedarfsgerechtes Regulierungsumfeld für Plattformen und Mittler"[58] zu etablieren sei. In der Folge wurden u. a. mit der VO (EU) 2019/1150 (Platform-to-Business-Verordnung; P2B-VO) sowie der VO (EU) 2022/2065 (Digital Services Act; DSA) neue plattformspezifische Rechtsakte erlassen, die auch für kleine und mittlere Plattformbetreiber neue Transparenzverpflichtungen vorsehen - etwa Art. 5 P2B-VO in Bezug auf Rankingparameter, Art. 7 Abs. 3 lit. a und Art. 9 P2B-VO in Bezug auf

55 *Chen u. a.*, Privacy Regulation and Firm Performance, 2022, S. 24; s. a. *Goldberg u. a.*, Regulating Privacy Online: An Economic Evualuation of the GDPR, 2019, S. 4, die gezeigt haben, dass die DSGVO bei kleinen E-Commerce-Webseiten zu etwa doppelt so hohen Umsatzverlusten (-16,7 %) wie bei größeren Webseiten (-7,9 %) geführt hat.

56 S. etwa *Schweitzer u. a,* Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen, 2018, S. 12 ff; *OECD,* An Introduction to Online Platforms and their Role in the Digital Transformation, 2019, S. 11; *Eisenmann*, Calif. Manag. Rev. 2008, 31 (36 f.).

57 COM (2015) 192 final, S. 10.

58 COM (2015) 192 final, S. 12.

Datenzugangsmöglichkeiten sowie Art. 14 und 15 DSA in Bezug auf die Moderation von Inhalten.[59]

Zusammenfassend sehen sich kleine und mittlere Plattformbetreiber mehreren Faktoren gegenüber, die ihre Wettbewerbsfähigkeit im europäischen Markt beeinträchtigen. Der insofern offenkundige Unterstützungsbedarf wurde auch durch eine im Rahmen des PERISCOPE-Projekts durchgeführten qualitativen Studie mit neun Plattformbetreibern identifiziert. Dabei gaben alle Interviewten an, dass insbesondere der Kosten- und Zeitaufwand eine sehr große wirtschaftliche Herausforderung bei der Umsetzung der DSGVO darstelle und bestätigten damit die oben aufgezeigten Ergebnisse. Ausschlaggebend dafür war die gerade bei kleinen Unternehmen oftmals fehlende Expertise, das Erfordernis zur Einbindung verschiedener Mitarbeiter aus nahezu allen Unternehmensbereichen, sowie die Unsicherheit sowohl bzgl. der Rechtskonformität der von ihnen etablierten Strukturen und Prozesse als auch bzgl. etwaiger Sanktionen bei mangelnder oder mangelhafter Umsetzung einzelner Pflichten aus der DSGVO.

4. Problembehandlung mittels Personal-Rights-Management-System

Bislang wurde zum einen aufgezeigt, welche Defizite für die betroffenen Personen derzeit in der Praxis sowohl bezüglich der Nachvollziehbarkeit der Datenverarbeitung als auch bei der Wahrnehmung der Möglichkeiten zur Intervention hinsichtlich der Verarbeitung sie betreffender personenbezogener Daten bestehen. Zum anderen wurde auf die unterschiedlichen Auswirkungen, die die zur Gewährleistung von DSGVO-Konformität notwendigen finanziellen und personellen Belastungen auf Unternehmen haben, hingewiesen. Insbesondere KMU-Plattformbetreiber wünschen sich deshalb ein technisches Werkzeug, das ihnen bei der Einhaltung der DSGVO-Pflichten hilft.

Das Forschungsvorhaben PERISCOPE widmet sich unter anderem der Entwicklung technischer Komponenten für ein PRM-System. Mit deren Hilfe sollen zum einen die tatsächliche Nachvollziehbarkeit der Datenverarbeitung und die Fähigkeit zur Wahrnehmung der Betroffenenrechte für die betroffenen Personen gefördert werden, sowie zum anderen KMU-Platt-

59 Die ebenfalls digitale Plattformen adressierende VO (EU) 2022/1925 (Digital Markets Act) kann an dieser Stelle vernachlässigt werden, da diese sich lediglich an die größten Betreiber digitaler Plattformen, sog. Gatekeeper, richtet.

formbetreiber bei der Umsetzung und Wahrnehmung einzelner Pflichten aus der DSGVO unterstützt werden. Dieses PRM-System besteht aus einer Reihe unterschiedlicher Komponenten, namentlich den Transaktionsjournalen, Komponenten zur Ausübung von Betroffenenrechten und zur Verwaltung von Einwilligungen sowie einem Datenverarbeitungsassistenten (s. Abb. 1). Im Zusammenspiel sollen diese Komponenten die genannten Schwerpunkte der Datenschutz-Schutzziele der Transparenz und Intervenierbarkeit für die betroffene Person bestmöglich fördern und zugleich die Ressourcenlast für Plattformbetreiber verringern.

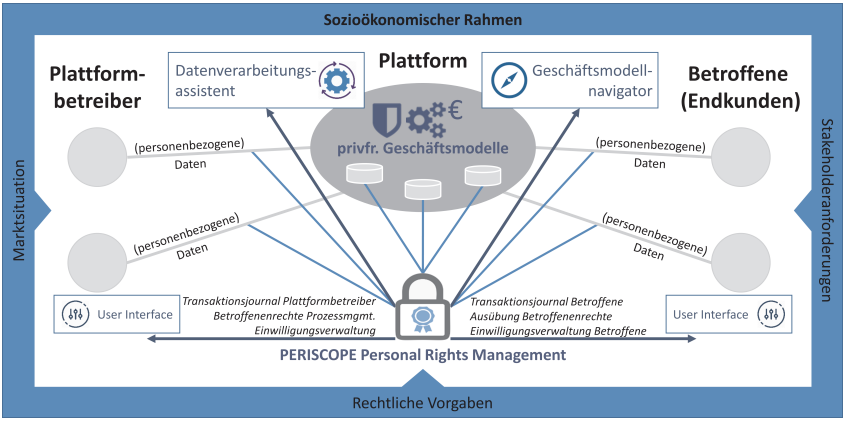

Abb. 1: Überblick über die Herangehensweise des PERISCOPE Projekts

Nachfolgend liegt der Schwerpunkt dieses Beitrags auf der Komponente des Transaktionsjournals, dessen Funktionalitäten sowie den Anforderungen, die sich aus multidisziplinärer Perspektive an ein solches ergeben.

4.1 Das PERISCOPE-Transaktionsjournal

Die oben skizzierten Unzulänglichkeiten in der heutigen Datenschutzpraxis sollen im Rahmen des PRM-Systems in erster Linie durch das sogenannte Transaktionsjournal adressiert werden.

Für die betroffene Person soll durch das Transaktionsjournal primär die Nachvollziehbarkeit der bei einem Plattformbetreiber stattfindenden Datenverarbeitung sichergestellt werden. Dies geschieht durch die Protokollierung von drei unterschiedlichen Aktivitäten. Erstens werden ausgewählte und als besonders privatsphäreninvasiv empfundene Datenverarbeitungs-

tätigkeiten protokolliert und der betroffenen Person angezeigt. Zweitens werden sämtliche Vorgänge rund um die Ausübung von Betroffenenrechten protokolliert, also beispielsweise von welchem Recht zu welchem Zeitpunkt Gebrauch gemacht wurde, wie viel Zeit dem Verantwortlichen noch zur fristgerechten Reaktion verbleibt sowie ob und mit welchem Ergebnis der Anfrage nachgekommen wurde. Drittens erfolgt eine „aktionsbasierte" Darstellung der „Veränderungen" bestimmter Rechtsgrundlagen, auf die der Verantwortliche seine Datenverarbeitungen stützt, also etwa das Entfallen einer Verarbeitung aufgrund berechtigter Interessen gem. Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO infolge eines erfolgreichen Widerspruchs gem. Art. 21 Abs. 1 DSGVO oder auch das Hinzukommen einer neuen Datenverarbeitung auf Basis einer Einwilligung gem. Art. 6 UAbs. 1 lit. a DSGVO.

Zudem soll dem Transaktionsjournal in Verbindung mit anderen Komponenten des PRM-Systems für den Plattformbetreiber in erster Linie die Funktion zukommen, ihn bzgl. der Einhaltung ausgewählter Dokumentations- und Rechenschaftspflichten zu unterstützen. Dies erfolgt u. a. durch die Erfassung und Archivierung der Prozesse im Zusammenhang mit der Ausübung von Betroffenenrechten, das Vorhalten der nötigen Nachweise rund um die Einwilligung sowie die Protokollierung der Datenweitergabe an Empfänger, damit der Plattformbetreiber in der Lage ist, dem Auskunftsrecht so nachzukommen, wie es der *EuGH* jüngst konkretisiert hat.[60]

4.2 Automatische Protokollierung von Verarbeitungstätigkeiten

Nachfolgend wird der Fokus auf lediglich eine der soeben skizzierten Funktionalitäten gelegt, nämlich die automatische Protokollierung ausgewählter Datenverarbeitungstätigkeiten zum Zweck der Gewährleistung der Nachvollziehbarkeit der Datenverarbeitung für die betroffene Person.

Hierbei sollen nicht undifferenziert sämtliche Verarbeitungsvorgänge des Verantwortlichen protokolliert werden, sondern vielmehr lediglich solche, die durch ein besonders hohes Risiko charakterisiert sind. Die Identifizierung solcher Vorgänge sollte dabei sowohl durch den Rückgriff auf anerkannte Risikobemessungskriterien – etwa jene, die von der *Artikel-29-Datenschutzgruppe* im Rahmen der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO entwickelt wurden, um festzustellen, ob ein Verarbeitungs-

60 *EuGH*, Urt. v. 12.01.2023 – C-154/21, EU:C:2023:3, Rn. 46.

vorgang wahrscheinlich ein hohes Risiko mit sich bringt[61] – als auch durch eine Orientierung daran, welche Verarbeitungen die betroffenen Personen selbst als besonders risikoreich empfinden, erfolgen. Anderenfalls würde in Anbetracht der Vielzahl und Vielfalt der unterschiedlichen in Betracht kommenden Datenverarbeitungstätigkeiten lediglich eine Situation gefördert, die erneut zu einem Informationsüberschuss (Information Overload) auf Seiten der betroffenen Person führen könnte. Die so verbleibenden Verarbeitungsvorgänge werden protokolliert und für die betroffene Person angezeigt – jeweils ergänzt um weitere Informationen zur einschlägigen Rechtsgrundlage gem. Art. 6 Abs. 1 UAbs. 1 lit. a-f DSGVO, zum mit dem Verarbeitungsvorgang verfolgten Zweck sowie der den Vorgang durchführenden Stelle. Zuletzt wird jeder dieser Verarbeitungsvorgänge angereichert um die der betroffenen Person im Einzelfall jeweils konkret zustehenden Interventionsmöglichkeiten, die sich aus Zweck und Rechtsgrundlage der Datenverarbeitung ergeben, um so eine möglichst niedrigschwellige Möglichkeit zur Wahrnehmung der Betroffenenrechte zu gewährleisten und damit die Fähigkeit der Betroffenen zur Intervention zu stärken.

5. Multi-Stakeholder Anforderungen an die automatisierte Protokollierung von Verarbeitungstätigkeiten

Aus einer solchen automatischen Protokollierung von Datenverarbeitungstätigkeiten ergeben sich eine ganze Reihe an Anforderungen aus multi- und interdisziplinärer Perspektive, im Konkreten aus Blickwinkel des (Datenschutz-)Rechts, der Sozio-Ökonomie sowie der technischen Machbarkeit und Funktionalität. Welche Herausforderungen und Anforderungen sich dabei jeweils stellen, wird nachfolgend erörtert.

5.1 Ausgewählte datenschutzrechtliche Anforderungen

Bei der automatisierten Protokollierung von Verarbeitungstätigkeiten handelt es sich nicht nur um eine Datenschutzmaßnahme, sondern zugleich auch selbst um eine Verarbeitungstätigkeit, die ein Sicherheitsrisiko darstellen kann.[62] Da zur vollständigen Überprüfbarkeit der Rechtmäßigkeit

61 *Artikel-29-Datenschutzgruppe*, WP 248 rev.01, S. 10 ff.

62 *Bedner*, Cloud Computing, 2013, S. 217; ähnlich *Rost*, Das Standard-Datenschutzmodell, 2022, S. 137 f.

einer erfolgten Verarbeitung auch die Instanz, die eine bestimmte Aktivität ausgelöst hat, zu protokollieren ist,[63] werden auch hier regelmäßig personenbezogene Daten verarbeitet, sodass darauf zu achten ist, die Protokollierungsaktivitäten selbst im Einklang mit den datenschutzrechtlichen Anforderungen aus der DSGVO auszugestalten.

Hier findet sich lediglich Platz für die Nennung einiger ausgewählter datenschutzrechtlicher Anforderungen, die sich zum Großteil aus den Datenschutzgrundsätzen in Art. 5 Abs. 1 lit. a-f DSGVO ergeben. So bedarf es auch bei der Protokollierung personenbezogener Daten einer entsprechenden Rechtsgrundlage aus Art. 6 Abs. 1 UAbs. 1 lit. a-f DSGVO (enges Verständnis[64] des Rechtmäßigkeitsgrundsatzes aus Art. 5 Abs. 1 lit. a DSGVO), und die Datenverarbeitung muss den Transparenzanforderungen aus Art. 5 Abs. 1 lit. a i. V. m. Art. 12 ff. DSGVO genügen. Zur Einhaltung des Zweckbindungsgrundsatzes bedarf es bereits vor Beginn der Protokollierungstätigkeiten der Festlegung eines eindeutigen und legitimen Zwecks und es muss darauf geachtet werden, dass die jeweiligen Protokolldaten in aller Regel nur für die Zwecke, die Anlass für ihre Speicherung gewesen sind, ausgewertet werden,[65] beispielsweise dürfen für Datenschutzzwecke generierte Protokolldaten nicht zur Leistungsmessung verwendet werden.[66] In Bezug auf den Grundsatz der Datenminimierung gem. Art. 5 Abs. 1 lit. c DSGVO ist darüber hinaus sicherzustellen, „dass die jeweiligen Daten hinsichtlich ihrer Verarbeitungszwecke angemessen und erheblich sowie auf das notwendige Maß beschränkt [sind]"[67], sodass insbesondere keine Inhaltsdaten im Transaktionsjournal dargestellt werden sollten. Zusätzlich müssen die verarbeiteten personenbezogenen Daten gem. Art. 5 Abs. 1 lit. d DSGVO sachlich richtig sowie erforderlichenfalls auf dem neuesten Stand sein. Bei Verarbeitung unrichtiger oder nicht aktueller personenbezogener Daten käme es dabei in der Regel nicht nur zu einem Verstoß gegen Art. 5 Abs. 1 lit. d DSGVO, sondern auch zu einem Verstoß gegen den Datenminimierungsgrundsatz, da unrichtige Daten insbesondere nicht erheblich für

63 So im Einklang mit *DSK*, Baustein 43 „Protokollieren", V1.0a, 2020, S. 2 f.
64 So etwa bei *Pötters*, in: Gola/Heckmann (Hrsg.), DS-GVO BDSG, 3. Aufl. 2022, Art. 5 DSGVO Rn. 7.
65 *DSK*, Baustein 43 „Protokollieren", V1.0a, 2020, S. 2.
66 *Rost*, in: Sowa (Hrsg.), IT-Prüfung, Sicherheitsaudit und Datenschutzmodell, 2017, 23 (47).
67 *Spindler/Dalby*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 4. Aufl. 2019, Art. 5 DSGVO Rn. 12.

die Erreichung eines bestimmten Zwecks sein können.[68] So ist insbesondere bei der hier angestrebten automatischen Generierung der Protokolldaten durch regelmäßige Überprüfung die Richtigkeit der generierten Daten zu überprüfen.[69] Der Speicherbegrenzungsgrundsatz gem. Art. 5 Abs. 1 lit. e DSGVO bringt darüber hinaus die Notwendigkeit mit sich, ein Löschkonzept für die Protokolldaten festzulegen, bei dem sich die Speicherdauer ebenfalls wieder anhand der Erforderlichkeit für die Zweckerreichung bemisst.[70] Und zuletzt bedarf es zur Einhaltung des Grundsatzes der Integrität und der Vertraulichkeit gem. Art. 5 Abs. 1 lit. f DSGVO der Sicherstellung, dass die Protokolldaten nicht nachträglich verändert werden können und zugleich nur Berechtigten zugänglich sind. Dies kann u. a. dadurch erreicht werden, dass bei der Generierung der Protokolldaten kryptographische Hashwerte verwendet werden,[71] dass die Protokolldaten verschlüsselt gespeichert und übermittelt werden[72] sowie durch die Festlegung im Rollen- und Berechtigungskonzept, wer zu welchen Zwecken auf die Protokolldaten zugreifen kann.[73]

5.2 Sozio-ökonomische Aspekte

Die sozio-ökonomischen Herausforderungen leiten sich anhand eines Multi-Methods-Designs ab, welches eine Untersuchung der Anforderungen seitens der Endanwender und seitens der Plattformbetreiber ermöglicht. Das Multi-Method-Design setzt sich aus einer quantitativen Studie mit Endanwendern (N = 589) als Online-Befragung inkl. Präferenzmessung, sowie qualitativen, halbstrukturierten Interviews (N = 9) mit kleinen und mittelständischen Plattformbetreibern verschiedener Branchen, zusammen. Die durchgeführte quantitative Studie ist repräsentativ für die deutsche Internetbevölkerung. Die Präferenzen der Endanwender wurden durch ein dis-

68 *Roßnagel*, in: Simitis u. a. (Hrsg.), Datenschutzrecht, 2019, Art. 5 DSGVO Rn. 138.
69 *Ammon u. a.*, Protokollierung und Protokollierungskonzept, 2020, S. 6.
70 *DSK*, Baustein 43 „Protokollieren", V1.0a, 2020, S. 3.
71 So auch *Ammon u. a.,* Protokollierung und Protokollierungskonzept, 2020, S. 24; *DSK,* Standard-Datenschutzmodell, S. 32; s. a. *BSI*, IT-Grundschutz-Kompendium, 2023, in dem unter "CON.1 Kryptokonzept" Maßnahmen zur Sicherung der Integrität und Vertraulichkeit von Datenbeständen und Kommunikationsverbindungen ausgewiesen sind.
72 *Rost*, in: Sowa (Hrsg.), IT-Prüfung, Sicherheitsaudit und Datenschutzmodell, 2017, 23 (46).
73 *Rost*, in: Sowa (Hrsg.), IT-Prüfung, Sicherheitsaudit und Datenschutzmodell, 2017, 23 (47).

kretes Entscheidungsexperiment (Choice-based Conjoint Experiment) erhoben und anschließend mittels eines hierarchisch bayesianischen Schätzverfahrens geschätzt. In der Online-Befragung der Studie wurden mittels Fragebogen ergänzende Informationen erhoben.

Im Hinblick auf die Ausgestaltung eines Transaktionsjournals zur Verbesserung der Transparenz und Intervenierbarkeit, haben Endanwender klare Präferenz bezüglich der Ausgestaltung ihrer Transparenzanforderungen. Die große Mehrheit der Endanwender bevorzugt einen digitalen Zugriff auf das Transaktionsjournal, einschließlich eines detaillierten Verzeichnisses der über sie gesammelten Daten und Datenkategorien. Dabei sollte das Transaktionsjournal aufzeigen, mit wem, zu welchem Zweck und in welchem Umfang Daten geteilt und verarbeitet werden. Grundsätzlich stehen die Befragten der Weitergabe von Daten für Marketingzwecke sehr restriktiv gegenüber und bevorzugen keine bzw. anonymisierte Datenweitergabe, zumindest insofern dies der Serviceverbesserung dient oder, z. B. in Form von Rabatten, incentiviert wird. Um für Endanwender Transparenz zu schaffen, sollte das Transaktionsjournal über Datenverarbeitungstätigkeiten und deren entsprechenden Rechtsgrundlagen informieren. Außerdem sollte in den Einträgen im Transaktionsjournal darauf hingewiesen werden, welche Betroffenenrechte den Endanwendern im Einzelfall zustehen, um so gegen eine Datenverarbeitung zu intervenieren oder beispielsweise weitere Informationen erhalten zu können. Weitere sozio-ökonomische Anforderungen aus Endanwender-Sicht umfassen, dass das Transaktionsjournal über robuste Sicherheitsmaßnahmen verfügt, benutzerfreundlich und leicht zugänglich ausgestaltet ist und laufend im Rahmen von Zertifizierungsmaßnahmen durch unabhängige Dritte geprüft wird.

Die durchgeführten qualitativen Interviews wurden anhand einer qualitativen Inhaltsanalyse nach *Mayring*[74] ausgewertet. Die Ergebnisse zeigen auf, dass für kleine und mittelständische Plattformbetreiber verschiedene Herausforderungen bezüglich der Umsetzung und Einhaltung der DSGVO bestehen, welche die in Abschnitt 3 aufgeführten Erkenntnisse bestätigen. Für alle neun interviewten Plattformbetreiber stellt die Umsetzung der DSGVO eine sehr große wirtschaftliche Herausforderung in Form eines Kosten- und Zeitaufwands dar. Infolgedessen resultiert diese Ressourcenbindung in einer fehlenden Kapazität für die Weiterentwicklung der Produkte und Services der Plattformbetreiber, was die Wettbewerbsfähigkeit

74 *Mayring,* in: Mey/Mruck (Hrsg.), Handbuch Qualitative Forschung in der Psychologie, 2020, 3 (17).

und erforderliche Time-to-Market verringert. Daher sehen die Plattformbetreiber ein Transaktionsjournal vor allem in Bezug auf die Dokumentationspflichten als „sehr hilfreich" und die damit verbundene Rechtssicherheit und Nachweisbarkeit als „essenziell". Hierbei gaben zwei Drittel der Interviewten an, einige Aspekte hinsichtlich der rechtssicheren Protokollierung bereits intern in einem dem Transaktionsjournal ähnlichen System umgesetzt zu haben, was dessen Bedeutung für die Plattformbetreiber weiter untermauert. Hieraus leitet sich die Anforderung eines modularen Aufbaus für das Transaktionsjournal bzw. die Komponenten des PRM-Systems ab, um eine ökonomisch vorteilhafte Integration in die vorliegenden Systeme der Plattformbetreiber zu ermöglichen. Denn bei sieben der neun interviewten Plattformbetreiber liegt eine hohe Bereitschaft zur Nutzung eines solchen modularen Angebots vor. Hinsichtlich der Funktionsweise steht für die Interviewten insbesondere der Protokollierungsmechanismus des Transaktionsjournals zur Ermöglichung einer erhöhten Rechtssicherheit im Fokus. Darüber hinaus ist eine Anwendbarkeit des Transaktionsjournals bzw. der anderen Komponenten für verschiedene, heterogene Kundengruppen, Geschäftsmodelle und Datenarten sowie eine schnelle Anbindung und Integration an Schnittstellen und vorliegende Systeme essenziell, um einen möglichen Wettbewerbsvorteil für Plattformbetreiber zu ermöglichen.

Zusammenfassend stellt die Transparenz-Dimension sowohl aus Plattformbetreiber-Sicht als auch aus Endanwender-Sicht einen wichtigen Aspekt dar. Während für die Plattformbetreiber die Protokollierungsfunktion des Transaktionsjournals aufgrund der Nachweisfähigkeit und der erhöhten Rechtssicherheit im Vordergrund steht, ist für Endanwender die Möglichkeit zur Intervention essenziell. Diese Erkenntnisse fließen in der weiteren Entwicklung des Transaktionsjournals ein.

5.3 Technisch-funktionale Anforderungen und Limitationen

Basierend auf den Ergebnissen der rechtlichen und sozio-ökonomischen Anforderungsanalyse lassen sich eine Reihe technischer Anforderungen für die automatisierte Protokollierung von Verarbeitungstätigkeiten im Rahmen eines Transaktionsjournals ableiten. Dazu gehört die Notwendigkeit für eine zweifache Umsetzung des Transaktionsjournals in der Referenzarchitektur: erstens als Komponente für Plattformbetreiber, die der Erfüllung einzelner Dokumentationspflichten der Plattformbetreiber dient, zweitens als eine separate Komponente zur Erhöhung der Transparenz für Betroffene. Dies berücksichtigt einerseits, dass eine Umsetzung von

beiden Stakeholdergruppen gewünscht wird und trägt andererseits den unterschiedlichen Zwecken, die mit den jeweiligen Komponenten verfolgt werden, durch eine technisch getrennte Umsetzung Rechnung.

Die automatisierte Protokollierung von Datenverarbeitungstätigkeiten durch ein Transaktionsjournal setzt zudem unvermeidlich eine Integration mit den Datenverarbeitungs- und Datenspeicherungssystemen des Plattformbetreibers voraus. Dabei liegt eine eventbasierende Architektur für den Datenaustausch mit der Steuerungskomponente des Transaktionsjournals ("Datenverarbeitungsassistent", s. Abb. 1) nahe. Dadurch wird eine unkomplizierte Anbindung an ein existierendes System möglich.

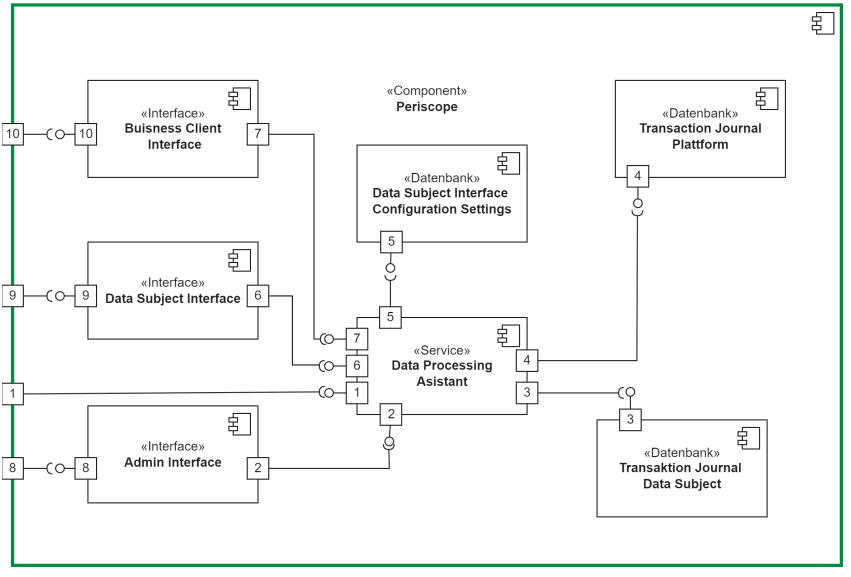

Abb. 2: Die PERISCOPE System-Architektur und -Schnittstellen

Das hat allerdings den Nachteil, dass die Aussagekraft des Transaktionsjournals vom Umfang der Integration in das System abhängt. Sollte bei der Integration beispielsweise die Entscheidung getroffen werden, bestimmte Verarbeitungsprozesse nicht zu protokollieren und an PERISCOPE weiterzuleiten, können diese an den Verbraucher nur über den Plattformbetreiber mitgeteilt werden. Dementsprechend ist der Grad der Transparenz, die das Transaktionsjournal ermöglicht, vom Plattformbetreiber abhängig.

Die Umsetzung des Transaktionsjournals als flexible und modulare Komponente benötigt mehrerer technischer Berücksichtigungen. Durch die Umsetzung des Transaktionsjournals als separate Komponente wird eine separate Datenbank benötigt. Diese kann zwar auf derselben physikalischen Datenbank laufen, sollte darüber hinaus allerdings logisch getrennt sein. Trotz der separaten Datenstruktur müssen die enthaltenen Daten des integrierenden Systems und des Transaktionsjournals gekoppelt sein, um die Verbindung der Daten auf dem Transaktionsjournal zu den Daten des Nutzers auf dem integrierenden System des Plattformbetreibers zu erhalten.

Außerdem muss das Transaktionsjournal durch ein sicheres Authentifizierungsverfahren geschützt sein, da personenbezogene Daten verarbeitet und gespeichert werden. Hierbei sollte kein separates Authentifizierungssystem erstellt werden, da dies zur Verwirrung bei Nutzern und reduzierter Usability führt. Stattdessen sollte für den Zugriff auf das Transaktionsjournal die Authentifizierung der integrierenden Plattform verwendet werden. Dadurch ist es dem Nutzer möglich, dieselben Zugangsdaten, die er beim Zugriff auf das integrierende System verwendet, auch bei der Einsicht seiner Daten im Transaktionsjournal verwenden. Diese Umsetzung wird daher im PERISCOPE Projekt verfolgt.

6. Fazit und Ausblick

Die Diskussion und Forschung um Möglichkeiten, die Nachvollziehbarkeit der Verarbeitung personenbezogener Daten für die betroffenen Personen zu fördern,[75] hat in den letzten Jahren ebenso stark zugenommen, wie die um Werkzeuge, die die Betroffenen bei der Ausübung ihrer Rechte sowie bei der Verwaltung ihrer Einwilligungen unterstützen sollen.[76] Das PERISCOPE PRM-System mit der Komponente des Transaktionsjournals reiht

75 Etwa durch mehrschichtige Informationsbereitstellung, s. dazu etwa *EDSA*, Leitlinien 05/2020, Rn. 69; durch kompakte Darstellung mittels „One-Pager", s. dazu u. a. *Stiftung Datenschutz*, Neue Wege bei der Einwilligung im Datenschutz, 2017, S. 40; sowie auch durch den Rückgriff auf die Vorzüge visueller Methoden zur Informationsbereitstellung, s. dazu *Specht-Riemenschneider/Bienemann*, in: Specht-Riemenschneider u. a. (Hrsg.), Datenrecht in der Digitalisierung, 2019, S. 324 (Rn. 17 ff.); *Nocun*, in: Roßnagel u. a. (Hrsg.), Die Fortentwicklung des Datenschutzes, 2018, S. 39 (54 f.).

76 Besonders rege diskutiert unter dem Begriff des Personal Information Management Systems (PIMS), s. dazu etwa *Schweitzer/Peitz,* NJW 2018, 275 (278); *EDSB*, Stellungnahme 9/2016 des EDSB zu Systemen für das Personal Information Management (PIM); in jüngerer Zeit zudem vermehrt diskutiert vor dem Hintergrund von sowohl

sich hier ein, fokussiert dabei allerdings einen vermittelnden Ansatz, der einen Mehrwert sowohl für die Betroffenen als auch für die Verantwortlichen der Datenverarbeitung schaffen soll. Die grundlegende Idee dahinter ist, dass nur durch Berücksichtigung der Bedürfnisse aller Stakeholder eine Form von Datenschutz ermöglicht wird, die das Recht auf Schutz bei der Verarbeitung personenbezogener Daten mit dem ebenso legitimen Interesse an der wirtschaftlichen Nutzbarkeit von personenbezogenen Daten ausbalanciert.

Durch die in diesem Beitrag beschriebene automatisierte Protokollierung von Datenverarbeitungstätigkeiten in einem Transaktionsjournal soll ein Aspekt dieses vermittelnden Ansatzes adressiert werden. Während für die Betroffenen leicht nachvollziehbar und chronologisch dargestellt wird, was mit denen sie betreffenden Daten geschieht und welche rechtlich zugestandenen Interventionsmöglichkeiten ihnen dabei jeweils zur Verfügung stehen, profitieren Plattformbetreiber von einem besseren Überblick der Datenverarbeitungstätigkeiten, die bei ihrem Geschäftsbetrieb anfallen und von der Förderung ihrer Fähigkeit zum Nachweis der Einhaltung datenschutzrechtlicher Anforderungen (die sich allerdings insbesondere aus dem Zusammenspiel mit den anderen Komponenten des PERISCOPE PRM-Systems, vor allem den anderen im Rahmen des Transaktionsjournals zu protokollierenden Aktivitäten, ergibt).

Besondere Schwierigkeiten, die sich bei der weiteren Entwicklung des Transaktionsjournals hinsichtlich der automatisierten Protokollierung von Datenverarbeitungstätigkeiten ergeben, liegen einerseits in der technischen Anbindung an die Systeme der Plattformbetreiber, andererseits in der angemessenen und an subjektiven Präferenzen orientierten Reduktion der den Betroffenen anzuzeigenden Vorgänge – was zur Vermeidung eines kognitiv nicht mehr verarbeitbaren Information Overloads unerlässlich ist. Hierfür wird im Rahmen des Forschungsprojekts eine Klassifizierung und Gruppierung unterschiedlicher Datenverarbeitungstätigkeiten entworfen, deren Praxistauglichkeit in der Folge durch eine quantitative Umfrage bei Endanwendern erprobt wird – mit einem Fokus auf der Frage, welche Verarbeitungstätigkeiten von Betroffenen als besonders privatsphäreninvasiv empfunden werden.

Art. 10 lit. b DGA, s. dazu u. a. *Ditfurth/Lienemann,* CRNI 2022, 270 (275), als auch § 26 TTDSG, s. dazu *Golland*, NJW 2021, 2238 (Rn. 19 ff.).

Literaturverzeichnis

Ammon, Danny; Backer-Heuveldop, Andrea u.a. (23.09.2020): Protokollierung und Protokollierungskonzept – Eine Einführung in die Thematik. URL: https://gesundheitsdatenschutz.org/download/protokollierungskonzept_2020.pdf (besucht am 24.02.2023).

Artikel-29-Datenschutzgruppe (2017): Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt". 17/DE WP 248-rev.01. Brüssel. URL: https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html (besucht am 24.02.2023).

Artikel-29-Datenschutzgruppe (2018): Leitlinien für Transparenz gemäß der Verordnung 2016/679. 17/DE WP260rev.01. Brüssel. URL: https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html (besucht am 24.02.2023).

Auer-Reinsdorff, Astrid und Conrad, Isabell (Hrsg.) (2019): *Handbuch IT- und Datenschutzrecht*. 3. Aufl. München: C.H.Beck.

Bedner, Mark (2013): *Cloud Computing. Technik, Sicherheit und rechtliche Gestaltung*. Kassel: kassel university press.

Bitkom (22. Sep. 2015): Datenschutz in der digitalen Welt. Berlin. URL: https://www.bitkom.org/sites/default/files/file/import/Bitkom-Charts-PK-Datenschutz-22092015-final.pdf (besucht am 24.02.2023).

Bitkom (17. Sep. 2019): DS-GVO, ePrivacy, Brexit – Datenschutz und die Wirtschaft, Berlin. URL: https://www.bitkom.org/sites/main/files/2019-09/bitkom-charts-pk-privacy-17-09-2019.pdf (besucht am 24.02.2023).

Bitkom (29. Sep. 2020): DS-GVO und Corona – Datenschutzherausforderungen für die Wirtschaft, Berlin. URL: https://www.bitkom.org/Presse/Presseinformation/Jedes-2-Unternehmen-verzichtet-aus-Datenschutzgruenden-auf-Innovationen (besucht am 24.02.2023).

Bitkom (27. Sep. 2022): Datenschutz in der deutschen Wirtschaft: DS-GVO & internationale Datentransfers, Berlin. URL: https://www.bitkom.org/sites/main/files/2022-09/Bitkom-Charts %20Datenschutz %2027 %2009 %202022_final.pdf (besucht am 24.02.2023).

Bock, Kirsten und Meissner, Sebastian (2012): Datenschutz-Schutzziele im Recht. Zum normativen Gehalt der Datenschutz-Schutzziele. *Datenschutz und Datensicherheit (DuD),* S. 425-431.

BSI (2023): IT-Grundschutz-Kompendium. Bonn: Bundesamt für Sicherheit in der Informationstechnik. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1 (besucht am 24.02.2023).

Capgemini Research Institute (Hrsg.) (2019): Championing Data Protection and Privacy. A source of competitive advantage in the digital century. URL: https://www.capgemini.com/gb-en/insights/research-library/championing-data-protection-and-privacy/ (besucht am 24.02.2023).

Chen, Chinchih; Frey, Carl Benedikt und Presidente, Giorgio (2022): Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally. *The Oxford Martin Working Paper Series on Technological and Economic Change.* Working Paper No. 2022-1. URL: https://www.oxfordmartin.ox.ac.uk/downloads/Privacy-Regulation-and-Firm-Performance-Giorgio-WP-Upload-2022-1.pdf (besucht am 24.02.2023).

Ditfurth, Lukas v. und Lienemann, Gregor (2022): The Data Governance Act: - Promoting or Restricting Data Intermediaries? *Competition and Regulation in Network Industries (CRNI)*, 23(4), S. 270-295.

DSK (2020): Baustein 43 „Protokollieren". Version 1.0a. URL: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V2.0_Protokollieren_V1.0a.pdf (besucht am 24.02.2023).

DSK (2020): Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele. Version 2.0b. URL: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/SDM-Methode_V20b.pdf (besucht am 24.02.2023).

EDPB (25. Mai 2018): Endorsement 01/2018. Brüssel: European Data Protection Board. URL: https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents.pdf (besucht am 24.02.2023).

EDSA (04. Mai 2020): Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679. Version 1.1. Brüssel: Europäischer Datenschutzausschuss. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf (besucht am 24.02.2023).

EDSB (20. Okt. 2016): Stellungnahme 9/2016. Stellungnahme des EDSB 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://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_de.pdf (besucht am 24.02.2023).

Eisenmann, Thomas R. (2008): Managing Proprietary and Shared Platforms. *California Management Review (Calif. Manag. Rev.)* 50(4), S. 31-53.

Engeler, Malte (2018): Das überschätzte Kopplungsverbot. Die Bedeutung des Art. 7 Abs. 4 DS-GVO in Vertragsverhältnissen. *Zeitschrift für Datenschutz (ZD),* S. 55-62.

Engert, Andreas (2018): Digitale Plattformen. *Archiv für die civilistische Praxis (AcP),* S. 304-376.

ENISA (2014): Privacy and Data Protection by Design – from policy to engineering. Athen, Heraklion und Brüssel: Agentur der Europäischen Union für Cybersicherheit. URL: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design (besucht am 24.02.2023).

European Commission (2015): Data Protection. Special Eurobarometer 431. URL: https://europa.eu/eurobarometer/surveys/detail/2075 (besucht am 24.02.2023).

European Commission (2019): The General Data Protection Regulation. Special Eurobarometer 487a, Summary. URL: https://cnpd.public.lu/content/dam/cnpd/fr/actualites/international/2019/ebs487a-GDPR-sum-en.pdf (besucht am 24.02.2023).

Freitas, Maria da Conceição und Mira da Silva, Miguel (2018): GDPR Compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management*, 3(4), Article No. 30. https://doi.org/10.20897/jisem/3941.

Freye, Merle (2022): Die Datenschutzerklärungen von Gesundheits-Apps. *Datenschutz und Datensicherheit (DuD),* S. 762-766.

Gerpott, Torsten J. und Mikolas, Tobias (2021): Lesbarkeit von Datenschutzerklärungen großer Internethändler in Deutschland. Ergebnisse einer empirischen Studie. *Multimedia und Recht (MMR)*, S. 936-941.

Gola, Peter und Heckmann, Dirk (Hrsg.) (2022): *Datenschutz-Grundverordnung VO (EU) 2016/679. Bundesdatenschutzgesetz*, 3. Aufl. München: C.H.Beck.

Goldberg, Samuel; Johnson, Garrett und Shriver, Scott (2019): Regulating Privacy Online: An Economic Evaluation of the GDPR. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3421731 (besucht am 24.02.2023).

Golland, Alexander (2021): Das Telekommunikation-Telemedien-Datenschutzgesetz. Cookies und PIMS als Herausforderungen für Website-Betreiber. *Neue Juristische Wochenschrift (NJW)*, S. 2238-2243.

Heidrich, Joerg und Maekeler, Nicolas (2018): Bürokratiemonster EU-Datenschutz? 100 Tage DSGVO – eine erste Bilanz. *c't magazin für Computertechnik*, 19, S. 162.

Husemann, Charlotte und Pittroff, Fabian (2018): Smarte Regulierung in Informationskollektiven – Bausteine einer Informationsregulierung im Internet der Dinge. In: Roßnagel, Alexander; Friedewald, Michael und Hansen, Marit (Hrsg.): *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung*, Wiesbaden: Springer, S. 337-359.

Jakobs, Madia (2022): Neue Bitkom-Umfrage zur DS-GVO und internationalen Datentransfers in der deutschen Wirtschaft, *Newsdienst ZD-Aktuell*, 01404.

Karaboga, Murat; Martin, Nicholas und Friedewald, Michael (2022): Governance der EU-Datenschutzpolitik: Harmonisierung und Technikneutralität in und Innovationswirkung der DSGVO. In: Friedewald, Michael und Roßnagel, Alexander (Hrsg.): *Die Zukunft von Privatheit und Selbstbestimmung: Analysen und Empfehlungen zum Schutz der Grundrechte in der digitalen Welt,* Wiesbaden: Springer Vieweg, (DuD-Fachbeiträge), S. 49–90.

Kelber, Ulrich (04. Feb. 2023): Digitalisierung und Datenschutz: Schluss mit Ausreden! URL: https://netzpolitik.org/2023/digitalisierung-und-datenschutz-schluss-mit-ausreden/#netzpolitik-pw (besucht am 24.02.2023).

Kozyreva, Anastasia; Herzog, Stefan u.a. (Februar 2020): Artificial Intelligence in Online Environments. Representative Sturvey of Public Attitudes in Germany. Joint Study by the Max Planck Institute for Human Development and the University of Bristol, supported by the Volkswagen Foundation. URL: https://pure.mpg.de/rest/items/item_3188061_4/component/file_3195148/content (besucht am 24.02.2023).

Lang, Rahel (30. Apr. 2022): Internes Dokument: Facebook hat keine Kontrolle über seine Daten. URL: https://netzpolitik.org/2022/internes-dokument-facebook-hat-keine-kontrolle-ueber-seine-daten/ (besucht am 24.02.2023).

Leupold, Andreas; Wiebe, Andreas und Glossner, Silke (Hrsg.) (2021): *IT-Recht. Recht, Wirtschaft und Technik der digitalen Transformation,* 4. Aufl. München: C.H.Beck.

Mayring, Philipp (2020): Qualitative Inhaltsanalyse. In: Mey, Günter und Mruck, Katja (Hrsg.): *Handbuch Qualitative Forschung in der Psychologie*, Wiesbaden: Springer, S. 3-17.

Nocun, Katharina (2018): Datenschutz unter Druck: Fehlender Wettbewerb bei sozialen Netzwerken als Risiko für den Verbraucherschutz. In: Roßnagel, Alexander; Friedewald, Michael und Hansen, Marit (Hrsg.): *Die Fortentwicklung des Datenschutzes. Zwischen Systemgestaltung und Selbstregulierung*, Wiesbaden: Springer, S. 39-58.

OECD (2019): An Introduction to Online Platforms and Their Role in the Digital Transformation, Paris: OECD Publishing. URL: https://www.oecd.org/innovation/an-introduction-to-online-platforms-and-their-role-in-the-digital-transformation-53e5f593-en.htm (besucht am 24.02.2023).

Paal, Boris P. und Pauly, Daniel A. (Hrsg.) (2021): *Datenschutz-Grundverordnung. Bundesdatenschutzgesetz*. 3. Aufl. München: C.H. Beck.

Roßnagel, Alexander (2018): Datenschutzgrundsätze – unverbindliches Programm oder verbindliches Recht? Bedeutung der Grundsätze für die datenschutzrechtliche Praxis. *Zeitschrift für Datenschutz (ZD),* S. 339-344.

Roßnagel, Alexander (Hrsg.) (2021): *Hessisches Datenschutz- und InformationsfreiheitsG. HDSIG. Handkommentar*. Baden-Baden: Nomos.

Roßnagel, Alexander und Hornung, Gerrit (2018): Die DS-GVO in den Startlöchern: Anfangszauber oder Reise ins Ungewisse? *Multimedia und Recht (MMR),* S. 197-198.

Rost, Martin (2017): Organisationen grundrechtskonform mit dem Standard-Datenschutzmodell gestalten. In: Sowa, Aleksandra (Hrsg.): *IT-Prüfung, Sicherheitsaudit und Datenschutzmodell. Neue Ansätze für die IT-Revision.* Wiesbaden: Springer, S. 23-56.

Rost, Martin (2022): *Das Standard-Datenschutzmodell (SDM). Einführung, Hintergründe und Kontexte zum Erreichen der Gewährleistungsziele*. Wiesbaden: Springer.

Rost, Martin und Pfitzmann, Andreas (2009): Datenschutz-Schutzziele – revisited. *Datenschutz und Datensicherheit (DuD),* S. 353-358.

Schweitzer, Heike; Haucap, Justus u.a. (29. Aug. 2018): Modernisierung der Missbrauchsaufsicht für marktmächtige Unternehmen. Endbericht. Projekt im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi). Projekt Nr. 66/17. URL: https://www.bmwk.de/Redaktion/DE/Publikationen/Wirtschaft/modernisierung-der-missbrauchsaufsicht-fuer-marktmaechtige-unternehmen.pdf?__blob=publicationFile&v=12 (besucht am 24.02.2023).

Schweitzer, Heike und Peitz, Martin (2018): Ein neuer europäischer Ordnungsrahmen für Datenmärkte? *Neue Juristische Wochenschrift (NJW)*, S. 275-280.

Simitis, Spiros; Hornung, Gerrit und Spieker genannt Döhmann, Indra (Hrsg.) (2019): *Kommentar Datenschutzrecht (DSGVO mit BDSG)*. Baden-Baden: Nomos.

Specht-Riemenschneider, Louisa und Bienemann, Linda (2020): Informationsübermittlung durch standardisierte Bildsymbole. In: Specht-Riemenschneider, Louisa; Werry, Nikola und Werry, Susanne (Hrsg.): *Datenrecht in der Digitalisierung.* Berlin: Erich Schmidt Verlag, S. 324-344.

Spindler, Gerald und Schuster, Fabian (Hrsg.) (2019): *Recht der elektronischen Medien – Kommentar*, 4. Aufl. München: C.H.Beck.

Stiftung Datenschutz (Hrsg.) (2017): Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. Studie. Leipzig. URL: https://stiftungdatenschutz.org/fileadmin/Redaktion/Video/Fremdveranstaltungen/PIMS-Abschluss-Studie-30032017/stiftungdatenschutz_Studie_Neue_Wege_zur_Einwilligung_final.pdf (besucht am 24.02.2023).

Sydow, Gernot und Marsch, Nikolaus (Hrsg.) (2022): *DS-GVO | BDSG, Handkommentar*, 3. Aufl. Baden-Baden: Nomos.

Tribess, Alexander (2020): Datenzugangsrechte in der Plattformökonomie. Auswirkungen der P2B-Verordnung im Bereich datenschutzrechtlicher Transparenzpflichten. *Zeitschrift für Datenschutz (ZD),* S. 440-444.

Veil, Winfried (2018): Accountability – wie weit reicht die Rechenschaftspflicht der DS-GVO? Praktische Relevanz und Auslegung eines unbestimmten Begriffs, *Zeitschrift für Datenschutz (ZD),* S. 9-16.

Zibuschka, Jan; Kurowski, Sebastian u.a. (2019): Anonymization is Dead - Long Live Privacy. In: Roßnagel, Heiko; Wagner, Sven und Hühnlein, Detlef (Hrsg.): *Open Identity Summit 2019.* Lecture Notes in Informatics, Bd. 293. Bonn: Gesellschaft für Informatik (GI). S. 71-82.

Privacy-Trade-offs: Zur Rolle technischer und regulativer Datenschutzinitiativen im Ökosystem des digitalen Journalismus[1]

Simon Engert, Jonathan Kropf und Markus Uhlmann

Zusammenfassung

Die Finanzierung digitaljournalistischer Inhalte ist zu großen Teilen von datenökonomischen Geschäftsmodellen geprägt und von diesen abhängig. Vor diesem Hintergrund setzen gegenwärtige Entwicklungen des Datenschutzes und technische Maßnahmen großer digitaler Infrastrukturanbieter zur Unterbindung von Third-Party-Cookies journalistische Geschäftsmodelle unter Druck, die auf Werbeeinahmen über Daten-Tracking angewiesen sind. Der Beitrag widmet sich diesen Dynamiken und nimmt auf der Grundlage einer empirischen Analyse des Ökosystems des digitalen Journalismus die verschiedenen Herausforderungen bestehender Geschäftsmodelle von Publishern und deren Reaktionen auf diese Entwicklungen in den Blick. Dabei zeigt sich, dass insbesondere technische Datenschutzinitiativen zur Unterbindung von Daten-Tracking nicht nur einen Wettbewerbsvorteil für große Plattformunternehmen bieten, sofern diese im Vergleich zu Publishern auf einen großen Bestand eigener First-Party-Daten setzen können. Auch befördert die Unterbindung von webseitenübergreifendem Tracking bei Publishern die Hervorbringung von Werbeformaten wie z. B. Affiliate Marketing, kontextuelles Targeting oder Native Advertising, die zwar weniger auf datenintensive Profilbildung setzen und deshalb als datenschutzfreundlicher gelten, dafür aber eine Angleichung von Werbung und journalistischen Inhalten nahelegen. Die Tatsache, dass Werbung im digitalen Journalismus in hohem Maße datengetrieben ist, führt somit dazu, dass journalistische Qualität nicht nur mit Fragen der Rentabilität, sondern auch mit neueren Entwicklungen der Datenschutzgestaltung relationiert werden muss, die bestimmte Geschäftsmodelle (perspektivisch) verhindern oder erschweren.

1 Der vorliegende Beitrag entstand im Rahmen des Verbundprojekts „Faire digitale Dienste: Ko-Valuation in der Gestaltung datenökonomischer Geschäftsmodelle (FAIR-DIENSTE)", das seit 02/2021 vom Bundesministerium für Bildung und Forschung (BMBF) gefördert wird (Förderkennzeichen: 16KIS1249K).

1. Einleitung

Der Journalismus ist nicht nur ein zentraler Ort, an dem gesellschaftliche Werte verhandelt werden und dem daher eine wichtige Funktion innerhalb demokratischer Öffentlichkeiten zugesprochen wird, in seiner digitalen Form ist er zugleich in hohem Maße von datenökonomischen Geschäftsmodellen geprägt und in weiten Teilen von diesen abhängig. Die jüngsten regulatorischen Bemühungen im Bereich des Datenschutzes und verschiedene technische Maßnahmen der großen digitalen Infrastrukturanbieter, wie die Ermöglichung des Einsatzes von AdBlockern durch Nutzende oder die Unterbindung von sog. Third-Party-Cookies, setzen dabei journalistische Geschäftsmodelle zunehmend unter Druck, die auf Werbeeinnahmen über Daten-Tracking angewiesen sind (Geradin u.a. 2021). Insbesondere die großen Publisher müssen sich neue Wege der Profitabilität erschließen, um wirtschaftlich überlebensfähig zu sein und ein journalistisches Angebot zu gewährleisten. Neben der verstärkten Tendenz, Bezahlinhalte anzubieten, zeigt sich eine Strategie, die auf Werbeformate setzt, die weniger auf webseitenübergreifendes Daten-Tracking über Drittanbieter angewiesen sind. Versuche, eigene First-Party-Daten zu nutzen oder eine zielgruppenspezifische Ansprache über kontextuelle Informationen zu gewährleisten, werden dabei von einem Rückgriff auf Werbeformate wie das *Affiliate Marketing* oder *Native Advertising* flankiert. Letztere ermöglichen zwar einerseits eine stärkere Unabhängigkeit von personalisierten Daten, können aber andererseits mit journalistischen Qualitätsnormen in Konflikt geraten, sofern eine Angleichung oder Vermischung von journalistischen Beiträgen und Werbung stattfindet. Während diese Entwicklungen der Hinwendung zu „hybriden Werbeformaten" (Lauerer 2021, S. 204ff.) vor dem Hintergrund sinkender Werbeerlöse schon länger beobachtet werden (Lobigs 2018), ist davon auszugehen, dass sie sich im Zuge konkreter regulatorischer oder technischer Datenschutzinitiativen weiter verstärken. Dabei wäre eine Einschätzung dieser Dynamiken jedoch einseitig, wenn die damit verbundene (vermeintliche) „Qualitätskrise" (Neuberger 2018, S. 39ff.) des digitalen Journalismus lediglich als Verschärfung des Dilemmas zwischen journalistischer Professionsethik und ökonomischer Realität betrachtet wird (Lorenz 2009, S. 168ff.). Denn die Tatsache, dass Werbung im digitalen Journalismus aktuell zu einem großen Teil auf Third-Party-Daten beruht, führt dazu, dass journalistische Qualität nicht nur mit Fragen der Rentabilität, sondern auch mit dem Wert der Privatheit relationiert werden muss, der über die oben beschriebenen Entwicklungen vermittelt wird, die

bestimmte Geschäftsmodelle (perspektivisch) verhindern oder erschweren. Insbesondere bei Akteuren, die nicht oder nur begrenzt auf Bezahlinhalte setzen können, dürften sich solche Tendenzen in Zukunft verstärkt zeigen. Aber auch dort, wo mit Bezahl- oder sog. Pur-Modellen experimentiert wird oder kontextuelles Targeting und First-Party-Daten zum Einsatz kommen, zeigen sich problematische Folgewirkungen für den Privatheitsschutz selbst, die Wettbewerbssituation sowie Medienvielfalt im digitalen Journalismus.

Vor diesem Hintergrund widmet sich der Beitrag den nichtintendierten Nebenfolgen, die im Zusammenhang technischer und regulativer Datenschutzinitiativen entstehen. *Dabei soll die Frage beantwortet werden, welche potenziellen Wertkonflikte zwischen Aspekten des Datenschutzes, der Gewährleistung ökonomischer Profitabilität des Journalismus und journalistischer Qualität im Zuge neuer Geschäftsmodelle auszumachen sind, die als Antwort auf die erwähnten Datenschutzmaßnahmen mobilisiert werden.* Die betrachteten Nebenfolgen dieser Maßnahmen zeigen zudem einen Bedarf für eine holistische Betrachtungsweise von Regulierungsmaßnahmen an, die sensibel für potenzielle Trade-offs zwischen unterschiedlichen Werten ist. Denn ein Großteil regulierungstheoretischer Überlegungen fokussiert auf einzelne Instrumente wie die Schaffung eines fairen Wettbewerbs oder die Regulierung des Datenschutzes, wodurch Trade-offs zwischen verschiedenen Regulierungsinstrumenten und datenökonomischen Gestaltungslogiken aus dem Blick geraten können (Popiel 2022). Ein grundlegendes Verständnis solcher Wertkonflikte ist notwendig, um perspektivisch Überlegungen zur *fairen Vermittlung* von verschiedenen Werten der Datenökonomie anzustellen (Uhlmann u.a. 2022).

Um im Folgenden mit der exemplarischen Analyse von Wertkonflikten Grundlagen für eine Perspektive der fairen Wertvermittlung im digitalen Journalismus zu schaffen, gilt es nicht nur die Position verschiedener Publisher zu verstehen, die mit unterschiedlichen Startbedingungen und Pfadabhängigkeiten auf die genannten Entwicklungen reagieren, sondern auch weitere Akteure des Ökosystems einzubeziehen, mit denen die Publisher über ihre Geschäftsmodelle verbunden sind oder die als Treiber der regulatorischen und technischen Veränderungen im Ökosystem auftreten. Dazu gehören unter anderem Werbeagenturen, Verbraucherzentralen, Journalismusverbände oder Plattformunternehmen, die Teil der vorliegenden empirischen Studie waren.

Der Beitrag orientiert sich an folgender Struktur: In Abschn. 2 wird das methodische Vorgehen beschrieben, das der vorliegenden Studie zugrunde

lag. In Abschn. 3 werden die genannten regulatorischen und technischen Datenschutzinitiativen erläutert und in ihrer Bedeutung für die Publisher im digitalen Journalismus dargestellt. Abschn. 4 beschreibt den Umgang verschiedener Akteure mit diesen Initiativen, der sich in der Verschiebung von Geschäfts- und Erlösmodellen mit teilweise problematischen Folgewirkungen zeigt. Das abschließende Fazit ordnet die beschriebenen Entwicklungen hinsichtlich der Rolle spezifischer Formen der Privatheitsregulierung im Ökosystem des digitalen Journalismus ein und wirft die Frage einer fairen Gestaltung dieses Ökosystems auf.

2. Methodisches Vorgehen

Um das Ökosystem des digitalen Journalismus sowie die Vielzahl der darin miteinander vernetzten Akteure zu beleuchten, folgt das methodische Vorgehen einem abduktiven Ansatz zur Analyse von Fallstudien (Alvesson/Sköldberg 2009). Als Kombination von induktivem und deduktivem Vorgehen spiegelt der abduktive Ansatz eine nicht-lineare Herangehensweise an die Untersuchung von Fallstudien wider. Mit dem übergeordneten Ziel der Theorieentwicklung wird dabei iterativ zwischen Erkenntnissen zum Untersuchungsgegenstand und theoretischen Zugängen gewechselt, um empirische Einblicke mit bestehender Theorie systematisch zu kombinieren. Das initiale Interesse am Ökosystem des digitalen Journalismus und die damit verbundenen Fragen bezüglich der Rolle von regulativ und technisch induzierten Datenschutzinitiativen offenbarte so im weiteren Verlauf des Analyseprozesses unter anderem die Bedeutung von Fragen der Privatheit und des Wettbewerbs sowie deren konfliktären Beziehungen.

Um sich dem komplexen Ökosystem holistisch zu nähern, diente ein digitaler Publisher und dessen unterschiedliche digitale Geschäftsmodelle als erster Zugang. Davon ausgehend wurden die vernetzten Beziehungen zu einer Vielzahl diverser Akteure wie Werbeagenturen, Anbietern von Analytics-Dienstleistungen, anderen Publishern, öffentlichen Stellen und Interessensvertretungen nachverfolgt. Dabei führten die Autoren im Zuge der Datenerhebung von November 2021 bis Februar 2023 25 ca. einstündige, semistrukturierte Interviews mit diversen Akteuren des Ökosystems des digitalen Journalismus (s. Tab. 1). Zusätzlich lieferten zwei Expert:innenworkshops mit sechs Branchenexpert:innen und einem Mitglied der Geschäftsführung eines digitalen Publishers sowie die Analyse von öffentlicher Berichterstattung und Unternehmensdokumenten weitere Einblicke.

Die Interviews, die von den Beitragsautoren in wechselnder Besetzung geführt wurden, umfassten allgemeine Fragen zu den Ansichten der Akteure über die Rolle von Daten für digitale Geschäftsmodelle des Journalismus, ihre Beziehungen zu anderen Akteuren und ihre Wahrnehmung von Veränderungen und Entwicklungen im Ökosystem. Um die Standpunkte der Akteure zu rekonstruieren, zu denen ein direkter Zugang nicht möglich war (insb. große digitale Infrastrukturanbieter), wurde auf öffentliche Aussagen und Unternehmensmitteilungen zurückgegriffen.

Die Analyse des reichhaltigen Datenmaterials erfolgte in einem permanenten Wechsel zwischen empirischem Material und potentiellen theoretischen Perspektiven. Zunächst wurde das empirische Material von allen Autoren des Beitrags offen codiert, einzelne Interviewabschnitte wurden zudem in regelmäßigen Gruppensitzungen vertiefend in einem an die Objektive Hermeneutik angelehnten sequenzanalytischen Verfahren interpretiert (vgl. z. B. Wernet 2021). Die entstehenden Strukturen wurden iterativ im Autorenteam diskutiert und gruppierten sich zunehmend um die zu erkennenden Spannungen, die sich aus den erwähnten regulativen und technischen Datenschutzinitiativen ergeben. Ausgehend von den im Ökosystem identifizierten dominanten digitalen Geschäftsmodellen und den damit verbundenen Konflikten kristallisierte sich insbesondere die Diversität an Reaktionen auf die systemischen Entwicklungen als Analyseobjekt heraus.

#	**Interviewpartner [Position, *Akteur*]**
1	Senior Sales Manager, *Digital Publisher*
2	Business Development Manager, *Digital Publisher*
3	Marketing Manager, *Digital Publisher*
4	Senior Sales Manager, *Digital Publisher*
5	Senior Technology Manager, *Digital Publisher*
6	Monetization Expert, *Digital Publisher*
7	Vorstand, *Digital Publisher*
8	Referatsleitung, *Verbraucherzentrale*
9	Director, *Technologiedienstleister*
10	Vorstand, *Nutzenden-Tech-Initiative*
11	Managing Director, *Werbeagentur*
12	Managing Director, *Werbeagentur*
13	Managing Director, *Werbeagentur*
14	Sprecher:in, *Journalistenverband*

#	**Interviewpartner [Position, *Akteur*]**
15	Digital Manager, *Publisher-Verband*
16	Journalist:in / Wissenschaftler:in, *Journalismus-Startup*
17	Sprecher:in, *Medien-Verwertungsgesellschaft*
18	Senior Executive, *Öffentlich-rechtlicher Rundfunk*
19	App-Entwickler:in, *Journalismus-Startup*
20	App-Entwickler:in, *Journalismus-Startup*
21	App-Entwickler:in, *Journalismus-Startup*
22	App-Entwickler:in, *Journalismus-Startup*
23	Journalist:in, *Journalismus-Startup*
24	Entwickler:in, *Digital Publisher*
25	Entwickler:in, *Digital Publisher*

Tabelle 1: Übersicht über interviewte Akteure

3. Spannungen zwischen Wettbewerb und Privatheit durch regulatorische und technische Datenschutzinitiativen

Die flächendeckende Nachverfolgung des Verhaltens von Internetnutzenden spielt vielfach eine Schlüsselrolle, damit Werbetreibende zielgerichtet personalisierte Werbung anzeigen und Webseitenbetreibende wie etwa Publisher auf dieser Grundlage ihre Inhalte finanzieren können (Geradin u.a. 2021, S. 3). Dabei ist für die Messung des Erfolgs von Werbekampagnen und die Identifizierung der Interessen verschiedener Nutzendengruppen das Tracking über mehrere Webseiten hinweg essentiell, das bislang insbesondere auf der Grundlage sogenannter Third-Party-Cookies ermöglicht wird. Hierbei handelt es sich um kleine Text-Dateien, die im Browser gespeichert werden und durch die Drittanbieter wie Werbetreibende Informationen über das Verhalten von Nutzenden sammeln (Heß/Kneuper 2023, S. 235). Die potenzielle Effizienz von Third-Party-Cookies wird allerdings nicht nur durch die Möglichkeit des Löschens von Cookies im Browser eingeschränkt; ebenso machen Datenschutzbedenken seit geraumer Zeit einen zentralen Ansatzpunkt der Kritik bezüglich der Nutzung von Third-Party-Cookies aus (Heß/Kneuper 2023, S. 235; Geradin u.a. 2021, S. 3). Diese Kritik materialisiert sich neben regulatorischen Entwicklungen wie etwa Cookie-Bestimmungen vor allem durch technische Maßnahmen zur grundsätzlichen Verhinderung von Third-Party-Cookies. Eine herausragende Rolle spielen hier große Browserhersteller wie Google (Chrome),

Apple (Safari) oder Mozilla (Firefox), die durch die jeweilige Browsergestaltung einen zentralen Einfluss auf die technischen Möglichkeiten der Nutzung von Third-Party-Cookies ausüben (Geradin u.a. 2021, S. 3). Paradigmatisch ist dabei die von Google bereits mehrfach verschobene und gegenwärtig für 2024 geplante Einführung der sog. Google Privacy Sandbox, mit der Google den von Apple und Mozilla angestoßenen Entwicklungen bezüglich der Verhinderung von Third-Party-Cookies folgt. Die Grundidee der Privacy Sandbox besteht darin, durch den Chrome Browser die Weitergabe von personenbezogenen Daten auf der Grundlage von Third-Party-Cookies zu unterbinden und Nutzenden die Möglichkeit zu geben, ihren Datenhaushalt eigenständig zu kontrollieren (Heß/Kneuper 2023, S. 238). Wie einem neueren Blog-Beitrag von Google zu entnehmen ist, kann die Einführung der Privacy Sandbox als direkte Reaktion auf Datenschutz- und Privatheitsbedenken verstanden werden:

> „Mit der Privacy Sandbox verfolgt Google das Ziel, den Datenschutz im Internet weltweit zu verbessern. […] Unser Ziel ist es, dass die neuen Tools Anforderungen erfüllen, die in der jüngsten Stellungnahme des Informationsbeauftragten zum Datenschutz und den Erwartungen an den Schutz der Privatsphäre bei Vorschlägen für Online-Werbung formuliert wurden. In dieser Hinsicht werden die neuen Tools so konzipiert, dass sie seitenübergreifendes Tracking vermeiden, Nutzer:innen mehr Transparenz und Kontrolle bieten und sowohl Menschen und Unternehmen bessere Ergebnisse im Internet anzeigen." (Malcom/Bethell 2022)

Aber nicht nur der Privatheitsschutz von Nutzenden soll durch neue digitale Werbemodelle verbessert werden; gleichsam muss – wie in einem weiteren Google Blog-Beitrag hervorgehoben wird – „digitale Werbung […] für die Verlage erfolgreich sein – sie muss Qualitätsjournalismus finanzieren und uns Zugang zu zuverlässigen und vielfältigen Perspektiven verschaffen. Und sie muss besser für die Wirtschaft sein […]" (Brittin 2022). Google versteht sich entsprechend als „einer der weltweit größten finanziellen Unterstützer des Journalismus […] und liefer[t] verlässliche Informationen und entwickel[t] Technologien, bei denen der Datenschutz im Vordergrund steht" (Brittin 2022). Folglich strebt Google mit der Privacy Sandbox nicht nur eine Harmonisierung von Datenschutz- und Informationsinteressen von Nutzenden an, sondern bekundet auch eine Sensibilität für die Vermittlung der Interessen von Werbetreibenden und Publishern. Als Alternative zur Nutzung von Third-Party-Cookies experimentierte Google bislang unter anderem mit technischen Konzepten, die nicht an der genauen Iden-

tität einer Person und damit personenbezogenen Daten interessiert sind, sondern unter Zuhilfenahme maschinellen Lernens auf die Bildung von sog. Kohorten zielen, zu denen Nutzendengruppen mit ähnlichen Interessen zugeordnet werden (Heß/Kneuper 2023, S. 239). Da diesem Ansatz des „Federated Learning of Cohorts" (FLoC) bereits frühzeitig kritisch begegnet wurde – u. a. mit dem Argument, dass Google mit der FLoC-Technologie eine detaillierte Profilbildung mit anderen Mitteln anstrebe und die marktführende Rolle im Werbebereich festige (z. B. Thomas 2021, S. 11) –, erprobt Google etwa auch den sogenannten „Topics-Ansatz", bei dem Webseiten mit Labeln zu öffentlich einsehbaren Themenbereichen wie etwa „Fitness" oder „Reisen" versehen werden. Ziel ist es, für Besuchende von Webseiten relevante Topics zu bestimmen, um sodann ohne die Weitergabe von Informationen zielgruppenorientierte Werbung zu schalten (Heß/Kneuper 2023, S. 243).

Wie das im Zuge von Datenschutzbedenken kritisierte FLoC-Konzept aufzeigt, ist es unerlässlich, die von Google angestoßenen alternativen Ansätze zur Nutzung von Third-Party-Cookies genauer unter Datenschutzgesichtspunkten zu prüfen.[2] Grundlegende Skepsis ist zudem hinsichtlich der angestrebten Harmonisierung unterschiedlicher Interessen von Publishern und Werbetreibenden durch die Privacy Sandbox angebracht. Insbesondere Publisher sehen sich mit der Verhinderung von seitenübergreifendem Tracking enorm unter Druck gesetzt und zur Änderung bisheriger Geschäftsmodelle gezwungen, wie etwa exemplarisch die folgende Textstelle aus einem Interview plausibilisiert:

> „[W]irklich einen richtigen Hammer wird es erst geben, wenn Google umstellt, weil Google um die 60 % Marktanteil hat. [...] [U]nd dann kommt es ganz heftig. [...] Ich sehe, dass diese Schockwelle immer noch nicht heftig genug ist und es wird erst passieren, wenn Google komplett die Sandbox und FLoC-Alternativen anbietet, und dann wird es sicherlich ein massives Umdenken geben." (I2, Pos. 29)

Vor dem Hintergrund des hohen Marktanteils von Google wird entsprechend im Zuge der Entwicklungen zur Privacy Sandbox diskutiert, inwiefern die angestrebte Verhinderung von Third-Party-Cookies einen unange-

2 Für eine kritische Auseinandersetzung aus einer Datenschutzperspektive mit den verschiedenen technischen Konzepten, die von Google als Ersatz für die Nutzung von Third-Party-Cookies entwickelt werden, siehe auch Heß/Kneuper (2023), Eliot/Wood (2022) sowie Geradin u.a. (2021).

messenen Wettbewerbsvorteil für Google biete (Geradin u.a. 2021; Nottingham 2021). Denn wenngleich auf Third-Party-Cookies verzichtet wird, gilt dies nicht für sogenannte „First-Party-Cookies", die etwa durch Login-Daten bereitgestellt werden und über verschiedene Services eines digitalen Dienstes hinweg die Bildung von Profilen erlauben. In diesem Sinne sind digitale Medienunternehmen im Vorteil, die über eine große Bandbreite verschiedener Services verfügen (Stallone u.a. 2022, S. 102). Google selbst bietet eine Vielzahl von Diensten wie z. B. Google Search, YouTube, Maps, Google Play, Gmail und Google Drive mit einem gemeinsamen Login an, mit denen die Beobachtung von Nutzendenverhalten und die Bildung von Profilen weiterhin umfassend möglich sind. Damit ist nicht nur mit möglichen Wettbewerbsvorteilen von Google im Werbemarkt zu rechnen; zudem fällt der versprochene Privatheitsschutz möglicherweise geringer aus, als von Google proklamiert (Geradin u.a. 2021, S. 37).[3] Wie etwa Eliot und Wood (2022) hinsichtlich der Praktiken von Google konstatieren, ist es keineswegs ausgemacht, dass etwa anonymisierte First-Party-Daten von vornherein privatheitsfreundlicher sind:

> „[W]ith enough independent websites […], Google could continue to track users across the web, even though the user's data would be more secure from third parties. We should be very wary of any claims about anonymization" (Eliot/Wood 2022, S. 271).

3 Diese Einschätzungen gelten aber nicht nur für Google, sondern auch für die von Apple implementierten Datenschutzmaßnahmen. Für den von Apple verfolgten App Tracking Transparency-Ansatz, der Nutzenden die Möglichkeit bietet webseitenübergreifendes Tracking durch die im App-Store erhältlichen Anwendungen zu verhindern, konstatieren Kollning u.a. (2022, S. 10): „We conclude that the new changes by Apple have traded more privacy for more concentration of data collection with fewer tech companies. […] Apple is now able to track its customers even more accurately, by […] getting unique access to user identifiers, including the device serial number. This underlies that privacy and competition problems can be highly intertwined in digital markets and need holistic study." Hoppner und Westerhoff (2021, S. 4) heben in diesem Zusammenhang hervor, dass Apple die Unterscheidung von First-Party-Daten und Third-Party-Daten einseitig zum eigenen Vorteil auslegt, sofern die Verwendung von ersteren Apple zufolge kein „Tracking" impliziere. Es ist zudem wahrscheinlich, dass es hier auch unter den Verlagen zu einem Verdrängungswettbewerb kommt, bei dem große Publisher, die über viele Medienkanäle und Abonnent:innen verfügen, einen Startvorteil gegenüber kleineren Verlagen haben. Ein solcher Verdrängungswettbewerb hätte das Potenzial die Vielfalt der Medienlandschaft dauerhaft zu verringern (Stallone u.a. 2022, S. 99).

Darüber hinaus können Argumente für einen fairen Wettbewerb und Datenschutzbemühungen gegeneinander ausgespielt werden, wenn Entwicklungen wie die Verhinderung von Third-Party-Cookies mit dem Verweis auf mögliche unfaire Wettbewerbsdynamiken problematisiert werden und verschiedene Akteure für Third-Party-Cookies zur Rettung des Wettbewerbs lobbyieren (Edelman 2021). Diese mögliche Tendenz kommt auch in einem Interview zur Sprache, in dem eine zivilgesellschaftliche Organisation Bedenken hinsichtlich der Tendenz eines Ausspielens von Datenschutz gegen den Wert des freien Journalismus anmeldet, die bei Medienunternehmen zu beobachten sei:

> „Bislang machen sich die meisten Medien ja nicht besonders gerade, was die Ad-Tech-Welt angeht, sondern versuchen jetzt auch gar nicht sich aus der Welt des Targeting Advertising zu verabschieden, sondern […] lobbyieren gegen stärkere Regulierungen von Webtargeting beispielsweise und sagen, dass wäre der Untergang des freien Journalismus im Netz." (I16, Pos. 24)

Die hier angesprochene Spannung zwischen Datenschutz und freiem Journalismus basiert letztlich auf der Abhängigkeit vieler digitaler Publisher von werbebasierten Geschäftsmodellen, die das Angebot eines freien und in diesem Sinne kostenlosen Journalismus ermöglichen. Neben der Frage, inwiefern technisch induzierte Privatheitsinitiativen wie die Google Privacy Sandbox einen Trade-off zwischen Wettbewerb und Datenschutz nahelegen, ist es im Folgenden zur Einschätzung der Nebenfolgen solcher Maßnahmen unerlässlich, genauer die verschiedenen Pfadoptionen und Geschäftsmodelle in den Blick zu nehmen, mit denen Publisher auf die skizzierten Entwicklungen reagieren.

4. Nichtintendierte Nebenfolgen der Datenschutzinitiativen und Strategien digitaler Publisher

Aktuell stehen Publisher vor der Herausforderung, dass durch die genannten Datenschutzmaßnahmen großer Infrastrukturanbieter die zugleich lukrativsten und datenintensivsten Werbemodelle erschwert und perspektivisch sogar verunmöglicht werden könnten. So wurde und wird ein Großteil der Werbeeinnahmen im digitalen Journalismus über das sog. *Programmatic Advertising* erzielt, das in hohem Maße von Third-Party-Cookies

abhängig ist (s. Tab. 2 am Ende des Kapitels für einen Überblick über die im Folgenden genannten Geschäftsmodelle).[4] Das Geschäftsmodell beruht auf der automatisierten, datengetriebenen Auktion von Werbeplätzen und -mitteln in Echtzeit mittels komplexer technischer Systeme (vgl. Alaimo/Kallinikos 2018). Dabei können Publisher Werbeplätze auf ihren Websites via Supply-Side-Plattformen anbieten, während Werbenetzwerke mittels nachfrageseitiger Plattformen ihre Werbemittel zur Verfügung stellen. Advertising-Server wie bspw. des Marktführers Google sorgen für die Ausspielung von Werbung auf den Displays von Nutzenden innerhalb eines „Wimpernschlags" (I5, Pos. 6), wenn die jeweiligen Seiten des Publishers aufgerufen werden.[5] Dabei werden die Nutzendendaten, die beim Publisher vorhanden sind, in sog. *Bid Requests* verschickt. Diese Daten umfassen meist Informationen über besuchte Seiten, die IP-Adresse, das Gerät, erstellte Warenkörbe oder den Browser. Um eine passgenaue Ausspielung der Werbeinhalte zu ermöglichen, spielen für Publisher die Menge und Tiefe an verfügbaren Nutzendendaten eine bedeutende Rolle, die aktuell nur über Third-Party-Daten gewährleistet werden kann. Während diese mittel- und langfristig nicht mehr im gleichen Umfang wie bisher zur Verfügung stehen, werden sie kurzfristig weiterhin intensiv genutzt, denn „so lange übergreifend Retargeting-Kampagnen funktionieren, macht man natürlich das, was noch geht" (I2, Pos. 29).

Zugleich stellt sich die Frage, mit welchen Strategien Publisher (zukünftig) reagieren, wenn die bisher lukrativste Werbeform zunehmend erschwert wird und perspektivisch sogar gänzlich unterbunden werden könnte. Bezahlmodelle für journalistische Inhalte scheinen dabei in ihrer aktuell verbreiteten Form nur bedingt eine Alternative zu sein, um auf die Finanzierungskrise des Journalismus zu reagieren. Zwar eröffnen bspw. Abos für exklusive Inhalte Möglichkeiten für Geschäftsmodelle, die unab-

4 Wie hoch die tatsächlichen Einnahmeeinbußen für Publisher durch den Wegfall von Third-Party-Daten sein werden, ist unklar. Verschiedene Schätzungen gehen aber von einem Verlust von ca. der Hälfte bis zu zwei Dritteln der Werbeeinnahmen (zumindest bei den größeren Publishern) aus (Bleier 2021, S. 9ff.; Ravichandran/Korula 2019).

5 Das hinter dem Programmatic-Advertising-Modell stehende komplexe und intransparente System an Anbietern und Nachfragern hat aufgrund der Anforderungen an die dahinterstehenden technischen Infrastrukturen insbesondere die Etablierung großer Intermediäre begünstigt. So verfügen Google, Amazon und Apple über große Werbedienste, aber auch teils in der öffentlichen Wahrnehmung unbekanntere Unternehmen, die jedoch in der Werbebranche in unzähligen Verbindungen im Datennetz verwoben sind.

hängiger von Werbung und Datentracking sind.[6] Diese Option steht aber erstens nur solchen Publishern offen, die Qualitätsinhalte anbieten und damit überhaupt erst mit einer Zahlungsbereitschaft rechnen können (Lobigs 2018, S. 311). Zweitens wird in den Interviews von Akteuren, die mit alternativen Bezahlmodellen für journalistische Inhalte experimentieren, die Vermutung geäußert, dass die gegenwärtigen Preismodelle etablierter Publisher nicht mehr den zeitgenössischen Praktiken des Medienkonsums entsprechen. Vor diesem Hintergrund müssten Rahmenbedingungen geschaffen werden, um „Paid-Journalismus lesen zu können von verschiedenen Zeitungen ohne ganz viele Abos abzuschließen. Weil die meisten Menschen können sich das ja gar nicht leisten […] und dann informiert man sich […] immer mehr einseitig" (I19, Pos. 4). Dementsprechend wären flexible Paid-Modelle und die Zugänglichkeit unterschiedlicher Inhalte verschiedener Publisher zentral, um Diskursvielfalt zu gewährleisten. In diesem Zusammenhang werden auch Plattformmodelle diskutiert (Wellbrock 2020), deren Umsetzung aber noch zahlreiche Fragen aufwirft. So ist davon auszugehen, dass es große Hürden für etablierte Publisher gibt, Inhalte über Plattformen auszuspielen, sofern diese „Angst [haben], eigene Abonnent:innen zu verlieren" (I19, Pos. 44). Zudem ist die Ausgestaltung der Preismodelle einer solchen Plattform gegenwärtig ungeklärt. Zwar werden Plattformmodelle wie bei Netflix oder Spotify zum Teil als Vorbild für Journalismus-Plattformen diskutiert (Wellbrock 2020). Zugleich zeigen die Erfahrungen der konkreten Umsetzung von Journalismus-Plattformen, dass solche Modelle nur schwerlich im Journalismus funktionieren, zumal „ernsthafte Publisher da eigentlich gar kein Geld mehr verdienen können, weil das Geld auf zu viele […] Publisher verteilt werden muss" (I23, Pos. 34).

Da Bezahlinhalte somit zwar einen relevanten, aber nicht den maßgeblichen Teil von Geschäftsmodellen im digitalen Journalismus ausmachen, wird der Blick im Folgenden auf solche Geschäftsmodelle gerichtet, die stärker auf Werbung setzen und bei denen sich die nichtintendierten Wirkungen der genannten Datenschutzinitiativen besonders deutlich zeigen. Dabei werden die verbleibenden Handlungsoptionen von Geschäftsmodellen anhand von zwei solcher Nebenfolgen geordnet: Der erste Komplex

6 Diese größere finanzielle Unabhängigkeit von Third-Party-Daten bedeutet selbstverständlich nicht, dass innerhalb von Bezahlmodellen notwendigerweise auf die Datenerhebung und -auswertung verzichtet wird. Insbesondere First-Party-Daten können durch Logins im Zuge von Abonnements erzeugt werden.

an Reaktionen beinhaltet paradoxe Effekte der Privatheitsregulierung, bei denen auf Regulierungsbemühungen mit Strategien der Datengenerierung und -analyse geantwortet wird, die Privatheitsprobleme reproduzieren oder sogar noch verschärfen (s. Abschn. 4.1). Während damit Reaktionen in den Blick geraten, die die Privatheit selbst betreffen, beziehen sich die restlichen Reaktionen eher auf Folgewirkungen für das Ökosystem des digitalen Journalismus, die auch als Probleme der Medienqualität (vgl. Eisenegger/Udris 2021; Zerback 2021) gefasst werden können. Dies gilt insoweit, dass hier insbesondere die Vielfalt der Medienlandschaft, die Relevanz von Inhalten sowie die professionelle Unabhängigkeit des Journalismus infrage stehen. Dabei ist eine Hinwendung zu weniger datenintensiven Werbeformaten zu beobachten, die gleichzeitig das Potenzial haben, journalistische Qualitätsnormen unter Druck zu setzen, indem sie eine Angleichung oder Vermischung von redaktionellen Inhalten und Werbung fördern (s. Abschn. 4.2).

4.1 Paradoxe Effekte der Privatheitsregulierung: Privatheitsrisiken durch vermeintlich datenschutzfreundliche Alternativen der Datengenerierung und -analyse

Eine Strategie, auf die Publisher im Zuge datenschutzrechtlicher Bemühungen zur Unterbindung von Third-Party-Cookies vermehrt zurückgreifen, besteht in dem sogenannten *Pur-Modell*. Hierbei werden Nutzende von Onlinediensten vor die Wahl gestellt, entweder dem Datentracking und personalisierter Werbung zuzustimmen oder alternativ einen Geldbetrag für ein werbefreies Angebot zu zahlen. Das *Pur-Modell*, dessen Name auf die werbefreie Nutzung des Dienstes anspielt, kann als Reaktion auf datenschutz*rechtliche* Entwicklungen verstanden werden, die sich in strengeren Cookie-Bestimmungen bemerkbar machen und das komplette Abschalten von Third-Party-Cookies vorsehen, wenn keine gleichwertige Alternative zum Datentracking vorhanden ist. So wird auch von einem Mitglied einer Sales-Abteilung hervorgehoben, dass das *Pur-Modell* eine Option ist, „um dieser Consent-Thematik zu begegnen" (I4, Pos. 33), da die Bezahlvariante als gleichwertige Alternative zum Datentracking ausgelegt wird. Wenn sich der Großteil von Nutzenden gegen das Tracking und die Bezahlvariante entscheidet, könnte das *Pur-Modell* das flächendeckende Tracking allerdings noch verstärken, ohne gegen Datenschutzbestimmungen zu versto-

ßen.[7] Dass das *Pur-Modell* die Zustimmung für das Datentracking erhöhen kann, merkt auch ein Publisher an, der im Zuge der aktuellen Cookie-Bestimmungen ein *Pur-Modell* eingeführt hat: „Wir haben schon auch immer mit dem Pur-Konzept geliebäugelt. [...] Weil wir [damit] einfach ne höhere Consent-Quote haben" (I25, Pos. 14), die – wie an späterer Stelle hervorgehoben wird – „der vermarktbaren Reichweite dient und […] [somit] eben auch die Umsätze größer sind" (I25, Pos. 32).

Zwar eröffnet das *Pur-Modell* für Publisher die Möglichkeit, um auf aktuelle Cookie-Bestimmungen zu reagieren. Allerdings ist fraglich, inwiefern diese Strategie langfristig eine probate Möglichkeit darstellt, um auf die beschriebenen technischen Entwicklungen zur Unterbindung von Third-Party-Cookies zu reagieren. Denn wie von einem weiteren Publisher problematisiert wird, stößt das *Pur-Modell* nicht nur auf Kritik bei Nutzenden, sofern sie „weder bereit [sind], ein Abo zu zahlen [noch] Werbung zu sehen" (I24, Pos. 34). Zudem kommen an dieser Stelle die technischen Maßnahmen großer Infrastrukturanbieter zum Tragen, die Möglichkeiten des Datentrackings wiederum einschränken und somit eine wichtige Säule des *Pur-Modells* herausfordern, sofern sie „Policies implementieren, die aktiv eben Publishern wehtun" (I24 Pos. 34).

Darüber hinaus ist das *Pur-Modell* aus einer Datenschutzperspektive umstritten. Die österreichische NGO „Europäisches Zentrum für digitale Rechte" (NOYB) hinterfragt etwa, inwiefern das *Pur-Modell* auf einer „freiwilligen Entscheidung" beruht, sofern Nutzende nicht ohne Nachteile ablehnen können (NOYB 2021, S. 12 ff.). Hier ist etwa hervorzuheben, dass die etablierten *Pur-Modelle* oftmals keine Möglichkeit der Granularität von Einwilligungsoptionen erlauben, was sich beispielsweise an den fehlenden Optionen zeigt, bestimmte Verarbeitungstätigkeiten abzuwählen. Die NGO kommt somit zu dem Schluss, dass das Verhalten von Nutzenden aufgrund der mangelnden Granularität der Einwilligung sogar umfassender als bei gewöhnlichen Cookie-Bestimmungen erfasst werden könnte, die zumindest eine Auswahl bestimmter Verarbeitungstätigkeiten erlauben (NOYB 2021,

7 So wird auch von einem Teamleiter aus der Sales-Abteilung eines Publishers die Zahlungsbereitschaft für werbefreie Inhalte gering eingeschätzt: „[A]us Gesprächen aus dem Markt heraus wissen wir, dass doch der Nutzer zu sehr, sehr großen Teil dazu neigt, dann doch mit seinen Daten zu bezahlen, weil er eben jetzt nicht noch 1, 2 oder 3 Euro, 4 Euro, 5 Euro oder auch nur ein neues Abonnement abschließen will." (I4, Pos. 33).

S. 20).[8] Vor diesem Hintergrund gibt auch ein Publisher zu bedenken: „Wir sind uns derzeit als Verlag nicht so ganz sicher, ob wir Pur in dieser Form also wirklich langfristig weiterführen, zumal es halt auch immer noch Bewegungen bei den Datenschutzbehörden gibt, wie […] sie d'accord sind mit den Pur-Modellen" (I25, Pos. 22).[9]

Derartige paradoxe Effekte der Privatheitsregulierung, bei denen auf Regulierungsbemühungen mit alternativen Tracking-Methoden geantwortet wird, die Privatheitsprobleme reproduzieren oder sogar noch verschärfen, werden auch hinsichtlich neuerer Formen des *kontextuellen Targetings* diskutiert. Beim (klassischen) *kontextuellen Targeting* wird das Interesse an bestimmten Artikeln als Anhaltspunkt für das mögliche Interesse an bestimmten Produkten herangezogen. Personen, die etwa Artikel über Elektromobilität lesen, bekommen in der Folge Werbung für Elektroautos angezeigt usw. Da *kontextuelles Targeting* somit nicht auf personenbezogene Daten angewiesen ist, erlaubt es vermeintlich das effiziente Ausspielen von Werbung, ohne dass dabei zugleich auf explizite Einwilligungen oder Third-Party-Cookies zurückgegriffen werden muss. Zwar erscheint dieser Ansatz in den Interviews für Publisher als Kompromiss, um „nicht den Willen des Gesetzgebers oder des Users […] zu umgehen" (I4, Pos. 31) und gleichzeitig potenzielle Zielgruppen für Werbekunden zu identifizieren. Neuere Formen des *kontextuellen Targetings*, die auf Verfahren des maschinellen Lernens zurückgreifen, könnten zukünftig jedoch Rückschlüsse auf einzelne Nutzende aufgrund von Gruppenzugehörigkeiten ermöglichen, die aus Sicht einer erweiterten Perspektive des Privatheitsschutzes als kritisch zu bewerten sind (z. B. Mühlhoff 2022) – auch wenn diese Verfah-

8 Wie weiterhin der Stellungnahme von NOYB zu entnehmen ist, trage das Pur-Modell zu einer unzulässigen Vermarktlichung des Grundrechtsschutzes bei, sofern „der Schutz der personenbezogenen Daten und der Achtung der Privatsphäre des Lesers, der sein Recht auf Informationsfreiheit verfolgt, eine Bedingung der Zahlung wird." (NOYB 2021, S. 24).

9 Hinsichtlich dieser Entwicklungen sind aber nicht nur paradoxe Privatheitseffekte, sondern auch Glaubwürdigkeitsprobleme des Journalismus zu erwähnen, sofern keine hinreichende Sensibilität für Privatheitsherausforderungen besteht. In diesem Zusammenhang konstatiert eine NGO, dass diese Praktiken des Datentrackings einen „inhärente[n] Konflikt" offenbaren, „wenn im […] Online-Feuilleton gegen den Überwachungskapitalismus angeschrieben wird und das auf 'ner Seite passiert, wo […] erstmal […] hunderte Third-Party-Cookies geladen werden […]. Das muss keine Auswirkungen auf die Qualität des Journalismus haben, aber es schwächt die Legitimität und das […] Nachrichtenökosystem an sich." (I16, Pos. 26).

ren aufgrund der vordergründigen Vermeidung des Personenbezugs datenschutzrechtlich als unproblematisch gelten:

> „Advances in machine learning allow firms to react to data that might not have been comprehensible to computers in the past, such as images or meaning. [...] When combined with session data, the information obtained from sentiment, image, or video analysis can be used to create complex inferences about users." (Bleier 2021, S. 21)[10]

Diese Herausforderungen gelten auch für die oftmals als unproblematisch angesehenen First-Party-Daten, deren Nutzung nicht nur wie oben aufgezeigt im Zusammenhang der Entwicklung der Google Privacy Sandbox aus Gesichtspunkten des Wettbewerbs kritisch zu bewerten ist. Angesichts des perspektivischen Endes von Third-Party-Cookies sind auch Publisher bestrebt solche Daten – bspw. über Plattform-Modelle, Apps oder Foren, die zugleich Logins und Traffic erzeugen – in größerem Stile zu generieren. Denn First-Party-Daten unterliegen vergleichsweise geringeren Datenschutzanforderungen, insbesondere dann, wenn die Zustimmung zur Nutzung dieser Daten mit dem Login erteilt wird. So konstatiert auch ein Werbemanager: „Login-Daten sind First-Party-Daten, die darf ich nutzen. Die sind schon wertvoll und die [werden] […] auch in der Zukunft […] noch viel mitbestimmen" (I5, Pos. 26-27). Die Relevanz der Generierung von First-Party-Daten beeinflusst dabei bspw. auch die Gestaltung von Kommentarfunktionen in Online-Foren von Publishern. Diese könnten perspektivisch essentiell sein, „um die Nutzer wieder enger an uns zu binden […] [und] dann auch mehr Daten von ihnen [zu] haben, wenn sie eingeloggt sind […]. Dann kann man genau das machen, was Facebook macht, wenn man sich zum Kommentieren anmeldet, dann muss man einmal aktiv akzeptieren, dass Werbung von Fremddaten rüberkommt. [...]." (I2, Pos. 43) Login-Daten erschließen somit neue Monetarisierungsquellen für Publisher, legen aber auch einen eher instrumentellen Zugriff auf die Gestaltung der Diskursarenen des digitalen Journalismus nahe, bei dem es nicht primär um die Steigerung der Diskursqualität geht, sondern die Konvertierung von Diskursteilnehmenden in zahlungsfähige Kund:innen im Zentrum steht. In diesem Sinne besteht die Gefahr, bestimmte Logiken

10 Aufgrund von Präzisionsverlusten in der Zielgruppenansprache ist außerdem zu erwarten, dass auch das kontextuelle Targeting die großen Internetunternehmen begünstigt, die weiterhin ein hohes Maß an Personalisierung gewährleisten können (vgl. Geradin u.a. 2021, S. 46).

der Datengenerierung und -nutzung zu reproduzieren, die bei den großen Plattformunternehmen regelmäßig kritisiert werden (vgl. z. B. Couldry/Mejias 2019; Zuboff 2018) – was sich schließlich auch daran zeigt, dass Facebook von Publishern als Referenz für die Generierung von Login-Daten erwähnt wird.

Entsprechend kann nicht nur das *Pur-Modell*, sondern auch die (künstliche) Abgrenzung datenschutzrechtlich relevanter personenbezogener Daten von weniger regulierungsbedürftigen First-Party-Daten oder kontextuellen Analysen dazu beitragen, dass privatheitsrelevante Herausforderungen nach wie vor eine Rolle spielen und sich sogar noch verschärfen können – insbesondere, wenn die entsprechenden Privatheitsgefährdungen innerhalb dieses Rahmens nicht als solche problematisierbar sind.

4.2 Angleichung und Vermischung von journalistischen Inhalten und Werbung

Steht das *Programmatic Advertising* lediglich in einer indirekten Beziehung zum journalistischen Inhalt,[11] scheinen vor dem Hintergrund der dargestellten Entwicklungen zunehmend solche Werbeformate eine Option zu sein, die tiefer in die inhaltliche Gestaltung eingreifen. Das vielfach thematisierte Spannungsverhältnis innerhalb des privatwirtschaftlich finanzierten Journalismus zwischen ökonomischen Interessen und demokratietheoretisch[12] fundierten journalistischen Qualitätsnormen (vgl. bspw. Weischenberg 2018, S. 29), wird aus Sicht zahlreicher Beobachter:innen im Zuge der Digitalisierung weiter verschärft (Lobigs 2018; Lünenborg 2012; Neuberger 2018; Schröder/Schwanebeck 2011). Zwar ist nicht von der Hand zu weisen, dass der ökonomische Druck es wahrscheinlicher macht, das vorhandene „Dilemma zwischen normativem Anspruch und beruflichen Realitäten" (Lorenz 2009, S. 169) etwa zugunsten von höheren Werbeeinnahmen aufzulösen. Wie im Folgenden argumentiert wird, bringen aber auch die genannten technischen und regulativen Datenschutzmaßnahmen nichtintendierte Nebenfolgen für journalistische Qualitätsnormen hervor, zumal die Unterbindung von Third-Party-Cookies den Rückgriff auf da-

11 Gleiches gilt auch für klassische Formen des *Display-, Banner- und Video-Advertising*, bei dem Werbeplätze meist über Werbeagenturen oder in Einzelfällen auch in direkter Aushandlung mit Werbekunden vergeben werden.

12 Zur demokratietheoretischen Fundierung vgl. Eisenegger/Udris 2021 sowie Zerback 2021.

tensparsame Werbeformate wahrscheinlicher macht, die eine Angleichung oder Vermischung von Werbung und redaktionellem Inhalt fördern. Das Verhältnis von Privatheit und journalistischen Qualitätsnormen stellt sich dabei zunehmend als Trade-off dar.

Das Geschäftsmodell des *Affiliate Marketing* weist potenziell in eine solche Richtung. Dieses umfasst die „Anreicherung von redaktionellem Content mit Affiliate-Links" (I1, Pos. 7), also die Hinterlegung bestimmter Schlagwörter mit Verlinkungen auf Seiten von Drittparteien (bspw. E-Commerce-Händler), bei denen das im Text erwähnte Produkt direkt gekauft werden kann. Dabei stellt das Modell eine Erweiterung der Customer Journey der User:innen über die Nutzung des redaktionellen Beitrags hinaus auf eine Transaktion dar, deren Abschluss im Zentrum steht. Die Publisher verhandeln mit Anbietern spezielle Angebote, die den Nutzenden dann auf thematisch passendem Content ausgespielt werden. Die Vergütung der Weiterleitung der Nutzenden auf Zielseiten, auf denen der Abschluss der Transaktion erfolgen soll, findet dabei in der Regel in Form variabler Provisionen statt, die im Erfolgsfall gezahlt werden. Spezialisierte Anbieter von Affiliate-Links-Diensten stellen die Nachverfolgbarkeit und technische Umgebung sicher. Anders als das *Programmatic Advertising* ist das *Affiliate Marketing* dabei nicht zwangsläufig auf Third-Party-Cookies angewiesen. Für bestimmte Erlösmodelle, die auf dem Last-Cookie-Wins-Prinzip basieren, bei denen der zuletzt gesetzte Cookie bestimmt, welchem Akteur die Provision zugerechnet wird, sind Third-Party-Cookies aktuell allerdings noch unverzichtbar.

Es ist anzunehmen, dass die wachsende Bedeutung des *Affiliate Marketings* – auch jenseits direkter Einflussnahmen durch Werbetreibende, die in den Interviews durchgängig bestritten werden – Konsequenzen für die inhaltliche Gestaltung des digitalen Journalismus hat. So eignen sich Nachrichteninhalte oder Hintergrundreportagen kaum für die Weiterleitung zu einem Webshop, da Affiliate-Links nach Einschätzung der Interviewpartner:innen hier unpassend erscheinen. Dagegen ist es im Falle von Produkt- oder Testberichten bzw. alltagsnahen Praxistipps, in denen Lesende eher als Konsument:innen denn als Bürger:innen adressiert werden, sehr viel naheliegender einen „Mehrwert" darin zu sehen „unsere User weiter[zu]leiten, weiter[zu]führen hin zum zufriedenstellenden Kauf" (I1, Pos. 18). Es sind solche Artikel, bei denen „es extrem Sinn [macht], dass auch so zu schreiben, dass wir sagen, wir geben da eine Kaufberatung, Kaufempfehlung, und dann kann man […] Werbebotschaft und Inhalt […] wahnsinnig gut

kombinieren“ (I7, Pos. 31). Hier findet mit anderen Worten eine Auflösung des erwähnten Spannungsverhältnisses von ökonomischen Interessen und demokratischem Auftrag durch Angleichung von Werbung und redaktionellen Inhalten statt: Wenn Journalismus als Kaufberatung auftritt, ist es auch legitim ihn gezielt mit Werbung ‚anzureichern'.[13] Die Tatsache, dass auf Third-Party-Cookies beruhende Geschäftsmodelle zukünftig erschwert werden, stellt für Publisher, die stark von Werbeeinnahmen abhängig sind, somit einen Anreiz dar, zunehmend auf *Affiliate Marketing* zu setzen. Damit werden solche Artikel wichtiger, die bereits nah am Kaufakt sind und bei denen es folglich keinen starken Bruch zwischen Inhalt und der Weiterleitung zu einem Webshop gibt.

Eine ähnliche Vermutung äußert Bleier (2021, S. 8) auch in Bezug auf das oben angesprochene *kontextuelle Targeting*:

> „An increased reliance on contextual advertising strengthens the incentives for publishers to focus on narrow, targetable audiences, since contextual targeting, in its traditional form, depends on webpage content itself to segment users […]. By contrast, behavioral advertising is rather content-neutral. […] Publishers' contextual ads may become less valuable when their audience does not have distinct features, since contextual targeting becomes less precise. As a result, revenue generated by general content websites (e.g., news, political news, or business news), might be lower than that generated by websites with specific product categories such as entertainment or automobile […].” (Bleier 2021, S. 8)

Diese stärkere Bedeutung zielgruppenspezifischer Inhalte im Rahmen des *kontextuellen Targetings* zeigt sich auch in Versuchen, die kontextuelle Analyse durch Verfahren des maschinellen Lernens anzureichern, um „Themen“ in redaktionellen Beiträgen zu identifizieren, die „nahe an einem Kaufinteresse“ sind (I4, Pos. 33).[14]

---

13 Diese Angleichung schlägt sich sprachlich im Begriff des „Contents“ nieder. So kritisiert Meckel (2010, S. 223) „die Vermischung und Nivellierung jeglicher von erheblichen kategorialen Unterschieden geprägten Inhalte im Internet unter dem Begriff ‚Content'. [...] Hier steht ‚Content' für eine generalisierte Produktkategorie von Angeboten, deren Gehalt erst einmal zweitrangig ist, solange sie sich vermarkten lassen.“

14 Lauerer (2021, S. 221ff.) beobachtet ähnliche Angleichungsdynamiken im *Affiliate Marketing*, stellt aber fest, dass diese Entwicklung unterschiedliche Bewertungen erfährt. Während einige Verlage es als unzulässige Grenzüberschreitung wahrnehmen

Während bisher argumentiert wurde, dass *Affiliate Marketing* und *kontextuelles Targeting* zu einer *Angleichung* von Werbung und redaktionellem Inhalt oder zu einer *Verschiebung* von Inhalten zur besseren Erreichbarkeit spezifischer Zielgruppen führen könnte, ist im Fall des *Native Advertising* eher von einer *Vermischung* von Inhalt und Werbung zu sprechen. Unter dem *Native-Advertising-Modell* versteht man den Ansatz, Werbeinhalte in Form von redaktionellen Beiträgen aufzuarbeiten, sodass beides kaum noch voneinander zu unterscheiden ist: „Das heißt Native Advertising, weil es sich eben recht nativ in den Content mit einbettet und dementsprechend weniger störend für den User ist" (I6, Pos. 7). Dabei geht es um Inhalte, die von oder für Werbekunden geschrieben werden, aber den Eindruck erwecken, redaktionelle Inhalte zu sein. Während auch für das *Native Advertising* technische Tools zur Verfügung stehen, um bspw. die teilautomatisierte Ausspielung von Leseempfehlungen über Netzwerke hinweg zu organisieren, findet die meiste Wertschöpfung in der Interaktion zwischen Publishern und Werbetreibenden und deren Agenturen statt. Die wohl am häufigsten genutzte Form des *Native Advertising* ist das Advertorial.

Die Bedeutung von Nutzerdaten für das Geschäftsmodell des *Native Advertising* ist in der Erfolgskontrolle nicht zu unterschätzen, rückt aber bei der Wertschöpfung in den Hintergrund. Während bei den von Analytics-Dienstleistern angebotenen Native-Advertising-Netzwerken die Ausspielung von Kampagnen und Leseempfehlungen ausschließlich datengetrieben abläuft, ist das Erstellen eines Advertorials für einen Werbekunden unabhängig von Nutzerdaten. In Abhängigkeit des vereinbarten Erlösmodells, das entweder fixe oder Performance-abhängige Ausspielungsraten vergütet, werden Daten benötigt, allerdings keine nutzerbezogenen. So sehen Publisher das Native-Advertising-Geschäft zunehmend als privatheitsfreundliche Alternative zum noch dominanten, aber schwindenden, programmatischen Modell. Entsprechend wird auch seitens der Werbeindustrie zu begründen versucht, „[w]hy native advertising is a smart choice in the era of privacy" (Bojikian/Xu 2022). Wenngleich *Native Advertising* als Werbung gekennzeichnet werden muss, sehen Kritiker:innen in diesem Werbeformat eine strukturell angelegte Täuschungsabsicht. So argumentiert z. B. Porlezza (2017, S. 250), dass „bei Native Advertising die Gefahr einer Täuschung des Lesers [besteht], indem unabhängige journalistische

Artikel auf das *Affiliate Marketing* auszurichten, verfügen andere bereits über speziell dafür vorgesehene Redaktionsteams (ebd., S. 222f.).

Inhalte vorgegaukelt werden, während faktisch handfeste werbliche und finanzielle Interessen im Spiel sind." Insbesondere der Qualitätsjournalismus drohe hier seine Glaubwürdigkeit und das Vertrauen der Lesenden einzubüßen (vgl. Bachmann u.a. 2019; Lauerer 2021, S. 217f.).[15]

Im *Affiliate Marketing*, dem *kontextuellen Targeting* und dem *Native Advertising* deutet sich also zusammenfassend ein Trade-off zwischen dem vorherrschenden Privatheitsverständnis und journalistischen Qualitätsnormen an. Dies zeigt sich daran, dass es gerade diejenigen Werbemodelle sind, die am wenigsten auf Third-Party-Cookies angewiesen sind, bei denen Angleichungs- und Vermischungsdynamiken von Werbung und journalistischen Inhalten am stärksten ausgeprägt sind. Gleichzeitig erscheint es vor dem Hintergrund technischer und regulatorischer Entwicklungen für Publisher nahezu unausweichlich, verstärkt auf diese Werbemodelle zu setzen, wenn Paid-Content als (alleinige) Finanzierungsoption weniger erfolgsversprechend ist (vgl. Lobigs 2018, S. 305ff.).

5. Fazit

Der vorliegende Beitrag widmete sich den Herausforderungen, die im Feld des digitalen Journalismus aufgrund verschiedener regulativer und technischer Datenschutzinitiativen auftreten. Durch die hohe Datenabhängigkeit werbegetriebener Geschäftsmodelle fordern Datenschutzinitiativen die ökonomische Profitabilität von Publishern heraus, weshalb diese mit alternativen Finanzierungsmöglichkeiten experimentieren, die den vermeintlichen Anforderungen des Datenschutzes genügen sollen, dabei aber nichtintendierte Nebenfolgen sowohl für Privatheit als auch für journalistische Qualitätsnormen generieren können. Wenngleich bestimmte Datenschutzmaßnahmen hinsichtlich ihrer Nebenfolgen kritisch betrachtet wurden, wäre eine grundsätzliche Kritik an Datenschutzbemühungen verkürzt. Vielmehr zielten die vorangegangenen Überlegungen auf eine Problematisierung von potenziellen Entwicklungen, die durch spezifische Umsetzungs-

15 Lauerer (2021, S. 218) zeigt aber auch, dass „Glaubwürdigkeit" als möglicher „gemeinsamer Nenner" von Werbung und journalistischen Inhalten dienen kann, da Werbetreibende bestrebt sind ihre Anzeigen in einem glaubwürdigen Umfeld zu platzieren. Publisher müssen zudem ihr langfristiges Kalkül der Kundenbindung mittels eines glaubwürdigen und in diesem Sinne „guten [inhaltlichen] Kern[s]" (I4, Pos. 51) mit der kurzfristigen Steigerung von Werbeeinnahmen ausbalancieren. Eine fehlende Ausgewogenheit (oder ein mangelndes Passungsverhältnis) von redaktionellem Inhalt und Werbung wird entsprechend als finanzieller Nachteil thematisiert.

Geschäftsmodell			Reaktionen	
	Beschreibung	*Daten-Typ (Bedeutung)*	*Privatheitsregulierung und Datennutzung*	*Journalistische Inhalte und Werbung*
Paid Content	Kostenpflichtige Bereitstellung von Inhalten; digitale Paywalls; Abo-Modelle	First-Party (niedrig)	Trend zu Bezahlmodellen, aber fehlende Zahlungsbereitschaft von Nutzenden; wachsende Bedeutung von First-Party-Daten; fehlende Wahlmöglichkeiten für Nutzende	Inhalt (meist) unabhängig von Werbung
Pur	Wahl zwischen Tracking und Bezahlung	First-Party (hoch)	Potentielle Verschärfung von Third-Party-Nutzung wegen fehlender Zahlungsbereitschaft von Nutzenden	
Programmatic	Algorithmische Ausspielung; Auktionsmechanismen; datengetriebene Ausspielung	First-/Third-Party (hoch)	Wachsende Bedeutung von First-Party-Daten; Ausweichen auf kontextuelles Targeting; Zuspitzung oder Verlagerung privatheits-rechtlicher Probleme	Werbung/redaktionelle Inhalte relativ unabhängig voneinander, aber trotzdem potenziell Diskussion um Passungsverhältnis von Werbung und Inhalt
Display-/Banner	Semi-manueller Handel von Werbeplätzen; Kampagnengetrieben	First-/Third-Party (hoch)		
Affiliate Marketing	Vermarktung E-Commerce; produktgetriebener Content; variable /fixe Provision	First-/Third-Party (hoch)		Wechselseitige Annäherung von Werbe-botschaft und Inhalt (Kauf-beratung, Praxis-Tipps); Wandel zu „Content“
Native	Werbeinhalte als redaktio-neller Content; transparente Kennzeichnung	First-Third-Party (medium)		Werbung im redaktionellen Gewand

Tabelle 2: Übersicht über dominante Geschäftsmodelle des digitalen Journalismus und assoziierte Reaktionen auf Datenschutzregulierungen

formen und Verständnisse der Datenschutzgestaltung entstehen können. Dabei wurde deutlich, dass große Plattformunternehmen wie Google oder Apple aktiv die Gestaltung des Datenschutzes voranbringen und dass die zum Teil unerfreulichen gesellschaftlichen Nebenfolgen auch durch bestimmte Grundsatzentscheidungen des Datenschutzrechts ermöglicht werden. Die erwähnten Angleichungstendenzen von Werbung und journalistischen Inhalten sind dabei als indirekte Nebenfolgen von Datenschutzmaßnahmen wie der Unterbindung von Third-Party-Cookies zu verstehen, in-

sofern diese ein Ausweichen auf datensparsamere Werbemodelle wie das *Affiliate Marketing* oder *Native Advertising* nahelegen, die zugleich journalistische Qualitätsnormen unter Druck setzen. Demgegenüber sind die verstärkten Tendenzen zur Generierung von First-Party-Daten, das *kontextuelle Targeting* oder das *Pur-Modell* direkte Konsequenzen bestimmter Grundsatzentscheidungen des Datenschutzes. Während das *Pur-Modell* die Nutzung von Third-Party-Cookies sogar noch verschärfen könnte, wenn Nutzende nicht bereit sind für den Verzicht auf Tracking zu bezahlen, sind die Privatheitsgefährdungen bei der Nutzung von First-Party-Daten und dem kontextuellen Targeting anders gelagert. Hier ist die (in anderen Zusammenhängen häufig problematisierte) Fokussierung des Datenschutzrechts auf die Regulierung personenbezogener Daten entscheidend, die wiederum z. B. die Effekte der Nutzung von vermeintlich als unproblematisch angesehenen anonymisierten Daten außer Acht lässt, die aber Privatheitsherausforderungen auf überindividueller Ebene generieren können, zu denen beispielsweise unzulässige Diskriminierungen von Personengruppen gehören (Floridi 2017; Mühlhoff 2022). Dabei wurde deutlich, dass sich bestimmte Nebenfolgen dieser datenschutzrechtlichen Grundsatzentscheidungen markant im Feld des digitalen Journalismus zeigen.

Vor diesem Hintergrund würde es zu kurz greifen, wenn die kritische Beobachtung erst bei der Verletzung bestimmter normativer oder rechtlicher Grundsätze ansetzt. Der kursorische Blick auf die verschiedenen datenökonomischen Praktiken der unterschiedlichen Akteure des digitalen Journalismus machte vielmehr deutlich, dass auch die formale Befolgung bestimmter Datenschutzgrundsätze zu gesellschaftlich unerfreulichen Nebenfolgen beitragen kann. Somit ist es gerade ein vertieftes Verständnis für die Generierung sog. struktureller Ungerechtigkeiten (Young 2011), die als Nebeneffekt des alltäglichen Vollzugs von Praktiken verschiedener Akteure entstehen, das für weiterführende Überlegungen grundlegend sein dürfte. Zudem legt ein differenzierter Blick auf das Ökosystem des digitalen Journalismus nahe, dass auch Reaktionsweisen und Strategien der Publisher auf bestimmte Datenschutzinitiativen nicht grundsätzlich kritisiert, sondern hinsichtlich vorhandener Pfadoptionen und Folgewirkungen im Ökosystem des digitalen Journalismus eingeordnet werden müssen. Die Publisher erscheinen dabei häufig als Getriebene externer Entwicklungen, sofern etwa große Plattformunternehmen mit ihren Infrastrukturentscheidungen, die selbst wettbewerbsstrategischen Überlegungen folgen und die Rahmenbedingungen des Datenschutzrechts zu ihrem eigenen Vorteil auslegen, den Publishern nur begrenzte Handlungsspielräume lassen. Statt also

einzelne Akteure für spezifische Konflikte verantwortlich zu machen, gilt es angesichts der hier favorisierten Ökosystemperspektive Überlegungen zur kollektiven Verteilung von Verantwortlichkeiten anzustellen (Young 2011). Dabei wäre zu fragen, wie ein Ökosystem des digitalen Journalismus beschaffen sein müsste, das für die hier diskutierten Trade-offs zwischen Werten wie Privatheit, Datenschutz, Wettbewerb und journalistischen Qualitätsnormen sensibel ist und damit eine *faire Vermittlung* verschiedener Wertgesichtspunkte ermöglicht (vgl. Uhlmann u.a. 2022).

Literatur

Alaimo, Christina und Kallinikos, Jannis (2018): Objects, Metrics and Practices: An Inquiry into the Programmatic Advertising Ecosystem. In: Schultze, Ulrike; Aanestad, Margunn u.a. (Hrsg.): *Living with Monsters? Social Implications of Algorithmic Phenomena, Hybrid Agency, and the Performativity of Technology*. Cham, Springer International Publishing, S. 110-123.

Alvesson, Mats und Sköldberg, Kaj (2009): *Reflexive Methodology: New Vistas for Qualitative Research*. London: SAGE Publications.

Bachmann, Philipp; Hunziker, Sévérine und Rüedy, Tanja (2019): Selling their souls to the advertisers? How native advertising degrades the quality of prestige media outlets. *Journal of Media Business Studies*, 16(2), S. 95-109.

Bleier, Alexander (2021): On the Viability of Contextual Advertising as a Privacy-Preserving Alternative to Behavioral Advertising on the Web: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3980001 (besucht am 26.01.2023).

Bojikian, Pedro und Xu, Nora (28. April 2022): Why native advertising is a smart choice in the era of privacy. URL: https://about.ads.microsoft.com/en-us/blog/post/april-2022/why-native-advertising-is-a-smart-choice-in-the-era-of-privacy (besucht am 07.02.2023).

Brittin, Matt (21. Sept. 2022): Die digitale Zukunft weiterdenken, um das werbefinanzierte Internet zu verbessern. URL: https://blog.google/intl/de-de/unternehmen/inside-google/dmexco-2022-die-digitale-zukunft-weiterdenken/ (besucht am 24.01.2023).

Couldry, Nick und Mejias, Ulises A. (2019): *The Costs of Connection. How Data Is Colonizing Human Life and Appropriating It for Capitalism*. Stanford: Stanford University Press.

Edelman, Gilad (12. April 2021): Antitrust and Privacy are on a collision course. URL: https://www.wired.com/story/antitrust-privacy-on-collision-course/ (besucht am 24.01.2023).

Eisenegger, Mark und Udris, Linards (2021): Medienqualität in der digitalen Ära. Konzeptuelle Herausforderungen und erste Antworten. In: Magin, Melanie; Rußmann, Uta und Stark, Birgit (Hrsg.): *Demokratie braucht Medien*. Wiesbaden: Springer, S. 91-113.

Eliot, David und Wood, David Murakami (2022): Culling the FLoC: Market forces, regulatory regimes and Google's (mis)steps on the path away from targeted advertising. *Information Polity*, 27(2), S. 259-274.

Floridi, Luciano (2017): Group Privacy: A Defence and Interpretation. In: Taylor, Linnet; Floridi, Luciano und van der Sloot, Bart (Hrsg.): *Group Privacy: New Challenges of Data Technologies*. Springer, S. 83-100.

Geradin, Damien; Katsifis, Dimitrios und Karanikioti, Theano (2021): Google as a *de facto* privacy regulator: analysing the Privacy Sandbox from an antitrust perspective. *European Competition Journal*, 17(3), S. 1-65.

Heß, Claudia und Kneuper, Ralf (2023): Googles neue Ansätze aus der Privacy Sandbox für zielgruppenorientierte Werbung im Internet. In: Lucas, Christian und Schuster, Gabriele (Hrsg.): *Innovatives und digitales Marketing in der Praxis. Insights, Strategien und Impulse für Unternehmen*. Wiesbaden: Springer, S. 233-248.

Hoppner, Thomas und Westerhoff, Philipp (2021): Privacy by Default, Abuse by Design: EU Competition Concerns About Apple's New App Tracking. Hausfeld Competition Bulletin, Spring 2021. Online verfügbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3853981 (besucht am 03.02.2023).

Kollning, Konrad; Shuba, Anastasia u.a. (2022): Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels. In: *2022 ACM Conference on Fairness, Accountability, and Transparency*. Online verfügbar unter: https://arxiv.org/pdf/2204.03556.pdf (besucht am 02.02.2023).

Lauerer, Corinna (2021): *Zaungespräche statt Brandschutzmauer. Die Beziehung von Werbung & Journalismus in Verlagen*. Wiesbaden: Springer.

Lobigs, Frank (2018): Wirtschaftliche Probleme des Journalismus im Internet. Verdrängungsängste und fehlende Erlösquellen. In: Nuernbergk, Christian und Neuberger, Christoph (Hrsg.): *Journalismus im Internet. Profession - Partizipation - Technisierung*. Wiesbaden: Springer, S. 295-334.

Lorenz, Dagmar (2009): *Journalismus*. Stuttgart: J.B. Metzler.

Lünenborg, Margreth (2012): Qualität in der Krise? *Aus Politik und Zeitgeschichte (APuZ)*, 29-31/2012, S. 3-8.

Malcom, William und Bethell, Oliver (11. Feb. 2022): Die nächsten Schritte mit Privacy Sandbox. URL: https://blog.google/intl/de-de/produkte/android-chrome-mehr/die-nachsten-schritte-mit-privacy-sandbox/ (besucht am 24.01.2023).

Meckel, Miriam (2010). Proudly content free. *Publizistik*, 55, S. 223-229.

Mühlhoff, Rainer (2022): Prädiktive Privatheit: Kollektiver Datenschutz im Kontext von Big Data und KI. In: Friedewald, Michael; Roßnagel, Alexander u.a. (Hrsg.): *Künstliche Intelligenz, Demokratie und Privatheit.* Baden-Baden: Nomos, S. 31-58.

Neuberger, Christoph (2018): Journalismus in der Netzwerköffentlichkeit. Zum Verhältnis zwischen Profession, Partizipation und Technik. In: Nuernbergk, Christian und Neuberger, Christoph (Hrsg.): *Journalismus im Internet. Profession - Partizipation - Technisierung*. Wiesbaden: Springer, S. 11-80.

Nottingham, Mark (2021): Playing Fair in the Privacy Sandbox: Competition, Privacy and Interoperability Standards. Online verfügbar unter: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891335 (besucht am 24.01.2023).

NOYB (2021): Beschwerde nach Artikel 77 (1), 80 (1) DSGVO. Noyb Fallnummer: C-050. Online verfügbar unter: https://noyb.eu/sites/default/files/2021-08/t-online_Beschwerde_PUBLIC.pdf (besucht am 26.01.2023).

Popiel, Pawel (2022): Regulating datafication and platformization: Policy silos and tradeoffs in international platform inquiries. *Policy & Internet,* 14(1), S. 28-46.

Porlezza, Colin (2017): Digitaler Journalismus zwischen News und Native Advertising - Risiken und Nebenwirkungen einer heiklen Beziehung. In: Meier, Werner A. (Hrsg.): *Abbruch - Umbruch - Aufbruch. Globaler Medienwandel und lokale Medienkrisen*. Baden-Baden: Nomos, S. 249-270.

Ravichandran, Deepak und Korula, Nitish (2019): Effect of disabling third-party cookies on publisher revenue: https://www.semanticscholar.org/paper/Effect-of-disablin g-third-party-cookies-on-revenue-Ravichandran-Korula/e570d982e9c6aa072dfdf0b4 106fc4b1d86cdb23 (besucht am 07.02.2023).

Schröder, Michael und Schwanebeck, Axel (2011): *Qualität unter Druck. Journalismus im Internet-Zeitalter*. Baden-Baden: Nomos.

Stallone, Valerio; Gägauf, Aline und Kaya, Tania (2022): Who Ate All Our Cookies? Investigating Publishers' Challenges Caused by Changes in Third-party Cookie Tracking. In: *Proceedings of the 18th International Conference on Web Information Systems and Technologies*, S. 97-104.

Thomas, Ian (2021): Planning for a cookie-less future: How browser and mobile privacy changes will impact marketing, targeting and analytics. *Applied Marketing Analytics*, 7(1), S. 6-16.

Uhlmann, Markus; Kropf, Jonathan und Lamla, Jörn (2022): Datenintermediäre als Fairness-Akteure in der Datenökonomie. Vortrag 15 der Reihe: "Zu treuen Händen". Verbraucherzentrale NRW e.V.: https://www.verbraucherforschung.nrw/sites/default /files/2022-02/zth-15-uhlmann-kropf-lamla-datenintermediaere-als-fairness-akteure -in-der-datenoekonomie.pdf (besucht am 09.02.2023).

Weischenberg, Siegfried (2018): *Medienkrise und Medienkrieg: Brauchen wir überhaupt noch Journalismus?* Wiesbaden: Springer.

Wellbrock, Christian-Mathias (2020): Spotify für Journalismus, Verlagsplattform, Digitales Pressegrosso. Drei Szenarien für eine anbieterübergreifende Journalismusplattform. *Journalistik. Zeitschrift für Journalismusforschung*, 2(3), S. 131-149.

Wernet, Andreas (2021): *Einladung zur Objektiven Hermeneutik. Ein Studienbuch für den Einstieg*. Opladen und Toronto: Barbara Budrich.

Young (2011): *Responsibility for justice*. Oxford: Oxford University Press.

Zerback, Thomas (2021): Qualität politischer Kommunikation. In: Borucki, Isabelle; Kleinen-von Königslöw, Katharina u.a. (Hrsg.): *Handbuch politische Kommunikation*. Wiesbaden: Springer, S. 1-14.

Zuboff, Shoshana (2018): *Das Zeitalter des Überwachungskapitalismus*. Frankfurt und New York: Campus.

Teil III: Fairness und Governance

Datenschutzzertifizierung: Ende des Dornröschenschlafs? Potentiale und Erfolgsfaktoren der Zertifizierung als Instrument für eine effektive und grundrechtsorientierte Data Governance[1]

Gerrit Hornung und Marcel Kohpeiß

Zusammenfassung

Das Vollzugsdefizit des „alten" Datenschutzrechts war ein zentrales Motiv des europäischen Gesetzgebers für seine Reform. Das Governance-System der DSGVO verfügt nunmehr über einen Instrumentenmix, bei dem gerade die Zertifizierung erhebliche Potentiale für eine Effektuierung des Datenschutzes hat. Die ersten genehmigten Programme und aktuelle Diskussionen zeigen allerdings, dass eine effektive Zertifizierung voraussetzungsvoll ist und etliche Fragen ungeklärt sind. Zwei zentrale Herausforderungen sind der Umgang mit spezialgesetzlichen Anforderungen und mit ungeklärten, für die Verarbeitungspraxis wichtigen Rechtsfragen; Letzteres lässt sich exemplarisch an der Frage der Drittlandsübermittlung verdeutlichen. (Nur) wenn diese und andere Herausforderungen adressiert werden, kann die Zertifizierung ein wichtiger Baustein einer grundrechtsorientierten Data Governance der Zukunft werden.

1. Einleitung

Das Konzept einer unabhängigen Prüfung, ob datenschutzrechtliche Vorgaben beim Angebot von Waren oder Dienstleistungen eingehalten werden, ist inzwischen mehr als 20 Jahre alt. Auf Basis dieser Überlegungen[2] und der überzeugenden Argumente für derartige unabhängige Überprüfungs-

1 Der Text ist im Rahmen des BMBF-Projekts Data Protection Certification for Educational Information Systems (DIRECTIONS) (FKZ 01PP21003C) entstanden.

2 Eine erste umfassende Konzeption eines Audits (die tlw. mit der „Zertifizierung" nach der DSGVO deckungsgleich ist) findet sich bei *Roßnagel*, Datenschutzaudit: Konzeption, Durchführung, gesetzliche Regelung, 2000; ferner *Bizer*, in: Bäumler/v. Mutius, Datenschutzgesetze der dritten Generation, 1999, S. 54 ff.; zum Überprüfungskonzept: *Königshofen*, DuD 2000, 357-360; *Drews/Kranz*, DuD 2000, 226-230.

konzepte verabschiedeten mehrere Bundesländer gesetzliche Regelungen.[3] Wichtigstes Beispiel für eine erfolgreich umgesetzte und genutzte Regelung war § 4 LDSG-SH a.F., der i.V.m. mit der Datenschutzauditverordnung-SH zu einer Vielzahl von Datenschutzaudits und Zertifizierung führte.[4]

Nicht zuletzt wegen des Erfolges dieses Selbstregulierungsinstruments sowie wegen nachfolgender, europaweiter Forschungsaktivitäten im Bereich der Datenschutzzertifizierungen und Datenschutzaudits[5] gelang es, das Thema in den Gesetzgebungsprozess der europäischen Datenschutzreform einzubringen und Zertifizierungsvorschriften in Art. 42 und Art. 43 DSGVO zu verankern. Diese dienen nunmehr als europaweit einheitliche Rechtsgrundlagen für die Zertifizierung, den Zertifizierungsprozess sowie die Akkreditierung von Zertifizierungsstellen und müssen nur an wenigen Stellen durch nationale Umsetzungsvorschriften ergänzt werden.[6]

Aus einer breiteren Perspektive fügen sich die genannten Regelungen der DSGVO in ein Geflecht von Zertifizierungen ein, das gerade im IT-Bereich in den letzten Jahren ständig dichter und zugleich heterogener geworden ist. Weitere Beispiele sind die Cybersicherheitszertifizierung gem. Art. 58 des Rechtsakts zur Cybersicherheit[7] i.V.m. § 9a BSIG, das KRITIS-Sicherheitszertifikat nach § 8a Abs. 3, Abs. 5 BSIG sowie das freiwillige IT-Sicherheitskennzeichen nach § 9c BSIG.[8]

Eine effektive Zertifizierung von Datenverarbeitungsvorgängen eröffnet erhebliche Chancen für eine Vielzahl von Akteuren (Abschnitt 2). Es ist deshalb nicht verwunderlich, dass große Hoffnungen in die neuen europäischen Regelungen gelegt werden. Demgegenüber ist das Zwischenergebnis einigermaßen ernüchternd, denn von außen betrachtet scheint die Zertifizierung seit der Verabschiedung der DSGVO im Jahre 2016 zu schlafen: Eine Zertifizierung von Datenverarbeitungsvorgängen nach der DSGVO ist bisher nicht erfolgt. Jedoch scheint es nach über fünf Jahren Licht am

3 Z.B. § 5 DSG-MV a.F., § 7b BremDSG a.F., § 4 LDSG-SH a.F.

4 Durch das ULD vergebenen Gütesiegel: https://www.datenschutzzentrum.de/guetesiegel/register/.

5 V.a. das EuroPriSe-Projekt, das sich bereits 2009 als Ansatz zu einem europäischen Datenschutzsiegel aus dem Siegel des ULD heraus entwickelte; zur historischen Entwicklung s. *Richter*, ZD 2020, 84 (85).

6 In Deutschland § 39 BDSG.

7 VO (EU) 2019/881; näher *Mirtsch*, in: Mangelsdorf u.a. (Hrsg.), Normen und Standards für die digitale Transformation, 2019, 141 (151 ff.); *Kowalski/Intemann*, DuD 2018, 415-419.

8 Dazu *Hornung*, NJW 2021, 1985 (1989); *Schallbruch*, CR 2021, 450 (457 f.); zum Verfahren: BSI, Verfahrensbeschreibung zur Erteilung von IT-Sicherheitskennzeichen, 2022.

Ende des Tunnels zu geben: Gegen Ende des Jahres 2022 bogen mehrere Zertifizierungsprogramme auf die Zielgerade ein, und ein erstes Programm wurde genehmigt (Abschnitt 3). Diese und andere noch folgende Programme werden sich in den nächsten Jahren teils ergänzen und teils zueinander in Konkurrenz treten. Im Rahmen dieses Wettbewerbs werden sich mit zunehmender Anwendung der einzelnen Kriterienkataloge neue Gewohnheiten und Best Practices herausbilden, aber auch neue Probleme in der Anwendung und hinsichtlich der zu erzielenden Wirkung offenbaren. Schon jetzt ist absehbar, dass eine effektive Datenschutzzertifizierung vor noch ungelösten Problemen steht, die von den bisherigen Zertifizierungsprogrammen noch nicht vollständig adressiert werden (Abschnitt 4). Der vorläufige Zwischenstand ergibt deshalb, dass die Zertifizierung erhebliche Chancen für eine effektive Data Governance eröffnet, bis auf Weiteres aber offenbleibt, ob diese Potenziale gehoben werden können (Abschnitt 5).

2. Zertifizierung als Data Governance-Instrument

Die DSGVO hat eine umfassende Konsolidierung des Datenschutzrechts auf europäischer Ebene bewirkt. Im Innovationsgehalt unterscheiden sich ihre materiellrechtlichen und ihre verfahrensrechtlichen Teile erheblich.[9] Während sich erstere nur moderat von der alten Datenschutz-Richtlinie (DSRL) abheben (wie etwa der Vergleich von Art. 5, 6 und 9 DSGVO mit Art. 6, 7 und 8 DSRL ergibt), hat die Verordnung die datenschutzrechtlichen Governance-Instrumente grundlegend neu geordnet, um dem noch unter der DSRL bestehenden Vollzugsdefizit des europäischen Datenschutzrechts zu begegnen.[10]

2.1 Governance-Instrumente der DSGVO

Bemerkenswert ist dabei, dass der europäische Gesetzgeber sowohl klassische hoheitliche Instrumente wie aufsichtsbehördliche Anordnungsbefugnisse und Bußgelder gestärkt, als auch andere Instrumente der DSRL modifiziert oder Governance-Instrumente gänzlich neu in das europäische Datenschutzrecht eingeführt hat, so u.a. im Bereich der regulierten Selbstregu-

9 *Hornung/Spiecker gen. Döhmann*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Einl. Rn. 208 ff.

10 Ebd., m.w.N.

lierung. Beispiele dafür bilden, neben der neuen Zertifizierung (Art. 42, 43 DSGVO), die Möglichkeit zur Ausarbeitung von Verhaltensregeln (Art. 40, 41 DSGVO) sowie die erstmals europaweit vorgesehene Pflicht zur Benennung eines Datenschutzbeauftragten (Art. 37, 38 DSGVO).

Mit der Stärkung bereits in der DSRL existierender und der Einführung neuer Durchsetzungsinstrumente hat der europäische Gesetzgeber demnach den Versuch unternommen, den zum großen Teil bereits in der DSRL enthaltenen materiellen Anforderungen an Datenverarbeitungsprozesse zu mehr praktischer Wirksamkeit zu verhelfen. Der Zertifizierung als zuvor nicht im europäischen Datenschutzrecht enthaltenes Governance-Instrument kommt dabei eine zentrale Rolle zu.

2.2 Funktionen der Datenschutz-Zertifizierung

Aus einer Governance-Perspektive vermag die Zertifizierung mehrere Funktionen zu erfüllen.[11] Wenn eine Zertifizierungsstelle oder eine Aufsichtsbehörde gemäß Art. 42 Abs. 1 DSGVO die Einhaltung der Verordnung bei Verarbeitungsvorgängen eines Verantwortlichen oder Auftragsverarbeiters bestätigt, so gewinnen diese – erstens – für sich selbst, aber auch im Falle eines späteren Rechtsstreits ein erhebliches Maß an Sicherheit hinsichtlich der Rechtskonformität ihres Vorgehens. Eine Zertifizierung bietet nach der Verordnung zwar keine vollständige Gewähr hierfür, da sie lediglich einen „Faktor" bzw. „Gesichtspunkt" bei der Bewertung bildet.[12] Es steht aber zu erwarten, dass in der aufsichtsbehördlichen und gerichtlichen Praxis eine zumindest weitreichende faktische Rechtssicherheit gewonnen werden kann.

Durch eine solche Orientierung der Aufsichtsbehörden an einer zuverlässigen Zertifizierung könnte – zweitens – die aufsichtsbehördliche Tätigkeit deutlich erleichtert werden. Dieser Faktor ist wichtig, da die Behörden trotz der personellen Erweiterung im Zuge der Verabschiedung der DSGVO nach wie vor nicht über die Ressourcen verfügen, um dem Daten-

11 *Scholz,* in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Art. 42 DSGVO Rn. 4 ff. m.w.N.

12 S. Art. 24 Abs. 3 DSGVO (allgemeine Verantwortlichkeit), Art. 25 Abs. 3 DSGVO (Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen), Art. 28 Abs. 5 DSGVO (Beauftragung eines zuverlässigen Auftragsverarbeiters), Art. 32 Abs. 3 DSGVO (Sicherheit der Verarbeitung). Darüber hinaus kann die Zertifizierung gemäß Art. 46 Abs. 2 lit. f DSGVO auch eine geeignete Garantie für die Übermittlung in Drittländer sein, s.u. Kap. 4.2.2.

schutz in den vielfältigen Einzelfallgestaltungen der Praxis zu Wirksamkeit zu verhelfen.[13]

Ein wesentliches Element schon der allerersten Konzepte einer Datenschutzzertifizierung gilt außerdem auch für die DSGVO, nämlich – drittens – die Hoffnung, mit einer freiwilligen Zertifizierung der Verantwortlichen und Auftragsverarbeiter Marktanreize zur Entwicklung und zum Einsatz rechtskonformer technischer Lösungen zu setzen.[14] Denn erfolgreiche Zertifizierungen bieten die Möglichkeit, gegenüber Kunden eine nicht nur behauptete, sondern eine nachgewiesene Einhaltung des geltenden Datenschutzrechts zu demonstrieren. Eine entsprechende Nachfrage anderer Marktteilnehmer vorausgesetzt, würde sich aus diesem Wettbewerbsvorteil ein Druck auf konkurrierende Anbieter ergeben, sich ebenfalls einer Zertifizierung zu unterziehen.

Wenn sich die Zertifizierung wichtiger Anbieter in dieser Weise allgemein verbreitet, so würde schlussendlich – viertens – die Durchsetzung des Datenschutzrechts in Europa allgemein verbessert und damit das Grundrecht auf Datenschutz der betroffenen Personen gestärkt. Dies gilt auch in internationaler Perspektive, also mit Blick auf eine globale Data Governance. Denn die Zertifizierung bietet mehrere Ansatzpunkte für eine Regulierung globaler Datenflüsse und einen „Export" europäischer Datenschutzstandards und der mit ihnen verbundenen Wertvorstellungen. Es ist nicht unwahrscheinlich, dass „weiche" Durchsetzungsinstrumente wie die Zertifizierung auf einer globalen Ebene sogar effektiver sind als der Versuch, mit klassischen Methoden von Befehl und Zwang zu operieren.[15]

---

13 *Roßnagel*, Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung, 2017, 179.

14 Zu diesen erhofften Markteffekten vgl. u.a.: *Roßnagel* in: Roßnagel (Hrsg.) Handbuch Datenschutzrecht, 2003, Kap. 3.7 Rn. 1ff.; *Bäumler*, DuD 2004, 80 ff.; s. allgemeiner die Beiträge in *Bäumler/v. Mutius* (Hrsg.), Datenschutz als Wettbewerbsvorteil, 2002.

15 Dieses Problem soll hier nicht vertieft werden. Das im Ausgangspunkt umfassendste Instrument zur globalen Verbreitung europäischer Standards ist die unmittelbare Erstreckung der DSGVO auf Anbieter in Drittländern, wie sie nach dem Marktortprinzip (Art. 3 Abs. 2 lit. a DSGVO) bzw. dem Beobachtungsprinzip (Art. 3 Abs. 2 lit. b DSGVO) erfolgt. Diese Erstreckung leidet jedoch an grundsätzlichen Durchsetzungsproblemen, da die Verantwortlichen in diesen Fällen noch nicht einmal eine Niederlassung in der Union haben. Zwar können auch Zertifizierungsstellen nur begrenzt auf Anbieter aus Drittländern Einfluss nehmen. Immerhin bleibt aber als Sanktionen der Entzug der Zertifizierung möglich, und allgemein könnten weiche Instrumente, die Gegebenheiten im Drittland gegebenenfalls stärker berücksichtigen, in anderen Weltregionen auf Dialogbereitschaft treffen und so besser zur globalen Standardsetzung beitragen als aufsichtsbehördliche Anstrengungen.

2.3 Komplexität der Abläufe

Das Instrument der Zertifizierung lässt sich auf verschiedene Arten gestalten. An einem Ende des Spektrums sind Selbstzertifizierungen zu verorten, bei denen keinerlei externe Stelle eine Prüfung vornimmt, sondern allenfalls Sanktionen für den Fall drohen, dass die Behauptung der Einhaltung bestimmter Standards nicht den Tatsachen entspricht. Am anderen Ende stehen staatliche Zertifizierungen, die gesetzlich als Voraussetzung für den Markteintritt eines Anbieters vorgeschrieben werden. Das Zertifizierungskonzept der DSGVO ist innerhalb dieses Spektrums in einem mittleren Bereich zu verorten. Die Zertifizierung ist nach Art. 42 Abs. 3 DSGVO freiwillig. Sie wird gemäß Art. 42 Abs. 5 DSGVO durch eine neutrale Stelle, d.h. eine Aufsichtsbehörde oder eine nach Art. 43 DSGVO akkreditierte Zertifizierungsstelle, vorgenommen. Die staatliche Letztverantwortung wird insbesondere bei privaten Zertifizierungsstellen durch die Akkreditierung, die aufsichtsbehördliche Kontrolle der akkreditierten Stelle (Art. 43 Abs. 7 i.V.m. Art. 58 Abs. 2 lit. h DSGVO) sowie die notwendige Genehmigung der Zertifizierungskriterien (Art. 42 Abs. 5 DSGVO) durch die zuständige Aufsichtsbehörde oder den Europäischen Datenschutzausschuss (EDSA) sichergestellt.

Nur unvollständig werden demgegenüber in der Verordnung selbst die Verfahrensabläufe geregelt, die im Vorfeld der Genehmigung der Zertifizierungskriterien absolviert werden müssen.[16] Dies gilt insbesondere für die Rolle des sog. Programmeigners, nämlich einer Person oder Organisation, die v.a. für die Entwicklung und Aufrechterhaltung des Konformitätsbewertungsprogrammes einer Zertifizierung verantwortlich ist[17] und dieses im Anschluss entweder selbst als Zertifizierungsstelle nutzt oder an andere Zertifizierungsstellen lizensiert.

16 Zum Verfahren: DSK, Anforderungen an datenschutzrechtliche Zertifizierungsprogramme, Version 1.8, v. 16.04.2021; EDSA, Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals, v. 14.02.2023.

17 Vgl. DIN EN ISO/IEC 17065:2021 Ziffer 3.11, sowie DIN EN ISO/IEC 17067:2013 Ziffer 6.3.

3. Aktueller Stand Deutschland und Europa

Nach einigen Jahren des Dornröschenschlafs seit Inkrafttreten der DSGVO hat die Entwicklung von Datenschutzzertifizierungen im Jahre 2022 eine erhebliche Dynamik gewonnen. Mehr als viereinhalb Jahre nach dem Geltungsbeginn der DSGVO genehmigte die luxemburgische Aufsichtsbehörde (CNPD) mit dem Kriterienkatalog „GDPR-Certified Assurance-Report based Processing Activities (GDPR-CARPA)" das europaweit erste DSGVO-Zertifizierungsprogramm.[18] Nach Akkreditierung der EY PFS Solutions S.à r.l ist die EU-weit erste akkreditierte DSGVO-Zertifizierungsstelle bereits fähig nach dem GDPR-CARPA-Programm zu zertifizieren. Bei CARPA handelt es sich um einen Kriterienkatalog, der einen allgemeinen Ansatz verfolgt. Der Anwendungsbereich der Zertifizierung, bzw. des Kriterienkataloges ist dementsprechend nicht beschränkt. Jegliche Verarbeitungsprozesse Verantwortlicher und Auftragsverarbeiter lassen sich, unabhängig von den verwendeten Technologien, anhand des Katalogs auf ihre Vereinbarkeit mit den Voraussetzungen der DSGVO überprüfen.[19]

Einen ebenso als allgemein zu klassifizierenden Ansatz verfolgt der nachfolgend im Jahr 2022 genehmigte Kriterienkatalog des European Privacy Seals (EuroPriSe), das mittlerweile durch eine privatwirtschaftliche GmbH getragen wird. Nach der Genehmigung durch die Aufsichtsbehörde Nordrhein-Westfalens im Oktober 2022 hat EuroPriSe nun auch seinen Kriterienkatalog veröffentlicht, eine genehmigte Akkreditierungsstelle gibt es (Stand August 2023) jedoch auch in Deutschland noch nicht. Die allgemein gehaltenen EuroPriSe-Kriterien können lediglich auf Verarbeitungsprozesse von Auftragsverarbeitern angewendet werden, dies allerdings unabhängig von den verwendeten Technologien.

Von diesen allgemeinen sind sektor- und technologiebezogene Zertifizierungen und deren Kriterienkataloge zu unterscheiden. Zu diesen gehören bspw. das Programm European Cloud Service Data Protection Certification (AUDITOR) sowie das Anschlussprojekt Data Protection Certification for Educational Information Systems (DIRECTIONS). AUDITOR adres-

18 Zum Verfahrensstand: CNPD, Die CNPD nimmt «GDPR-CARPA» an.; CARPA-Kriterien: CNPD, Décision N° 15/2022, 2022; CNPD, Die CNPD ist die erste Datenschutzbehörde in Europa, die einer DSGVO-Zertifizierungsstelle Akkreditierung erteilt hat.

19 Zum Inhalt *Helmke/Link/Schild*, DuD 2023, 100-107.

siert bisher ausschließlich Anbieter von Cloud-Dienstleistungen.[20] Der AUDITOR-Kriterienkatalog befindet sich aktuell in den letzten Zügen des Genehmigungsverfahrens, dem informellen Reviewverfahren, das begleitet durch die federführende Landesaufsichtsbehörde vor dem EDSA geführt wird. Erfolgt im Rahmen des Verfahrensabschlusses die finale Stellungnahme des EDSA, so wird es zeitnah durch die federführende Landesbehörde zur Genehmigung der Kriterien kommen.[21] Das Anschlussprojekt DIRECTIONS[22] verfolgt den Ansatz einer sektorspezifischen und technologieabhängigen Zertifizierung für den Bereich von schulischen Informationssystemen.

Allgemeine Ansätze einer Zertifizierung haben den Vorteil, dass sie auf jegliche Art der Datenverarbeitung anwendbar sind. Der Vorteil von sektorspezifischen, technologieabhängigen Ansätzen ist demgegenüber die rechtliche und verfahrenstechnische Konkretisierungsleistung, die durch spezielle Kriterienkataloge erbracht werden kann. So kann durch Konkretisierung der datenschutzrechtlichen Anforderungen, die im besonderen Maße die jeweiligen bereichspezifischen Risiken in Betracht ziehen (bspw. Risiken bei der Verarbeitung personenbezogener Daten von Kindern) eine genauere und verlässlichere Aussage über das erforderliche Schutzniveau der Verarbeitungsvorgänge getroffen werden. Die dargestellten Governance-Effekte der Zertifizierung verstärken sich dementsprechend. Diesen Vorteilen stehen der – ggf. deutlich – eingeschränkte Anwendungsbereich sowie der gegenüber einem allgemeinen Ansatz höhere Aufwand der Erarbeitung einer Vielzahl von Kriterienkatalogen gegenüber. Es lässt sich deshalb zum jetzigen Zeitpunkt noch nicht beurteilen, ob sich im Ergebnis eher allgemeine oder eher spezifische Ansätze durchsetzen werden.

20 Näher https://www.auditor-cert.de/; zur Zertifizierung von Cloud-Angeboten s. Krcmar/Eckert/Roßnagel/Sunyaev/Wiesche (Hrsg.) Management sicherer Cloud-Services. Entwicklung und Evaluation dynamischer Zertifikate, 2018; aus rechtlicher Perspektive *Hofmann,* Dynamische Zertifizierung, 2019.

21 Zum letzten offiziellen Stand *Müller,* ZD-Aktuell 2022, 01239; zum Verfahrensablauf s. Fn. 16.

22 https://directions-cert.de/; die Autoren verantworten zusammen mit weiteren Kollegen die rechtswissenschaftlichen Teile des Projekts.

4. Einzelfragen einer effektiven Zertifizierung

Um der Zertifizierung als Governance-Instrument zu praktischer Wirksamkeit zu verhelfen und ihre spezifischen Vorteile nutzen zu können, müssen verschiedene Bedingungen erfüllt sein. Da die Zertifizierung nach Art. 42 Abs. 3 DSGVO für Verantwortliche und Auftragsverarbeiter freiwillig ist, muss sie für diese hinreichend attraktiv sein. Aufwand und Kosten müssen mithin in einem auch betriebswirtschaftlich vernünftigen Verhältnis zu den erhofften Vorteilen stehen.[23] Aus Governance-Perspektive kann dies zu Zielkonflikten führen. Schlanke Zertifizierungsprogramme mögen für Verantwortliche und Auftragsverarbeiter zunächst vorzugswürdig erscheinen. Wenn dies jedoch zu stark zulasten der angewendeten Prüftiefe geht, so wird die Funktion der Rechtssicherheit gefährdet, zumal die Zertifizierung die Verantwortung des Verantwortlichen oder Auftragsverarbeiters für die Einhaltung der Verordnung nicht mindert (Art. 42 Abs. 4 DSGVO). Prüfungsmaßstab und Prüftiefe sind letztlich entscheidende Weichenstellungen für alle oben erläuterten Funktionen der Datenschutz-Zertifizierung.

In diesem Bereich sind etliche Fragen noch ungeklärt. Von diesen werden im Folgenden zwei herausgegriffen, nämlich die Zertifizierungen bereichsspezifischer Vorschriften sowie der Umgang mit offenen bzw. umstrittenen Rechtsfragen.

4.1 Zertifizierbarkeit von Anforderungen außerhalb der DSGVO

Die DSGVO ist keine abschließende Regelung des Datenschutzrechts. Neben ihr existieren weitere Vorgaben auf europäischer Ebene, und die

23 U.a. diesem Grund ist gemäß Art. 42 Abs. 1 S. 2 DSGVO den Bedürfnissen von Kleinstunternehmen sowie kleinen und mittleren Unternehmen (KMU) Rechnung zu tragen. Dahinter steht wohl der Gedanke, diese wirtschaftlich nicht überbelasten und im Wettbewerb mit größeren Unternehmen nicht benachteiligen zu wollen, vgl. auch Art. 30 Abs. 5, EG 13 DSGVO. In der Literatur wird Art. 42 Abs. 1 S. 2 DSGVO dementsprechend vielfach so ausgelegt, dass KMU die Zertifizierung für geringere Kosten die Zertifizierung nutzen können sollen, sa.: *Scholz,* in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Art. 42 DSGVO Rn. 20; *Paal/Kumkar*, in: Paal/Pauly (Hrsg.), DS-GVO BDSG, 2021, Art. 42 Rn. 8; *Duisberg*, ZD 2018, 53. Wie dies ausgestaltet und wie insbesondere Marktverzerrungen verhindert werden sollen, ist bisher ebenso unklar wie eine denkbare Berücksichtigung der Interessen von KMU in anderen Rollen (z.B. als Zertifizierungsstelle). Eindeutig ist dagegen, dass für KMU keine Absenkung des DSGVO-Schutzniveaus vorgenommen werden darf, s. *Hofmann*, Dynamische Zertifizierung, 2019, S. 318 m.w.N.

Verordnung selbst lässt mit ihren zahlreichen Öffnungsklauseln mitgliedstaatliche Spezialregelungen zu. Je nach mitgliedstaatlichem Regelungsansatz wird eine umfassende datenschutzrechtliche Bewertung der Verarbeitungsvorgänge eines Verantwortlichen oder Auftragsverarbeiters dementsprechend die Anwendung nicht nur der Verordnung, sondern auch derartiger spezialgesetzlicher Regelungen erfordern. Es ist jedoch unklar, ob diese auch im Rahmen der Zertifizierung zu berücksichtigen sind.

Grundsätzliche Überlegungen

Für die Unzulässigkeit der Zertifizierung von Kriterien, die sich nicht den Vorschriften der DSGVO selbst entnehmen lassen, lässt sich zunächst der Wortlaut des Art. 42 Abs. 1 S. 1 DSGVO anführen. Danach dienen Zertifizierungsverfahren dazu, nachzuweisen, dass „diese Verordnung" eingehalten wird. Eine Berücksichtigung jedenfalls mitgliedstaatlicher Spezialgesetze könnte außerdem zu einer Fragmentierung der Zertifizierungsverfahren führen, die einer europaweiten einheitlichen Anwendung und einem produktiven Wettbewerb der Verfahren im Binnenmarkt abträglich sein könnte.

Demgegenüber spricht für eine über den Wortlaut der DSGVO hinausgehende Berücksichtigung von spezialgesetzlichen Datenschutzregelungen, dass die erläuterten Zwecke und Funktionen der Zertifizierung bei einer Beschränkung auf die Verordnung als Prüfungsmaßstab gefährdet werden würden. Denn die durch das Zertifikat bestätigte Rechtskonformität würde sich in diesem Fall regelmäßig nur auf einen Teil der für einen Verantwortlichen oder Auftragsverarbeiter geltenden materiell- und verfahrensrechtlichen Anforderungen erstrecken. Eine Entlastung der Aufsichtsbehörden und eine verbesserte Durchsetzung des Datenschutzrechts (das zweite und vierte der oben erläuterten Ziele) könnte auf diesem Wege zwar noch partiell erreicht werden. Der Zugewinn an Rechtssicherheit dürfte dagegen jedoch mehr als nur teilweise leiden. Denn mit den speziellen datenschutzrechtlichen Regelungen, würde regelmäßig der Teil der rechtlichen Vorgaben ausgeklammert, dessen Einhaltung im jeweiligen Marktsegment von besonderer Bedeutung ist. Dies kann den Eintritt der genannten Markteffekte erheblich bedrohen.[24]

24 Wenn Anbieter beispielsweise im Markt schulischer Informationssysteme mit einem Zertifikat auftreten, das lediglich die Einhaltung der DSGVO-Vorschriften bestätigt, die Einhaltung der der Schulgesetze der Länder jedoch ausklammert, könnten Schul-

Differenzierung nach Typen von Spezialgesetzen

Um sich einer Lösung des Problems zu nähern, bietet es sich an, zwischen verschiedenen speziellen Vorschriften zu unterscheiden. Dies sind

1. bereichsspezifische, unmittelbar geltende europäische Datenschutznormen (Verordnungen),
2. nationale Normen in Umsetzung bereichsspezifischer europäischer Richtlinien sowie
3. nationale Normen, die in Ausfüllung von Öffnungsklauseln der DSGVO erlassen werden.

Das wohl wichtigste Beispiel für eine bereichspezifische Verordnung wäre eine künftige e-Privacy-VO, so deren Gesetzgebungsgeschichte irgendwann enden sollte.[25] Aber auch in anderen Verarbeitungssektoren zeichnet sich eine Tendenz des europäischen Gesetzgebers ab, bereichsspezifische Datenschutznormen zu verabschieden. Dies gilt beispielsweise für mehrere Regelungen der geplanten KI-Verordnung.[26] Die Entwürfe zu diesen Rechtsakten enthalten weder eine Erweiterung des Anwendungsbereichs von Art. 42 Abs. 1 DSGVO noch andere Regelungen zur Datenschutzzertifizierung.[27] Soweit ersichtlich, gilt dasselbe für alle bereits existierenden bereichsspezifischen EU-Verordnungen mit datenschutzrechtlichen Regelungen.[28] Daraus ließe sich der Schluss ziehen, dass die spezialgesetzlichen

---

träger und Schulen bei entsprechenden Beschaffungsentscheidungen nicht anhand des Zertifikats darauf vertrauen, dass die Informationssysteme rechtskonform einsetzbar sind.

25 Entwurf: COM(2017) 10 Final. Das Parlament hat am 26.10.2017 (Report: A8-0324/2017), der Rat am 10.02.2021 (Council, 6078/21) eine Position verabschiedet. Ein Ende des Trilogs ist nicht in Sicht.

26 Der Entwurf (COM(2021) 206 final) enthält etwa eine Verarbeitungsbefugnis zur Vermeidung von Verzerrungen der KI-Systeme (Art. 10 Abs. 5 KI-VO-E) und eine Erlaubnis zur Zweckänderung für die Verarbeitung in KI-Reallaboren (Art. 54 Abs. 1 KI-VO-E); näher *Hornung*, in: Rostalski (Hrsg.), Künstliche Intelligenz. Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?, 2022, 91 ff.

27 Dies gilt bspw. für die Entwürfe zur e-Privacy-VO. Art. 1 Abs. 3 e-Privacy-VO-E (COM/2017/010 final) und Art. 1 Abs. 3 e-Privacy-ÄndV-Parlament (A8-0324/2017) ordnen an, dass die e-Privacy-VO die DSGVO präzisieren und ergänzen soll. Dies lässt Rückschlüsse auf eine gewünschte Harmonisierung der Rechtsakte zu, klärt aber nicht, ob die „ergänzenden" Normen der geplanten Verordnung trotz des Wortlauts von Art. 42 Abs. 1 DSGVO zertifizierbar sein sollen.

28 Eine Ausnahme bildet die VO (EU) 2018/1725, die die Datenverarbeitung durch Organe, Einrichtungen und sonstige Stellen der Union regelt. Sie ist allerdings keine echte Spezialregelung, sondern das Äquivalent zur DSGVO in diesem Bereich, sodass

Anforderungen nicht Maßstab einer Datenschutzzertifizierung sein sollen. Allerdings gibt es für eine derartige Regelungsabsicht des Gesetzgebers ebenfalls keinerlei Anhaltspunkte. Angesichts fehlender Hinweise in den Gesetzgebungsmaterialien spricht alles dafür, dass dem europäischen Gesetzgeber das Problem überhaupt nicht bewusst war. Ohne derartige Anhaltspunkte sollte mit Blick auf die Gefahr einer erheblichen Gefährdung der Regelungsziele der DSGVO-Zertifizierung nicht angenommen werden, dass europaweite bereichsspezifische Regelungen nicht zertifizierbar sind. Dies würde wichtige Segmente der europäischen Datenwirtschaft von der Zertifizierung ausschließen. Dieses Ergebnis allein auf den Wortlaut von Art. 42 Abs. 1 DSGVO zu stützen, ist übermäßig formalistisch und deshalb nicht überzeugend.

Bis zu einer künftigen e-Privacy-Verordnung ist das instruktivste Beispiel für die zweite Gruppe nationales Datenschutzrecht, das in Umsetzung der aktuellen e-Privacy-Richtlinie erlassen wurde. In Deutschland betrifft dies die Vorgaben des Telekommunikation-Telemedien-Datenschutz-Gesetzes (TTDSG). Verarbeitungsvorgänge im Anwendungsbereich der Richtlinie und dieses Gesetzes fallen grundsätzlich in den Anwendungsbereich der DSGVO,[29] die speziellen nationalen Anforderungen gehen jedoch nach Art. 95 DSGVO vor. Auch bei diesen Regelungen gibt es keinen Anhaltspunkt dafür, dass der europäische Gesetzgeber ihre Zertifizierbarkeit im Rahmen der Verabschiedung der DSGVO ausschließen wollte. Mit Blick auf den europaweit zumindest grundsätzlich einheitlichen Norminhalt dürfte eine Zersplitterung von Zertifizierungsprogrammen beherrschbar sein. Für eine Einbeziehung in die Zertifizierung spricht auch, dass komplexe Gesamtsysteme Teilkomponenten enthalten können, die unter das TTDSG fallen (etwa Videokonferenzfunktionen oder Messenger).[30] Die Anbieter derartiger Systeme von einer weitreichenden Rechtssicherheit

die Übernahme der Rechtsfolgen der Zertifizierung (Art. 26 Abs. 3, Art. 27 Abs. 3, Art. 29 Abs. 5 und Abs. 6, Art. 33 Abs. 4, Art. 48 Abs. 2 lit. d, EG 49, EG 51 S. 2, EG 65 S. 2 VO (EU) 2018/1725) gesetzgeberisch nahe lag.

29 Bereichsspezifische europäische Regelungen, die nicht aufgrund Spezialität der DSGVO vorgehen, sondern jenseits ihres Anwendungsbereichs liegen, werden hier ausgeklammert – v.a. die Datenverarbeitung zur Straftatbekämpfung (Regelung in der JI-Richtlinie und nationalen Umsetzungen) sowie die VO (EU) 2018/1725 (s. Fn. 28). Die JI-Richtlinie wirft im Bereich der Zertifizierung spezielle Fragen auf, s. *Johannes*, Die Polizei 2020, 409.

30 Auf die genaue Abgrenzung zwischen TTDSG und DSGVO bei derartigen Komponenten kommt es hier nicht an; dazu *Schellhas-Mende/Wiedemann/Blum*, DuD 2022, 291; *Roßnagel*, NJW 2023, 400.

auszuschließen und auf eine Teilzertifizierung zu verweisen, dient weder deren Interessen noch den Interessen anderer Marktteilnehmer. Dementsprechend erscheint es sinnvoll, im Rahmen eines modularen Aufbaus von Kriterienkatalogen die Anforderungen beispielsweise des Telekommunikation-Telemedien-Datenschutz-Gesetzes in einem Teilmodul zu kapseln, das immer dann angewendet wird, wenn die zu zertifizierenden Verarbeitungsvorgänge insgesamt oder Teile von ihnen in den Anwendungsbereich dieses Spezialgesetzes fallen.

Das Argument der fehlenden Aussagekraft gilt schließlich auch für nationale Normen, die in Ausfüllung von Öffnungsklauseln der DSGVO erlassen werden. Der Wortlaut von Art. 42 Abs. 1 DSGVO dürfte hier sogar weniger entgegenstehen als bei bereichsspezifischen Regelungen auf europäischer Ebene, da es immerhin möglich ist, nationale Normen im Bereich der Öffnungsklauseln (insbesondere bei verpflichtenden Regelungsaufträgen) in einem weiten Sinne als Teil der Verordnung zu begreifen. Gewichtiger sind jedoch die bereits erläuterten teleologischen Argumente. Insbesondere im Bereich besonders umfassender Öffnungsklauseln (vor allem Art. 6 Abs. 2 und Abs. 3, aber auch Art. 88 DSGVO) würde man bei einem engen Verständnis große Teile der für einen zu zertifizierenden Datenverarbeitungsvorgang geltenden rechtlichen Anforderungen von der Zertifizierung ausschließen. Hinzu kommt wie im Bereich des TTDSG das Problem, dass einzelne, gegebenenfalls sehr spezielle nationale Normen das angestrebte Ziel einer rechtssicheren Zertifizierung eines Gesamtsystems torpedieren würden.

Betrachtet man also abschließend die vorgenommenen Untersuchungen der drei identifizierten Vorschriftsbereiche, so stehen dem schlichten Wortlautargument, auf welches sich die Annahme der Unmöglichkeit einer Zertifizierung von bereichspezifischen Vorschriften stützt, eine Fülle an Argumenten entgegen. Im Ergebnis ist deshalb, insbesondere wegen der genannten teleologischen Argumente, die Miteinbeziehung von bereichsspezifischen, außerhalb der DSGVO liegenden Datenschutzvorschriften in die Zertifizierung nach Art. 42 DSGVO vorzugswürdig.

Konkrete Umsetzung

Mit Blick auf das wünschenswerte Ziel einer europaweit einheitlichen Zertifizierung hebt sich die erste Gruppe von Spezialgesetzen von den anderen beiden ab. Wenn über die DSGVO hinausgehende, europaweit einheitliche Normen existieren, so können Zertifizierungsprogramme aus verschiede-

nen Mitgliedstaaten diese im Rahmen von Kriterienkatalogen berücksichtigen, die sich gegenseitig ergänzen oder miteinander in Konkurrenz treten. Sollen dagegen nationale Normen in Umsetzung von Richtlinien oder Ausfüllung von Öffnungsklauseln[31] in die Kriterienkataloge eingebunden werden, so muss eine Lösung für das Problem gefunden werden, dass die mitgliedstaatlichen Entscheidungsbefugnisse praktisch unvermeidlich zu einer erheblichen Heterogenität der speziellen Anforderungen führen werden.[32] Zumindest für Programmeigner in Mitgliedstaaten mit einer hohen Anzahl von Datenverarbeitungen, die durch spezifische nationale Normen reguliert sind, könnte ein Weg darin bestehen, auf eine europaweite Genehmigung des Kriterienkatalogs zu verzichten und sich auf ein nationales Zertifizierungsprogramm zu beschränken. Allerdings stellt dies jedenfalls in föderalen Mitgliedstaaten wie Deutschland nur eine Teillösung dar, wenn die Gliedstaaten für die entsprechende Rechtsmaterie zuständig sind.

Eine Lösung für dieses Problem hat sich bisher nicht herausgebildet. Der kleinteiligste Ansatz bestünde darin, für jede (Teil-)Rechtsordnung ein spezifisches Kriterienmodul zu erstellen. Wenn ein Anbieter die Märkte mehrerer Rechtsordnungen adressieren möchte, könnten die Kriterien kumuliert oder (bei entsprechender Inhaltsgleichheit) abstrahiert und gemeinsam geprüft werden. Allerdings würde ein solches Vorgehen den Aufwand sowohl bei der konkreten Zertifizierung als auch bei der Erarbeitung und kontinuierlichen Aktualisierung des Kriterienkatalogs erheblich vergrößern. Je mehr (Teil-)Rechtsordnungen zu berücksichtigen und je variantenreicher die einzelnen Gesetzgeber aktiv sind, desto unrealistischer wird es, dass ein Programmeigner die erforderlichen Überarbeitungen und eine Aufsichtsbehörde die nachfolgenden Genehmigungen der Änderungen in einer für die Praxis der Zertifizierung notwendigen Geschwindigkeit erledigen können.

---

31 Auch wenn diese Fälle dogmatisch zu trennen sind, verschwimmen die Unterschiede in der praktischen Wirkung hinsichtlich der Handlungsspielräume der Mitgliedstaaten. Angesichts der vielen Öffnungsklauseln ist es deshalb zwar rechtlich unzutreffend, faktisch aber korrekt, die DSGVO als „Hybrid" zwischen Verordnung und Richtlinie zu bezeichnen, vgl. *Martini* u.a., Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 1 f; *Hornung/Spiecker gen. Döhmann*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Einl. Rn. 226.

32 Zu den Öffnungsklauseln s. insoweit allgemein *Martini* u.a., Die Datenschutz-Grundverordnung und das nationale Recht, 2016, S. 9 ff; *Hornung/Spiecker gen. Döhmann*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Einl. Rn. 226 ff. und *Weiß*, Öffnungsklauseln in der DSGVO und nationale Verwirklichung im BDSG, 2022.

Zumindest in solchen Fällen stellt sich die Frage, in welchem Umfang die Berücksichtigung konkreter spezialgesetzlicher Anforderungen entweder in den Prozess der Zertifizierung oder sogar in die zu zertifizierenden Prozesse des Verantwortlichen oder Auftragsverarbeiters verlagert werden kann. Letzteres könnte darauf hinauslaufen, im Zertifizierungsprozess nicht die Einhaltung von ohnehin rasch veränderlichen spezialgesetzlichen Regelungen zu prüfen und zu bestätigen, sondern die Existenz eines wirksamen organisatorischen Prozesses beim Verantwortlichen oder Auftragsverarbeiter, mit dessen Hilfe die jeweils für einen spezifischen Verarbeitungsvorgang geltenden spezialgesetzlichen Regelungen geprüft, operationalisiert und eingehalten werden.[33] Der DSGVO lässt sich nichts dazu entnehmen, ob ein solches Modell zulässig ist und welche Anforderungen an dieses zu stellen sein könnten; eine Stellungnahme jedenfalls der deutschen Aufsichtsbehörden und des EDSA zu dieser Frage fehlt. Zumindest in stark volatilen spezialgesetzlichen Regelungsbereichen dürfte ein solcher oder ähnlicher Weg aber alternativlos sein, wenn man nicht auf die Prüfung der entsprechenden speziellen Anforderungen verzichten möchte.

4.2 Umgang mit ungeklärten Rechtsfragen

Eine zweite grundsätzliche Herausforderung der datenschutzrechtlichen Zertifizierung ist der vielfach generische Charakter insbesondere der materiellrechtlichen Vorgaben der DSGVO.[34] Dieser führt gemeinsam mit dem immer noch jungen Alter der Verordnung dazu, dass viele konkrete Anforderungen an unterschiedliche Verarbeitungsvorgänge unklar und umstritten sind. Der erforderliche Prozess der Konkretisierung umfasst ein komplexes Geflecht von Akteuren.[35] Von diesen kann nur der EuGH Vorgaben machen, die für alle anderen Beteiligten verbindlich sind. Schon aufgrund der begrenzten Kapazität des Gerichtshofs, aber auch aufgrund seiner spezifischen, einzelfallorientierten Arbeitsweise wird es aber auch mittel- und langfristig unmöglich sein, sich ausschließlich an seiner Rechtsprechung zu orientieren. Dies führt dazu, dass die an einem Zertifizierungsprozess Beteiligten (Verantwortliche und Auftragsverarbeiter, Zerti-

33 Diesen Ansatz verfolgt der GDPR-CARPA-Kriterienkatalog aus Luxemburg: *Helmke/Link/Schild*, DuD 2023, 100, 101; zur dynamischen Zertifizierung vgl. *Hofmann*, Dynamische Zertifizierung, 2019.

34 Näher *Hornung/Spiecker gen. Döhmann*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Einl. Rn. 211.

35 Ebd. Rn. 234, 180 ff., 264 ff.

fizierungsstellen, Programmeigner, Aufsichtsbehörden, ggf. Europäischer Datenschutzausschuss) einen Weg finden müssen, um mit ungelösten und umstrittenen Rechtsfragen umzugehen.

Verdeutlichung: Drittlandsübermittlung als Problem der globalen Data Governance

Die Notwendigkeit der Konkretisierung ist ein allgemeines Governance-Problem der DSGVO, das sich – in Verbindung mit der Zertifizierung – an etlichen Beispielen verdeutlichen lässt. Im Folgenden wird zu diesem Zweck der vielfach diskutierte Bereich der Übermittlung personenbezogener Daten in Drittländer gewählt. Die Frage der Konkretisierung der in der Praxis oft unklaren Übermittlungsgrundlagen wird in diesem Zusammenhang zu einer Frage der globalen Data Governance.

Die DSGVO hat die früheren Bestimmungen der DSRL zur Übermittlung in Drittländer in vielen Details verändert und neue Schutzinstrumente eingeführt. Dabei wurden insbesondere die Kriterien für derartige Übermittlungen konkretisiert und etliche Anforderungen aus der Rechtsprechung des EuGH zu Art. 25 f. DSRL in den Normtext übernommen. Der Grundansatz ist indes unverändert:[36] Die Harmonisierung der datenschutzrechtlichen Vorschriften im Binnenmarkt führt zum grundsätzlichen Wegfall von Beschränkungen der Datenflüsse zwischen den Mitgliedstaaten; dieser Wegfall kann aber nur gerechtfertigt werden, wenn bei Übermittlungen aus dem Binnenmarkt[37] in andere Jurisdiktionen harmonisierte Anforderungen gelten, die ein Absenken des Schutzes ausschließen oder zumindest auf ein erträgliches Maß beschränken. Dass damit durchaus erhebliche Einschränkungen globaler Datenflüsse einhergehen können, kann für Datenverarbeiter Probleme verursachen, die – wegen bestehender Verarbeitungsprozesse und globaler Abhängigkeiten – schwierig für sie zu lösen sind. Diesen Umstand nimmt der europäische Gesetzgeber jedoch in gewissem Umfang hin.

36 *Schantz,* in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Art. 44 DSGVO Rn. 4 ff. zu den Herausforderungen nach dem Brexit: *Hofmann/Stach*, ZD 2021, 1 ff.; *Wittershagen*, The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit, 2023.

37 Dies schließt EWR-Staaten ein, die aufgrund des Beschlusses des EWR-Ausschusses Nr. 154/2018 v. 6.7.2018 (Abl. L 183, 19.7.2018, S. 23–26) nicht als Drittländer iSd. Art. 44 DSGVO gelten.

Die für Datenexporteure und -importeure einfachste Variante ist die Übermittlung in Drittländer, für die die Europäische Kommission einen Angemessenheitsbeschluss nach Art. 45 DSGVO getroffen hat.[38] Allerdings hat der EuGH in den zwei wegweisenden Entscheidungen Safe Harbor[39] und Privacy Shield[40] hohe Anforderungen an die Bejahung eines angemessenen Datenschutzniveaus gestellt und die jeweiligen Kommissionsbeschlüsse für ungültig erklärt.[41] Mit der Executive Order 14086 von US-Präsident Biden[42] und dem darauf gestützten erneuten Angemessenheitsbeschluss der Kommission[43] ist das Problem zwar für die USA – jedenfalls bis zu einer zu erwartenden weiteren gerichtlichen Prüfung auch dieses Beschlusses – gelöst . Die Diskussionen in Wissenschaft und Praxis seit der Privacy-Shield-Entscheidung und die erheblichen Probleme, die der Wegfall des Angemessenheitsbeschlusses für Datenverarbeiter verursacht hat, die Geschäftsmodelle mit transatlantischen Datenübermittlungen auf ihn gestützt haben,[44] sind aber weiterhin relevant. Dies betrifft zum einen das Szenario einer Ungültigkeitserklärung des Privacy Frameworks durch den EuGH,[45] zum anderen aber auch Datenübermittlungen in Drittstaaten, für die kein Angemessenheitsbeschluss vorliegt.

38 Dies gilt aktuell für Korea, Andorra, Argentinien, Kanada, Färöer, Guernsey, Israel, Isle of Man, Japan, Jersey, Neuseeland, Schweiz, Uruguay und das Vereinigte Königreich.

39 EuGH, Urt. v. 6.10.2015 – C-362/14 (Schrems/Digital Rights Ireland – Schrems I), NJW 2015, 3151.

40 EuGH, Urt. v. 16.7.2020 – C-311/18 (Facebook Ireland/Schrems – Schrems II), NJW 2020, 2613.

41 Der EuGH bemängelte die extensiven Zugriffsrechte der US-Geheimdienste nach der Übertragung (vgl. insb. Sec. 702 FISA) sowie die mangelhaften Rechtschutzmöglichkeiten gegen Zugriffe. Beide Beschlüsse wurden deshalb wegen Unvereinbarkeit mit Art. 7, 8 und 47 GRCh für ungültig erklärt, vgl. EuGH NJW 2015, 3151 Rn. 94 ff.; EuGH, NJW 2020 2613 Rn.198 f. Näher *Vladeck*, DSK-Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse.

42 POTUS, Executive Order 14086.

43 EU-KOM, Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework.

44 *Dehmel/Ossman-Magiera/Weiss*, MMR 2023, 17 ff.

45 Das EU-Parlament hat eine Beschlussvorlage des LIBE-Ausschusses angenommen, in dem es seine Zweifel am Angemessenheitsbeschluss aufführt und die EU-KOM zu Änderungen aufruft: Resolution 2023/2501(RSP); EDSA fordert EU-KOM zur genauen Prüfung der EO auf: Opinion 5/2023; die EO als unzureichend betrachtend: LfDI BW, interne Einschätzung v. 22.10.2022; differenzierend: HmbBfDI, Datenschutz in den USA v. 29.11.2022.

In beiden Szenarien werden weiterhin die Anforderungen zum Tragen kommen, die der EuGH und in der Folge auch der EDSA für Datenübermittlungen mit Hilfe von geeigneten Garantien im Sinne des Art. 46 DSGVO formuliert haben. Für Standarddatenschutzklauseln (SCCs, Art. 46 Abs. 2 lit. c DSGVO) hat der EuGH die grundsätzliche Vereinbarkeit mit Art. 7, 8 und 47 der GRCh bestätigt. Voraussetzung ist jedoch, dass im Rahmen der SCCs durch individuelle Verpflichtungen der Datenimporteure und Datenexporteure ein Schutzniveau sichergestellt wird, das dem europäischen Grundrechtsschutz gleichwertig ist. Dies müssen die Datenexporteure vor einer Übermittlung überprüfen, während die Datenimporteure, zumindest im Rahmen der SCCs, den Exporteur benachrichtigen müssen, falls sie nicht (mehr) in der Lage sind, ein gleichwertiges Schutzniveau zu garantieren. Fehlt es von Anfang an oder nachträglich an einer Gleichwertigkeit, sind die Datenexporteure verpflichtet, die Übermittlung auszusetzen, wenn sie nicht durch anderweitige Maßnahmen ein gleichwertiges Schutzniveau (wieder)herstellen können. Dementsprechend gewährleisten die SCCs, in rechtmäßiger und konsequenter Anwendung, ein gleichwertiges und damit den Anforderungen des Art. 44 Abs. 1 DSGVO entsprechendes Schutzniveau.[46]

Die Überprüfungsverpflichtung der Datenexporteure wird in der Praxis durch sogenannte Transfer-Impact-Assessments (TIAs) umgesetzt.[47] Der EDSA hat diese Verpflichtung folgerichtig auch auf andere Übermittlungsinstrumente des Art. 46 DSGVO erweitert. [48] Ergibt die Beurteilung im Zuge eines TIA (oder einer gleichwertigen Überprüfung), dass kein gleichwertiges Schutzniveau besteht, benennt der EDSA als anderweitige Maßnahmen eine Vielzahl an vertraglichen, technischen oder organisatorischen Instrumenten, von denen die Anonymisierung, bzw. eine dieser gleichstehende Verschlüsselung, regelmäßig unverzichtbar sein wird.[49]

Für die Zertifizierung bedeutet dies, dass für alle Drittländer, in die ein Verantwortlicher oder Auftragsverarbeiter Daten übermitteln möchte,

46 Zur Rechtmäßigkeit der SCCs und den Anforderungen an die Datenexporteure: EuGH, NJW 2020, 2613, Rn. 134 ff.

47 *Baumgartner/Hansch/Roth*, ZD 2021, 608, 609.

48 EDSA, Empfehlungen 01/2020, Rn. 15 ff., vgl. zudem die Anforderung zur Überprüfung der tatsächlichen Möglichkeit der Gewährleistung eines gleichwertigen Schutzniveaus iRd. Empfehlungen zu den folgenden Übermittlungsinstrumenten: BCRs: EDSA, Recommendations 1/2022, Rn. 39; CoCs: EDSA, Leitlinien 4/2021, Rn. 36. Zertifizierungen: EDSA, Guidelines 07/2022, Rn. 45.

49 EDSA, Empfehlungen 01/2020, Rn. 79 ff., insb. Rn. 85 ff.

die datenschutzrechtliche Rechtslage, die Möglichkeiten und Grenzen der gewählten Übermittlungsinstrumente sowie gegebenenfalls zusätzlich erforderliche (vor allem technische) Maßnahmen zur Gewährleistung eines angemessenen Schutzniveaus eine Rolle spielen müssen.

Zwei Varianten der Zertifizierung: Datenexporteur oder Datenimporteur

Die Zertifizierung kann nach der DSGVO im Rahmen der Drittlandsübermittlung in zwei Konstellationen eine Rolle spielen. Zum einen besteht die Möglichkeit, die Art. 44 ff. DSGVO in die Zertifizierung von Verarbeitungsvorgängen eines Datenexporteurs in der Union einzubeziehen. Soll eine Übermittlung in ein Drittland erfolgen, für das kein Angemessenheitsbeschluss vorliegt, so muss im Rahmen der Zertifizierung das Vorliegen einer geeigneten Garantie nach Art. 46 Abs. 2 DSGVO geprüft werden.

Zum anderen hat der europäische Gesetzgeber im Zuge der Regelung der Datenschutzzertifizierung in der DSGVO diese auch selbst als geeignete Garantie aufgenommen (Art. 42 Abs. 2 und Art. 46 Abs. 2 lit. f DSGVO). Diese adressiert Fälle, in denen sich der Datenimporteur im Drittland einer Zertifizierung nach Art. 42 DSGVO unterzieht, um durch die Einhaltung der jeweiligen Zertifizierungskriterien die Gewährleistung eines gleichwertigen Schutzniveaus sicherzustellen.[50] Der Gesetzgeber hat zugleich die Governance-Herausforderung realisiert, dass die Einhaltung der Vorgaben eines Kriterienkatalogs in Drittländern schwerer kontrollierbar ist und außerdem im Falle von Verstößen entsprechende Sanktionen deutlich schlechter durchsetzbar sein werden.

Der Gesetzgeber versucht, dieses Durchsetzungsproblem durch die Vorgabe in Art. 42 Abs. 2 und Art. 46 Abs. 2 lit. f DSGVO zu adressieren, dass die Verantwortlichen oder Auftragsverarbeiter mittels vertraglicher oder sonstiger rechtlich bindender Instrumente die verbindliche und durchsetzbare Verpflichtung eingehen müssen, die geeigneten Garantien anzuwenden; dies bezieht sich insbesondere auf die Rechte der betroffenen Personen. Eine solche Verpflichtung ändert zwar nichts daran, dass die rechtlichen Befugnisse und praktischen Möglichkeiten der Aufsichtsbehörden als staatliche Letztverantwortliche im System der regulierten Selbstregulierung der Zertifizierung in diesem Bereich erheblich schwächer ausgeprägt sind als innerhalb des Binnenmarktes. Dies ist allerdings ein Problem aller Garantien von Art. 46 Abs. 2 DSGVO, die auf Drittländer angewendet werden,

50 EDSA, Guidelines 07/2022.

welche weder allgemein noch im konkreten Verarbeitungssektor ein angemessenes Schutzniveau aufweisen.

Der EDSA hat sich mit dieser neuen Variante bereits befasst. Er betont, dass die allgemeinen Leitlinien für die Zertifizierung auch für ihre Nutzung als Übermittlungsinstrument gelten.[51] Wie bei den anderen geeigneten Garantien sind außerdem auch im Rahmen der Art. 42 Abs. 2 und Art. 46 Abs. 2 lit. f DSGVO die zusätzlichen Maßnahmen zur Gewährleistung eines gleichwertigen Schutzniveaus zu beachten.[52]

Die Empfehlungen des EDSA zielen darauf ab, die in der Folge der Schrems II-Entscheidung konkretisierten Anforderungen (s.o. 4.2.1) auch im Rahmen von Datenübermittlungen anzuwenden, die auf genehmigte Zertifizierungsmechanismen gestützt werden sollen. Der EDSA verlangt deshalb u.a. die Durchführung eines TIA sowohl auf Seiten des Datenimporteurs im Drittland, wenn dieser sich zertifizieren lassen will,[53] als auch auf Seiten des Datenexporteurs in der Union, wenn er sich auf dieses Instrument stützen möchte; Letzterer kann allerdings die Bestätigung der Zertifizierungsstelle, dass der Importeur das TIA ordnungsgemäß durchgeführt hat, als „important element" für seine eigene Bewertung verwenden.[54] Wenn der konkrete Zertifizierungsmechanismus keinen effektiven Schutz gewährleisten kann, so sind (wie bei Standarddatenschutzklauseln und anderen Übermittlungsinstrumenten) ergänzende Maßnahmen zu ergreifen.

Folgen für Zertifizierungsverfahren und Kriterienkatalog

Im Ergebnis bietet die Datenschutzzertifizierung damit ein umfassendes Instrument zur Übermittlung in Drittländer ohne angemessenes Datenschutzniveau, wenn sich:

1. der Datenexporteur einer Zertifizierung unterzieht, in der er die Einhaltung des Kapitel V (einschließlich der Vornahme eines TIA bzw. einer Gleichwertigkeitsüberprüfung) nachweist, oder

51 Ebd. Rn. 37. Dies bezieht sich auf EDSA, Leitlinien 1/2018.

52 EDSA, Empfehlungen 01/2020.

53 Dies hat der Datenimporteur als allgemeine Anforderung an die Nutzung einer geeigneten Garantie ohnehin vorzunehmen: EDSA, Empfehlungen 01/2020, Rn. 28, vgl. zudem EDSA, Guidelines 07/2022, Rn. 45.

54 S. EDSA, Guidelines 07/2022, Rn. 21. In der ersten Fassung der Guidelines sollte der Exporteuer nicht auf die Bewertung der Zertifizierungsstelle, sondern auf die des Importeurs vertrauen dürfen. Außerdem ist die Qualifizierung „important" hinzugetreten; dies dürfte die Bewertungspraxis des Exporteurs erleichtern.

2. der Datenimporteur einer Zertifizierung unterzieht und damit die Einhaltung der Art. 42 Abs. 2 und 46 Abs. 2 lit. f DSGVO nachweist, sowie beide Parteien eine Gleichwertigkeitsüberprüfung vornehmen.

Der EDSA handelt konsequent, wenn er seine Konkretisierung der materiellrechtlichen Vorgaben aus Art. 46 Abs. 2 DSGVO für alle Übermittlungsinstrumente anwendet. Aus der Perspektive des Programmeigners ist damit allerdings noch nicht geklärt, auf welcher Stufe des Prozesses diese Konkretisierung „eingebaut" oder (falls die Konkretisierungsleistung des Ausschusses als ganz oder teilweise nicht überzeugend bewertet wird) modifiziert werden kann oder muss. Zu dieser Frage haben sich die Aufsichtsbehörden bisher nicht geäußert.

Eine Möglichkeit dürfte darin bestehen, im Kriterienkatalog mehr oder weniger den Inhalt der Art. 44 ff. DSGVO auf abstrakter Ebene zu wiederholen und die Prüfung der Anforderungen an das konkrete Übermittlungsinstrument auf die Zertifizierungsstellen zu übertragen. Es bliebe sodann in Zertifizierungsstellen überlassen, im Einzelfall Art. 46 Abs. 2 DSGVO anzuwenden und bei der insoweit erforderlichen konkretisierenden Auslegung den Empfehlungen des EDSA ganz, teilweise oder gar nicht zu folgen. Eine Abweichung dürfte allerdings den Einsatz aufsichtsbehördlicher Maßnahmen gegen die akkreditierte Zertifizierungsstelle nach sich ziehen (Art. 43 Abs. 7 DSGVO), die zum Widerruf der Zertifizierung führen können (Art. 42 Abs. 7 DSGVO). Gegen derartige Maßnahmen könnten sich sodann die Zertifizierungsstelle und der Verantwortliche bzw. der Auftragsverarbeiter gerichtlich zur Wehr setzen. Diese Möglichkeit der gerichtlichen Kontrolle der Maßstäbe, die der EDSA für den Einsatz der Zertifizierung zur Drittlandsübermittlung formuliert hat, ist vor allem deshalb bedeutsam, da die Leitlinien, Empfehlungen und Beschlüsse des Ausschusses grundsätzlich nicht direkt angegriffen werden können.[55]

Die zweite Möglichkeit liegt darin, dass ein Programmeigner in einem Kriterienkatalog demgegenüber eine selbstständige Konkretisierung der Art. 44 ff. DSGVO vornimmt. Für diese Variante stellen sich wiederum neue, bislang nicht diskutierte Fragen.

55 So jedenfalls EuG, T-709/21 v. 7.12.2022 (WhatsApp v. EDSA) Rn. 50 ff., a.A. *Hermann/Miller*, ZeuS 2021, 617-662. Die Rechtswegmöglichkeiten werden hier aus systematischer Perspektive aufgezeigt. Es soll nicht bewertet werden, ob die EDSA-Vorgaben rechtskonform sind.

Naheliegend dürfte es sein, im ersten Schritt die Anforderungen des EuGH und des EDSA für den Kriterienkatalog zu übernehmen. Für Übermittlungen in die USA folgt daraus allerdings das Problem, dass der neue Angemessenheitsbeschluss der Kommission nach Ansicht vieler Kritiker die Vorgaben des Gerichtshofs gerade nicht einhält.[56] Es würde jedoch zu weit gehen und die in der DSGVO normierte Rolle der Zertifizierungsstelle überschreiten, wenn man von ihr verlangen würde, im Rahmen der Zertifizierung einen existierenden Angemessenheitsbeschluss am Maßstab der gerichtlichen Entscheidungen auf seine Gültigkeit hin zu überprüfen und im Falle eines negativen Ergebnisses von dem Verantwortlichen oder Auftragsverarbeiter zu fordern, eine andere Rechtsgrundlage für die Übermittlung zu wählen. Eine Ausnahme dürfte allenfalls für evidente Fälle denkbar sein.

In einem zweiten Schritt könnten für die Nutzung von Art. 46 Abs. 2 DSGVO die Vorgaben des EDSA zu TIAs und ergänzenden vertraglichen, technischen oder organisatorischen Maßnahmen in einen Kriterienkatalog aufgenommen werden. Vergleichbar ihrer Berücksichtigung (erst) in der konkreten Zertifizierung stellt sich auch hier die Frage von Abweichungen. Nimmt ein Programmeigner Modifizierungen vor, so steht zu erwarten, dass ein entsprechender Kriterienkatalog von der zuständigen Aufsichtsbehörde oder vom EDSA nicht genehmigt wird. Eine entsprechende Ablehnung könnte sodann gerichtlich angegriffen werden. Im Rahmen eines solchen Prozesses (der bisher noch nicht vorgekommen ist) würden damit auch die Konkretisierungsleistungen des Ausschusses für Art. 46 DSGVO geprüft.

Eine letzte, restriktive Möglichkeit des Umgangs mit Drittlandsübermittlungen im Rahmen eines Kriterienkatalogs bestünde in ihrem Ausschluss. Da die nach Art. 42 Abs. 1 DSGVO zu bestätigende Einhaltung der Verordnung auch gegeben ist, wenn in einem Kriterienkatalog engere oder zusätzliche Anforderungen formuliert werden, ist es zulässig, im Rahmen von Zertifizierungsprogrammen freiwillig über das Niveau der DSGVO hinausgehende Anforderungen zu erfüllen.[57] Es wäre deshalb möglich, Verantwortlichen und Auftragsverarbeitern im Rahmen einer Zertifizierung

56 Die Gründe können nicht vertieft werden, insoweit Fn. 45 sowie *Roßnagel*, ZD 2022, 305 ff.

57 Für die Zulässigkeit der Integration strengerer Anforderungen: *Hornung*, in: Auernhammer, DSGVO/BDSG, 7. Aufl. 2020, Art. 42 DSGVO Rn. 48; *Scholz*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, 2019, Art. 42 DSGVO Rn. 26; a.A. *Will*, in: Ehmann/Selmayr, DSGVO, 2. Auflage 2018, Art. 42 Rn. 33.

zu bestätigen, dass sie auf eine Datenübermittlung in alle Länder außerhalb der EU oder beispielsweise in Länder mit (gegebenenfalls: trotz Angemessenheitsbeschlusses) zweifelhaftem Datenschutzniveau verzichten. Ob für eine solche Zertifizierung eine Nachfrage besteht oder die Verantwortlichen und Auftragsverarbeiter auf andere Zertifizierungsverfahren ausweichen, ist eine offene Frage. Es erscheint aber zumindest nicht ausgeschlossen, dass Dienstleister sich in dieser Weise zertifizieren lassen, um gegenüber potentiellen Auftraggebern demonstrieren zu können, dass die derzeitige unsichere Rechtslage und das Damoklesschwert einer Entscheidung des EuGH zum Data Privacy Framework sie nicht tangiert.

5. Fazit und Ausblick

Die Genehmigung der ersten Kriterienkataloge für DSGVO-Zertifizierungen verspricht spannende Zeiten: Sowohl interessierte Verantwortliche und Auftragsverarbeiter als auch betroffene Personen und Aufsichtsbehörden werden mit großem Interesse auf die beginnende Praxis der Zertifizierung blicken. Dies betrifft vor allem die Prüftiefe bei der Anwendung der Kriterien, aber auch den Umgang mit noch offenen Fragen des Zertifizierungsprozesses.

Die Untersuchung hat gezeigt, dass eine wirksame Zertifizierung zumindest im Grundsatz die Zertifizierbarkeit bereichsspezifischer Anforderungen an die Datenverarbeitung voraussetzt. Bisher haben sich aber noch keine Maßstäbe dafür herausgebildet, auf welcher Ebene und durch welche Akteure die Anwendung bereichsspezifischer Normen erfolgen soll.

Der unbestimmte Charakter vieler Normen der DSGVO ist eines ihrer allgemeinen Governance-Probleme. Dieses muss im Rahmen der Zertifizierung in spezifischer Weise adressiert werden. Programmeigner und Zertifizierungsstellen stehen dabei vor der Herausforderung, die Konkretisierungen der Rechtsprechung und des EDSA zu übernehmen und zu rationalisieren, oder aber sie (um den Preis von Rechtsstreitigkeiten) zu hinterfragen. Das Beispiel der Datenübermittlungen in Drittländer zeigt, dass dies für die Praxis der Datenschutzzertifizierung keine kleine Herausforderung sein wird. Angesichts des neuen Angemessenheitsbeschlusses der Kommission steht zu erwarten, dass die Zertifizierung im transatlantischen Verhältnis jedenfalls bis zu einer gerichtlichen Kontrolle durch das Data Privacy Framework überlagert werden wird. Dies mindert ihre grundsätzliche Rolle insbesondere für andere Weltregionen jedoch nicht.

Trotz dieser und weiterer Herausforderungen zeigt sich im Gesamtbild, dass die Datenschutzzertifizierung erhebliche Potenziale hat, um in Zukunft als Instrument einer effektiven und grundrechtsorientierten Data Governance zu dienen. Die Zertifizierung kann nicht alle offenen Fragen der DSGVO adressieren oder gar alle Durchsetzungsdefizite des Datenschutzrechts beheben. Sie könnte aber einen wesentlichen Baustein des Instrumentenkastens der Zukunft bilden. Dies gilt sowohl innerhalb der EU als auch – gerade wegen der Möglichkeit einer Zertifizierung von Verantwortlichen und Auftragsverarbeitern außerhalb der Union – mit Blick auf globale Datenflüsse und die Herausbildung weltweiter Regeln.

Literatur

Baumgartner, Ulrich; Hansch, Guido; Roth, Heiko (2021): Die neuen Standardvertragsklauseln der EU-Kommission für Datenübermittlungen in Drittstaaten. *Zeitschrift für Datenschutz (ZD)*, S. 608-613.

Bäumler, Helmut (2004): Ein Gütesiegel auf den Datenschutz. Made in Schleswig-Holstein. *Datenschutz und Datensicherheit (DuD)*, S. 80-84.

Bäumler, Helmut; Mutius, Albert von (1999): *Datenschutzgesetze der dritten Generation.* Köln: Luchterhand.

–– (2002): *Datenschutz als Wettbewerbsvorteil.* Wiesbaden: Vieweg.

Bundesamt für Sicherheit in der Informationstechnik (BSI); Verfahrensbeschreibung zur Erteilung von IT-Sicherheitskennzeichen. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT-Sicherheitskennzeichen/Verfahrensbeschreibung.pdf?__blob=publicationFile&v=3 (besucht am 01.08.2023).

Comission Nationale pour la Protection des Données (CNPD) (08.06.2022): Die CNPD nimmt das Zertifizierungsverfahren «GDPR-CARPA» an. URL: https://cnpd.public.lu/de/actualites/national/2022/06/adpoption-gdpr-carpa.html (besucht am 01.08.2023).

Comission Nationale pour la Protection des Données (CNPD) (13.05.2022): Décision N° 15/2022 du 13 mai 2022 de la Commission nationale pour la protection des données portant exécution de l'article 15 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données. URL: https://cnpd.public.lu/dam-assets/fr/professionnels/certification/decision-n-15-2022-du-13-mai-2022-criteres-de-certification.pdf (besucht am 01.08.2023).

Comission Nationale pour la Protection des Données (CNPD) (14.10.2022): Die CNPD ist die erste Datenschutzbehörde in Europa, die einer DSGVO Zertifizierungsstelle eine Akkreditierung erteilt hat. URL: https://cnpd.public.lu/de/actualites/national/2022/10/premier-agrement-certification.html (besucht am 01.08.2023)

Datenschutzkonferenz (DSK) (2021): Anforderungen an datenschutzrechtliche Zertifizierungsprogramme, Version 1.8, v. 16.04.2021. URL: https://www.datenschutzkonferenz-online.de/media/ah/DSK_Anwendungshinweis_Zertifizierungskriterien.pdf (besucht am 01.08.2023).

Dehmel, Susanne; Osmann-Magiera, Ludmilla Lea; Weiß, Rebekka (2023): Drittstaatentransfers nach Schrems II. *Zeitschrift für IT-Recht und Recht der Digitalisierung (MMR)*, S. 17-22.

Drews, Hans-Ludwig; Kranz, Hans Jürgen (2000): Datenschutzaudit – Anmerkungen zum Rechtsgutachten von Alexander Roßnagel vom Mai 1999. *Datenschutz und Datensicherheit (DuD)*, S. 226-230.

Duisberg, Alexander (2018): Zertifizierung und der Mittelstand – Quo Vadis?. *Zeitschrift für Datenschutz (ZD)*, S. 53-54.

Ehmann, Eugen; Selmayr, Martin (Hrsg.) (2018): *DSGVO-Kommentar*, 2. Auflage. München: C.H. Beck.

Europäischer Datenschutzsauschuss (EDSA) (04.06.2019): Leitlinien 1/2018 für die Zertifizierung und Ermittlung von Zertifizierungskriterien nach den Artikeln 42 und 43 der Verordnung (EU) 2016/679.

–– (18.06.2021): Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten.

–– (22.02.2022): Leitlinien 4/2021 über Verhaltensregeln als Instrument für Übermittlungen.

–– (20.06.2023): Recommendations 1/2022 on the application for approval and on the elements and principles to be found in Controller Binding Corporate Rules (Art. 47 GDPR).

–– (14.02.2023): Guidelines 07/2022 on certification as a tool for transfers. Version 2.0.

–– (14.02.2023) Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Protection Seals.

–– (28.02.2023) Opinion 5/2023 on the EU- Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework.

EU-Kommission (10.01.2017): Proposal for a Regulation of the European Parliament and the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 Final. URL: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52017PC0010 (besucht am 01.08.2023)

EU-Parlament (20.07.2017): Report on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), A8-0324/2017. URL: https://www.europarl.europa.eu/doceo/document/A-8-2017-0324_EN.html (besucht am 01.08.2023)

–– (11.05.2023): Adequacy of the protection afforded by the EU-U.S. Data Privacy Framework European Parliament resolution of 11 May 2023 on the adequacy of the protection afforded by the EU-US Data Privacy Framework (2023/2501(RSP)). URL: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.pdf (besucht am 01.08.2023).

–– (10.07.2023): Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework C(2023) 4745 final. URL: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf (besucht am 01.08.2023)

Eßer, Martin; Kramer, Philipp; v. Lewinski, Kai (Hrsg.) (2020): *Auernhammer – DSGVO/BDSG Kommentar*, 7. Auflage. Köln: Carl Heymanns.

EWR-Ausschuss (06.07.2018): Beschluss des gemeinsamen EWR-Ausschusses zur Änderung des Anhangs XI (Elektronische Kommunikation, audiovisuelle Dienste und Informationsgesellschaft) und des Protokolls 37 (mit der Liste gemäß Artikel 101) des EWR-Abkommens [2018/1022], OJ L 183, 19.7.2018, p. 23–26.

Hamburgischer Beauftragter für Datenschutz und die Informationsfreiheit (LfDI HH) (29.11.2022): Datenschutz in den USA – aktuelle Lage. URL: https://datenschutz-hamburg.de/pages/executiveorder/ (besucht am 01.08.2023).

Hermann, Christoph; Miller, A. Simon (2021): Direktklagemöglichkeiten gegen Beschlüsse des EDSA. *Zeitschrift für Europarechtliche Studien (ZeuS)*, S. 617-662.

Hofmann, Johanna (2019): *Dynamische Zertifizierung – Datenschutzrechtliche Zertifizierung nach der DSGVO am Beispiel des Cloud Computing?* Baden-Baden: Nomos.

Hofmann, Johanna; Stach, Benjamin (2021): Soft Brexit – die Ruhe vor dem Sturm? Was müssen Unternehmen ab 2021 beachten? *Zeitschrift für Datenschutz (ZD)*, S. 3 – 8.

Hornung, Gerrit (2021): Das IT-Sicherheitsgesetz 2.0: Kompetenzaufwuchs des BSI und neue Pflichten für Unternehmen. *Neue Juristische Wochenschrift (NJW)*, S. 1985-1991.

–– (2022): Trainingsdaten und die Rechte von betroffenen Personen – in der DSGVO und darüber hinaus? In: Rostalski, Frauke (Hrsg.): *Künstliche Intelligenz. Wie gelingt eine vertrauenswürdige Verwendung in Deutschland und Europa?* Tübingen: Mohr Siebeck, S. 91-120.

Johannes, Paul Christoph (2020): Zertifizierung von Datenverarbeitungsvorgängen bei der Polizei. *Die Polizei*, S. 409-415.

Kowalski, Bernd; Intemann, Matthias (2018): Perspektiven der IT-Sicherheits-Zertifizierung für Europas Märkte. *Datenschutz und Datensicherheit (DuD)*, S. 415-419.

Königshofen, Thomas (2000): Chancen und Risiken eines gesetzlich geregelt Datenschutzaudits. Der Versuch einer Versachlichung der Diskussion. *Datenschutz und Datensicherheit (DuD)*, S. 357-360.

Krcmar, Helmut; Eckert, Claudia; Roßnagel, Alexander; Sunyaev, Ali; Wiesche, Manuel (2018): *Management sicherer Cloud-Services – Entwicklung und Evaluation dynamischer Zertifikate*. Wiesbaden: Springer Fachmedien.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI BW) (22.10.2022): Interne Einschätzung des LfDI Baden-Württemberg zur Frage, ob die Executive Order des US-Präsidenten der erhoffte Befreiungsschlag in Sachen internationaler Datentransfers darstellt. URL: https://fragdenstaat.de/anfrage/einschaetzung-zum-eu-u-s-data-privacy-framework/746772/anhang/executiveorder-lfdi-bawu.pdf (besucht am 01.08.2023).

Martini, Mario; Kühling, Jürgen; Heberlein, Johanna; Kühl, Benjamin; Nink, David; Quirin, Weinzierl; Wenzel, Michael (2016): *Die Datenschutz-Grundverordnung und das nationale Recht*. Münster: Monsenstein und Vannerdat.

Mirtsch, Mona (2019): Kapitel 9: Konformitätsbewertung im Bereich Cybersicherheit. In: Mangelsdorf, Axel and Weiler, Petra (Hrsg.): *Normen und Standards für die digitale Transformation: Werkzeuge, Praxisbeispiele und Entscheidungshilfen für innovative Unternehmen, Normungsorganisationen und politische Entscheidungsträger*. Berlin, Boston: De Gruyter Oldenbourg, S. 141-164.

Müller, Johannes (2022): AUDITOR: Zwischenstand im Forschungsprojekt „European Cloud Service Data Protection Certification". *Zeitschrift für Datenschutz-Aktuell (ZD-Aktuell)*, 2022, 01239.

Paal, Boris P.; Pauly, Daniel A. (Hrsg.) (2021), *DS-GVO BDSG – Kompakt Kommentar*, 3. Auflage, München: C.H. Beck.

President of the United States (7.10.2022): Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/ (besucht am 01.08.2023).

Rat der EU (10.02.2021): Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) – Mandate for negotiations with EP, 6087/21.

Richter, Frederik (2020): Zertifizierung unter der DS-GVO – Chance eines erleichterten internationalen Datenverkehrs darf nicht verpasst werden. *Zeitschrift für Datenschutz (ZD)*, S. 84-87.

Roßnagel, Alexander (2000): *Datenschutzaudit: Konzeption, Durchführung, gesetzliche Regelung*. Wiesbaden: Springer.

–– (2003): *Handbuch Datenschutzrecht*. München: C.H. Beck.

–– (2017): *Datenschutzaufsicht nach der EU-Datenschutz-Grundverordnung*. Wiesbaden: Springer.

–– (2022): Was folgt auf das Privacy Shield? Ein Privacy Framework oder Schrems III? *Zeitschrift für Datenschutz (ZD)*, S. 305-306.

–– (2023): Videokonferenzen als Telekommunikationsdienste. *Neue Juristische Wochenschrift (NJW)*, S. 400-405.

Schallbruch, Martin (2021): Das IT-Sicherheitsgesetz 2.0 – neue Regeln für Unternehmen und IT-Produkte. *Computer und Recht (CR)*, S. 450-458.

Schellhas-Mende, Friederike; Wiedemann, Nils; Blum, Nicolas (2022): Videokonferenzsysteme als Telekommunikationsdienst. *Datenschutz und Datensicherheit (DuD)*, S. 291-295.

Simitis, Spiros; Hornung, Gerrit; Spiecker gen. Döhmann, Indra (Hrsg.) (2019): *Kommentar Datenschutzrecht (DSGVO mit BDSG)*. Baden-Baden: Nomos.

Unabhängiges Landeszentrum für Datenschutz, Register der verliehenen Datenschutzsiegel, URL: https://www.datenschutzzentrum.de/guetesiegel/register/ / (besucht am 01.08.2023).

Vladeck, Stephen I. (15.11.2021): Datenschutzkonferenz (DSK) Gutachten zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse. URL: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_de.pdf (besucht am 01.08.2023).

Weiß, Martin (2022): *Öffnungsklauseln in der DSGVO und nationale Verwirklichung im BDSG*. Baden-Baden: Nomos.

Wittershagen, Leonie (2023): *The Transfer of Personal Data from the European Union to the United Kingdom post-Brexit*. Berlin, Boston: De Gruyter.

eIdentity im neuen Datenrecht: Das Zusammenspiel dezentraler rechtssicherer elektronischer Identifizierung und dem Recht auf Anonymität

Maxi Nebel und Paul C. Johannes

Zusammenfassung

Zentraler Bestandteil von eGovernment-Überlegungen ist die sichere Authentifizierung natürlicher Personen. Dies ergibt sich nicht nur aus einem Bedürfnis der Rechtssicherheit, sondern auch aus Praktikabilitätserwägungen. Die Europäische Kommission hat einen Vorschlag zur neuen Europäischen digitalen Identität (EUid) vorgelegt: Dabei handelt es sich um eine Art digitaler Brieftasche, in der die nationale elektronische Identität (eID) hinterlegt ist, aber auch Nachweise anderer persönlicher Attribute gespeichert werden können. Ziel soll es sein, dass Nutzende online auf Dienste zugreifen können, ohne private Identifizierungsmethoden verwenden oder unnötig personenbezogene Daten weitergeben zu müssen. Der Beitrag nimmt die Reform der eIDAS-VO zum Anlass, um diese vorzustellen, einen Überblick über den neuen Vertrauensdienst EUid zu geben und zu untersuchen, ob die Notwendigkeit der Identifizierung einer Person bei der Nutzung digitaler Dienste mit den Bedürfnissen nach Anonymität im Internet ausreichend ausgeglichen werden kann. Dabei wird auch auf das neue europäische Datenrecht eingegangen.

1. Einleitung: Identifizierung und Authentifizierung als zentrale Bausteine der Sicherheit digitaler Dienste

Digitale Geschäftsmodelle boomen und auch die öffentliche Verwaltung erweitert ihr Angebot für Online-Dienste stetig.[1] Grundlegende Vorausset-

1 Siehe z.B. Onlinezugangsgesetz (OZG), entsprechendes Änderungsgesetz „OZG 2.0", das Anfang 2023 auf den Weg gebracht wurde. Die Verwaltungsportale von Bund, Ländern und Kommunen sollen demzufolge interoperabel werden und Bürger und Unternehmen sollen eine digitale Identität bekommen, um Verwaltungsdienstleistungen online zu nutzen.

zung hierfür ist die sichere Authentifizierung der Nutzenden. Es geht dabei um Datensicherheit durch die Autorisierung der Nutzenden und die Authentizität der übermittelten Daten, aber auch um Vertrauen in rechtssichere digitale Dienste und Geschäfte. Dem steht das Recht auf Datenschutz und insbesondere das Bedürfnis nach Anonymität in einem schwer auflösbaren Widerspruch gegenüber. So müssen Anbieter von Social Networks beispielsweise Nutzenden nach § 19 Abs. 2 Telemedien-Teledienste-Datenschutzgesetz (TTDSG) die Möglichkeit bieten, die Plattform – wenn zumutbar – anonym zu nutzen, unterliegen andererseits nach § 3a Abs. 4 Nr. 2 NetzDG aber der Pflicht, strafbare Inhalte nebst Nutzername, IP-Adresse und ähnliches des erstellenden Nutzenden dem Bundeskriminalamt zu melden.[2]

Zentraler Bestandteil von eGovernment-Anwendungen muss dennoch die sichere Authentifizierung natürlicher Personen sein. Dies ergibt sich nicht nur aus einem Bedürfnis der Rechtssicherheit, um Rechtsgeschäfte und Verwaltungsvorgänge digital abzuwickeln, sondern auch aus Praktikabilitätserwägungen, um etwa Berechtigungen für System- und Dienstezugriffe nachzuweisen. Letzteres zeigt sich insbesondere durch die Nachfrage nach Single-Sign-On (SSO) und die Entwicklung von Modellen der Self-Sovereign Identity (SSI).[3] Insbesondere zentral gesteuerte Systeme bergen jedoch datenschutzrechtliche Risiken, etwa hinsichtlich der Nachverfolgbarkeit oder Profilbildung.[4]

2. eIDAS-VO: Europäisches Dateninfrastrukturrecht

Elektronische Transaktionen in Wirtschaft und Verwaltung benötigen Sicherungsmittel wie Signaturen und Zeitstempel, um Manipulationen

2 Möglicherweise schafft das das „Gesetz gegen digitale Gewalt" einen Ausweg aus diesem Widerspruch zu Gunsten des Betroffenen, zu dessen Vorbereitung das BMJ im April 2023 ein Eckpunktepapier vorgestellt hat. In diesem ist eine Accountsperre für den Fall wiederholter Rechteverletzung vorgesehen, die es ermöglichen würde, die Persönlichkeitsrechtsverletzung durch einen bestimmten Account eines Social Networks oder sonstigen Diensteanbieters zu verhindern. Eine Identifizierung des Accounterstellers, mögliche strafrechtliche Konsequenzen sowie die (dauerhafte) Sperrung der hinter dem Account stehenden Person werden dadurch jedoch nicht verbessert.

3 Dazu *Kudra/Seegebart/Schwalm*, DuD 2022, 9.

4 Hinweis zum Stand: Die Ausführungen beziehen sich auf die Rechtslage zum März 2023. Da das Verfahren noch nicht abgeschlossen ist, sind weitere Änderungen möglich.

zu verhindern, Formerfordernisse einzuhalten und Beweissicherheit zu gewährleisten. Um diese zusammenhängend zu regeln, hat die Union die eIDAS-VO erlassen.[5] Diese „Verordnung 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt" koordiniert zum einen die nationalen Systeme zur elektronischen Identifizierung und zum anderen die unionseinheitliche Regelung von Vertrauensdiensten. Ihr Ziel ist es unter anderem, einen einheitlichen europäischen Markt für elektronische Sicherungsmittel zu schaffen und hierdurch das Vertrauen in den elektronischen Rechtsverkehr in der EU zu stärken. Die eIDAS-VO sieht zu diesem Zweck Vorgaben zur Vereinfachung und Harmonisierung der Nutzung von elektronischen Signaturen und vergleichbaren Identifikationssystemen vor, die für alle EU-Mitgliedstaaten unmittelbar und verbindlich gelten. Neben allgemeinen Bestimmungen enthält die eIDAS-VO vor allem zwei voneinander getrennte inhaltliche Regelungskomplexe: Einen zur Koordination nationaler Systeme zur elektronischen Identifizierung[6] und einen zur unionseinheitlichen Regelung von Vertrauensdiensten.[7] Ein „Vertrauensdienst" ist nach Art. 3 Nr. 16 eIDAS-VO „ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und entweder der Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln und Diensten für die Zustellung elektronischer Einschreiben sowie von diese Dienste betreffenden Zertifikaten oder der Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung oder der Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten dient". Vertrauensdienste können einfach,[8] fortgeschritten oder qualifiziert sein. Die jeweiligen Anforderungen ergeben sich aus der eIDAS-VO, wobei die Einstufung aufeinander aufbaut.[9]

Die eIDAS-VO gilt seit 1. Juli 2016 unmittelbar in allen Mitgliedstaaten, bedarf also keiner zusätzlichen Umsetzungs- oder Anpassungsakte durch die Mitgliedstaaten. Verordnungen sind Teil der Rechtsordnungen der

5 Zu Entstehungsgeschichte und Entwurf *Roßnagel/Johannes*, ZD 2013, 65.
6 Dazu *Spindler/Rockenbauch*, MMR 2013, 139.
7 *Johannes*, in: Hentschel/Hornung/Jandt (Hrsg.), Mensch – Technik – Umwelt: Verantwortung für eine sozialverträgliche Zukunft, 2020, 587 (588).
8 „Einfach" ist ein allgemein anerkannter Sammelbegriff für die Arten von Vertrauensdiensten, die die Anforderungen „fortgeschritten" nicht erreichen.
9 Qualifizierte Vertrauensdienste sind fortgeschrittene Vertrauensdienste, die zusätzlich die einschlägigen Anforderungen der eIDAS-VO erfüllen.

Mitgliedstaaten und genießen Anwendungsvorrang vor mitgliedstaatlichen Gesetzen. Ergänzt und präzisiert wird die eIDAS-VO in Deutschland unter anderem durch das Vertrauensdienstegesetz, das Personalausweisgesetz und diverse Vorschriften in Verfahrensordnungen. Nationale Vorschriften behalten gegenüber der eIDAS-VO grundsätzlich ihre Gültigkeit und können sogar die Regelungen der eIDAS-VO ergänzen und konkretisieren, soweit sie inhaltlich nicht im Widerspruch zu diesen stehen.[10] Der nationale Gesetzgeber darf kein gegen Unionsrecht verstoßendes Recht setzen.[11]

3. Reformvorschlag zur eIDAS-VO: Regulierung digitaler Identitäten

Um die Wirksamkeit der eIDAS-VO zu verbessern, ihre Vorteile auf den privaten Sektor auszuweiten und vertrauenswürdige digitale Identitäten für alle Europäer zu fördern, hat die EU-Kommission einen Vorschlag zur Reform der eIDAS-VO vorgelegt.[12] Der Gesetzgebungsprozess ist noch nicht abgeschlossen. Der Rat der EU hat am 6. Dezember 2022 einen gemeinsamen Standpunkt[13] veröffentlicht. Anfang 2023 hat das Europäische Parlament erste Änderungsvorschläge vorgelegt[14] und eine entsprechende Position für die Trilog-Verhandlungen beschlossen (A9-0038/2023).[15] Der Europäische Rat und das Parlament erzielten am 29. Juni 2023 eine vorläufige politische Einigung über die Kernelemente der eIDAS-Reform.[16] Bis Anfang August 2023 war noch keine finale Version des Reformgesetzes veröffentlicht. Es wird erwartet, dass das Gesetzgebungsverfahren noch im Jahr 2023 abgeschlossen wird.

10 *Roßnagel*, MMR 2015, 359, 360.
11 EuGH, Rs. C-74/86, ECLI:EU:C:1988:198, Rn. 10 – Kommission/Deutschland; EuGH, Rs. C-106/77, ECLI:EU:C:1978:49, Rn. 17, 18 – Simmenthal II.
12 Vorgang 2021/0136/COD.
13 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, Gemeinsamer Standpunkt vom 6 Dezember 2022, Dokument ST 15706 2022 INIT.
14 Konsolidierter Vorschlag des Europäischen Parlaments: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2023/02-09/05_CA_eIDAS_EN.pdf;
15 https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_DE.pdf.
16 PM Rat der EU vom 29. Juni 2023, https://www.consilium.europa.eu/de/press/press-releases/2023/06/29/council-and-parliament-strike-a-deal-on-a-european-digital-identity-eid/.

Anstoß der Reform ist, dass sich auf dem Markt ein neues Umfeld abzeichnet, in dem sich der Schwerpunkt von der Bereitstellung und Verwendung starrer digitaler Identitäten auf die Bereitstellung und Verwendung einzelner Attribute dieser Identitäten verlagert hat. Die Nachfrage nach Lösungen für die elektronische Identität, mit denen diese Anforderungen erfüllt werden und nicht nur Effizienzgewinne, sondern auch ein hohes Maß an Vertrauen sowohl im privaten als auch im öffentlichen Sektor in der gesamten EU erzielt werden, ist gestiegen.[17] Die derzeitige Verordnung würde diesen neuen Marktanforderungen nicht gerecht, weil sie ausschließlich auf den öffentlichen Sektor beschränkt ist, die Verknüpfung privater Online-Anbieter mit eID-Lösungen kompliziert und nur begrenzt möglich ist, notifizierte eID-Lösungen nicht in allen Mitgliedstaaten ausreichend verfügbar sind und die Verordnung keine ausreichende Flexibilität böte, um eine Vielzahl von Anwendungsfällen abzudecken. Alternative Identitätslösungen, die nicht in den Anwendungsbereich der eIDAS-Verordnung fallen, etwa solche, die von Betreibern sozialer Medien und von Finanzinstituten angeboten werden, geben zudem Anlass zu Bedenken hinsichtlich des Schutzes der Privatsphäre und des Datenschutzes.[18] Außerdem ist es bisher den meisten Menschen nicht möglich, Informationen über ihre Identität, Alter, berufliche Qualifikation, Führerschein oder andere Berechtigungen sowie Zahlungsdaten sicher und unter Einhaltung eines hohen Datenschutzniveaus grenzüberschreitend auszutauschen.[19]

3.1 EUid-Brieftasche

Um diese Lücke zu schließen, schlägt die EU-Kommission die sogenannte EUid-Brieftasche vor.[20] Diese soll es den Nutzenden gemäß Art. 6a Abs. 1

17 Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS), COM(2021) 290 final, S. 7 f.

18 Bericht der Kommission an das Europäische Parlament und den Rat über die Bewertung der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (eIDAS), COM(2021) 290 final, S. 8.

19 Erwägungsgrund 35 eIDAS-VO-E.

20 Der Architecture and Reference Framework (Architektur und Referenzrahmen für die EUid-Brieftasche) Januar 2023, Version 1.0, Repository: https://code.europa.eu/eudi/architecture-and-reference-framework soll als gemeinsamer Standard zur Entwicklung der EUid-Brieftasche dienen.

und Erwägungsgrund 9 eIDAS-VO-E ermöglichen, sich online und offline grenzübergreifend für öffentliche und private Dienste elektronisch zu identifizieren und zu authentifizieren. Neben dem Ziel, bürger- und unternehmensfreundliche digitale Dienste anzubieten, soll vor allem eine Alternative zu Wallets großer US-Konzerne wie Apple Wallet geboten werden, um zu verhindern, dass EU-Bürger wichtige Daten und Dokumente dort hinterlegen.[21] Das ist wirtschaftlich für die EU unvorteilhaft. Für die EU-Bürger ist es riskant, da für personenbezogene Daten von EU-Bürgern, die in den USA gespeichert werden, kein ausreichender Schutz gewährleistet werden kann und dem Zugriff der jeweiligen Nachrichtendienste ausgesetzt sind.[22] Die Regelungen zum „EU-US Data Privacy Framework" bieten hier zwar neue Rechtschutzmöglichkeiten, lösen das in der Speicherung wichtiger elektronischer Dokumente in Drittländern liegende immanente Probleme jedoch nicht auf.

Um eine möglichst breite Verfügbarkeit und Nutzbarkeit der EUid-Brieftasche zu erreichen, sollen neben der öffentlichen Verwaltung auch private Anbieter etwa in den Bereichen Verkehr, Energie, Bank- und Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Wasserversorgung, Postdienste, digitale Infrastruktur, Bildung oder Telekommunikation als sogenannte private vertrauende Beteiligte die Nutzung der Brieftasche akzeptieren, wenn aufgrund rechtlicher oder vertraglicher Verpflichtungen eine starke Nutzerauthentifizierung notwendig ist.[23] Dies würde das Online-Ausweiswesen erheblich voranbringen. Zudem sollen auch große Online-Plattformen im Sinne des Art. 33 DSA die EUid-Brieftasche akzeptieren müssen, sofern sie von den Nutzenden eine Authentifizierung für Online-Dienste, etwa zur Überprüfung des Alters, verlangen.[24] Der Verordnungsentwurf statuiert damit einen zumindest teilweisen Anbindungszwang privater Diensteanbieter.[25]

Jeder Mitgliedstaat hat gemäß Art. 6a Abs. 1 eIDAS-VO-E 12 Monate nach Inkrafttreten der Verordnung eine EUid-Brieftasche herauszugeben.

21 So können in einzelnen Bundesstaaten der USA bereits Führerscheindaten in der Apple Wallet hinterlegt werden, *Wölbert*, c't 09/2022, S. 144.

22 Zu letzterem Punkt *Roßnagel u.a.*, DuD 2022, 156.

23 Erwägungsgrund 28 und Art. 12b Abs. 2 eIDAS-VO-E.

24 Art. 12 Abs. 3 eIDAS-VO-E und Erwägungsgrund 28 eIDAS-VO-E. Der für diese Ausarbeitung zugrunde liegende eIDAS-VO-E spricht noch von Art. 25 DSA. In der rechtsgültigen Fassung des DSA (Verordnung (EU) 2022/2065) handelt es sich dabei aber um Art. 33 DSA.

25 *Liptak*, DuD 2022, 18 (19).

Gemäß Abs. 2 kann diese alternativ von einem anderen Aussteller herausgegeben werden, entweder im Auftrag des Mitgliedstaates (lit. b) oder auch unabhängig, aber von einem Mitgliedstaat anerkannt (lit. c). Der Ausbau der nationalen eID-Systeme wird so beschleunigt und der Prozess der Notifizierung verändert, denn eID-Systeme sollen nach Art. 12a eIDAS-VO-E zertifiziert werden und die Übergangsfrist zur Pflicht einer gegenseitigen Anerkennung wird von zwölf auf sechs Monate verkürzt.[26]

Mindestanforderungen an die EUid-Brieftasche sind nach Art. 6a Abs. 3 eIDAS-VO-E die Online- und Offline-Authentifizierung für öffentliche und private Online-Dienste durch sicheres, transparentes und nachvollziehbares Anfordern und Erhalten, Speichern, Auswählen, Kombinieren und Weitergeben der erforderlichen gesetzlichen Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen (lit. a) sowie das Unterzeichnen mit qualifizierten elektronischen Signaturen (lit. b).[27]

Für eine größtmögliche Praktikabilität und weitreichende Anwendbarkeit der EUid-Brieftasche definiert Art. 6a Abs. 4 lit. a eIDAS-VO-E, für wen und für welche Zwecke gemeinsame Schnittstellen vorhanden sein müssen. Zur Gewährleistung der Vertrauenswürdigkeit der EUid-Brieftasche formuliert der Verordnungsentwurf verschiedene Anforderungen. So muss die EUid-Brieftasche gemäß Art. 6a Abs. 4 lit. c eIDAS-VO-E das Sicherheitsniveau „hoch" im Sinne des Art. 8 eIDAS-VO erfüllen, insbesondere bezüglich der Anforderungen an Identitätsnachweis und Identitätsüberprüfung und an die Verwaltung und Authentifizierung elektronischer Identifizierungsmittel. Außerdem dürfen gemäß Art. 6a Abs. 4 lit. b eIDAS-VO-E die Vertrauensdiensteanbieter, die Attributsbescheinigungen ausstellen, keinerlei Informationen darüber erhalten, wie das entsprechende Attribut verwendet wurde.

Weiterhin verspricht der Verordnungsentwurf in Art. 6a Abs. 7 Satz 1 eIDAS-VO-E, dass die uneingeschränkte Kontrolle über die EUid-Brieftasche beim Nutzenden liegt. Das bedeutet gemäß Satz 2 insbesondere, dass Aussteller der Brieftasche Informationen über die Verwendung der Brieftasche, die für die Erbringung der damit verbundenen Dienste nicht erforderlich sind, nicht sammeln dürfen. Außerdem darf der Aussteller auch andere Personenidentifizierungsdaten oder andere Daten nicht mit personenbezogenen Daten aus anderen vom Aussteller angebotenen Diensten oder aus

26 *Seegebart*, DuD 2022, 5 (6).
27 *Seegebart*, DuD 2022, 5 (6).

Diensten Dritter kombinieren. Etwas anderes gilt nur, wenn der Nutzende dies ausdrücklich verlangt.

Die zur Bereitstellung der Brieftasche erforderlichen Daten (der Verordnungsentwurf spricht von „Daten in Bezug auf die Bereitstellung") müssen gemäß Art. 6a Abs. 7 Satz 3 eIDAS-VO-E von allen anderen gespeicherten Daten physisch und logisch getrennt gehalten werden. Genauere technische Vorgaben gibt es keine. Zwar darf die Kommission gemäß Art. 6a Abs. 11 eIDAS-VO-E innerhalb von 6 Monaten nach Inkrafttreten der Verordnung per Durchführungsrechtsakt technische und betriebliche Spezifikationen erlassen, dies gilt jedoch nur für die Anforderungen der Absätze 3, 4 und 5, nicht jedoch für das Versprechen der uneingeschränkten Kontrolle des Nutzenden und die physische und logische Trennung der Daten nach Absatz 7.

Nach Art. 11a eIDAS-VO-E müssen Mitgliedstaaten für ihre notifizierten Identifizierungsmittel und EUid-Brieftaschen eine eindeutige Identifizierung gewährleisten. Dies soll durch eine eindeutige und dauerhafte Kennung geschehen, die mit einem von den Mitgliedstaaten nach Art. 12 Abs. 4 lit. d eIDAS-VO-E zu definierenden Mindestsatz an Personenidentifizierungsdaten verknüpft werden, um den Nutzenden zu identifizieren, wenn diese gesetzlich vorgeschrieben ist.

3.2 Neue Vertrauensdienste

Vertrauensdienste dienen dazu sicherzustellen, dass elektronische Daten nicht unbemerkt verändert wurden und schaffen so einen Vertrauensraum im elektronischen Rechtsverkehr. Neben den in der eIDAS-VO bisher schon geregelten Vertrauensdiensten zur Erstellung, Überprüfung, Validierung von Signaturen, Siegeln Zeitstempeln und Zertifikaten zur Webseitenauthentifizierung kommen in Art. 3 Nr. 16 eIDAS-VO-E neue hinzu. Diese dienen in erster Linie der Durchführung und Umsetzung der EUid-Brieftasche.

Die Vertrauensdienste zur Beweiswerterhaltung von Signaturen und Siegeln werden ergänzt um einen Vertrauensdienst zur langfristigen Aufbewahrung elektronischer Dokumente. Der Vertrauensdienst zur elektronischen Archivierung elektronischer Dokumente gemäß Art. 3 Nr. 16 lit. d, Nr. 47 eIDAS-VO-E ist ein Dienst für die Entgegennahme, Speicherung Löschung und Übermittlung elektronischer Daten und Dokumente, der ihre Unversehrtheit, die Richtigkeit ihrer Herkunftsangaben und ihre recht-

lichen Merkmale während des gesamten Aufbewahrungszeitraums gewährleistet.[28] Denkbarer Anwendungsbereich könnte die revisionssichere elektronische Finanzbuchhaltung sein,[29] mit dem erklärten Ziel bestehende nationale Anforderungen zur Archivierung zu vereinheitlichen und grenzüberschreitende Anerkennung qualifizierter Dienste zu erleichtern.[30] In jedem Fall sind aber weitere technische Vorgaben notwendig, die gemäß Art. 45g eIDAS-VO-E per delegiertem Rechtsakt durch die Kommission zu erlassen wären.

Der Vertrauensdienst zur Verwaltung von elektronischen Fernsignatur- und Siegelerstellungseinheiten gemäß Art. 3 Nr. 16 lit. e eIDAS-VO-E gehört ebenfalls zu den im Reformvorschlag neu aufgenommenen Vertrauensdiensten. Gemäß Art. 3 Nr. 23 a und b eIDAS-VO-E sind qualifizierte elektronische Fernsignatur- und Siegelerstellungseinheiten solche, bei denen ein qualifizierter Vertrauensdiensteanbieter die elektronischen Signatur- bzw. Siegelerstellungsdaten im Namen eines Unterzeichners bzw. Siegelerstellers erzeugt, verwaltet oder vervielfältigt. Konkrete Anforderungen an die qualifizierten Dienste finden sich in Art. 29a und 39a eIDAS-VO-E. Soweit die Authentifizierung eines Fernsignaturnutzers durch eine eID abgesichert würde, könnten solche Fernsignaturen schnell im Bedarfsfalle genutzt werden, da ein längeres und medienbrechendes Authentifizierungsverfahren vermieden werden könnte.[31]

Das elektronische Vorgangsregister aus Art. 3 Nr. 16 lit. f eIDAS-VO-E ist gemäß Art. 3 Nr. 53 eIDAS-VO eine fälschungssichere Aufzeichnung elektronischer Daten, die die Echtheit und Unversehrtheit der enthaltenen Daten, die Richtigkeit ihres Datums und ihrer Uhrzeit sowie die Richtigkeit ihrer chronologischen Reihenfolge gewährleistet. Es dient damit der fälschungssicheren Gewährleistung der Eindeutigkeit, Echtheit und richtigen Abfolge von Dateneinträgen.[32] So können zuverlässige Audit-Trails für die Herkunft von Waren im grenzüberschreitenden Handel geschaffen, der Schutz der Rechte des geistigen Eigentums unterstützt, Flexibilitätsmärkte für Strom ermöglicht, die Grundlage für fortgeschrittene Lösungen für eine

28 *Granc/Fiedler*, DuD 2022, 27 (28 f.).
29 *Liptak*, DuD 2022, 18 (21).
30 Erwägungsgrund 33 eIDAS-VO-E.
31 Einsatzszenario: Eine Bank bietet Kreditabschlüsse online an. Verbraucherkreditverträge bedürfen der Schriftform. Die Unterschrift des Kunden kann durch Fernsignatur erfolgen, wobei die Authentifizierung durch den Vertrauensdiensteanbieter mittels eID erfolgt. Der Vorgang geschieht aus Sicht des Verbrauchers medienbruchfrei.
32 Erwägungsgrund 34 eIDAS-VO-E.

selbst-souveräne Identität geschaffen und effizientere und transformative öffentliche Dienstleistungen unterstützt werden. Abschnitt 11 des Reformvorschlags schafft einen Rahmen für Vertrauensdienste in Bezug auf die Erstellung, Pflege und Rechtswirkungen elektronischer Vorgangsregister und Anforderungen an qualifizierte elektronische Vorgangsregister.

Kein Vertrauensdienst im engeren Sinne, weil nicht in Art. 3 Nr. 16 eIDAS-VO-E genannt, aber von größter Bedeutung für die Praktikabilität und Akzeptanz der EUid-Brieftasche, sind elektronische Attributsbescheinigungen im Sinne des Art. 3 Nr. 44 eIDAS-VO-E. Dabei handelt es sich um elektronische Bescheinigung zur Authentifizierung von Attributen. Attribute sind gemäß Art. 3 Nr. 43 eIDAS-VO-E elektronische Elemente, Eigenschaften oder Merkmale einer natürlichen oder juristischen Person. Mögliche Anwendungsbereiche sind vielfältig, etwa Sozialversicherungsdaten, Geburtsurkunden, Führerschein, Abschlusszeugnisse oder Reisedokumente.[33] Denkbar sind darüber hinaus auch Angaben über die Vertretungsmacht des EUid-Nutzenden für eine andere natürliche oder juristische Person, amts- und berufsbezogene oder sonstige Angaben zur Person des EUid-Nutzenden oder weitere personenbezogene Angaben.[34] Abschnitt 9 des Reformentwurfs beinhaltet Bestimmungen über die Rechtswirkung elektronischer Attributsbescheinigungen in Art. 45a eIDAS-VO-E, ihre Verwendung in öffentlichen Diensten in Art. 45b eIDAS-VO-E und die Anforderungen an qualifizierte Attributsbescheinigungen in Art. 45c eIDAS-VO-E. Um ein hohes Maß an Vertrauen zu gewährleisten, beinhaltet Art. 45d eIDAS-VO-E eine Bestimmung über die Überprüfung von Attributen anhand authentischer Quellen. Damit die Verfügbarkeit elektronischer Attributsbescheinigungen den Nutzenden der EUid-Brieftasche zugutekommt und damit die Nutzenden sich solche Bescheinigungen für EUid-Brieftaschen ausstellen lassen können, müssen Anbieter elektronischer Attributsbescheinigungen nach Art. 45e eIDAS-VO-E eine Schnittstelle zur EUid-Brieftasche bereitstellen. Art. 45f eIDAS-VO-E enthält zusätzliche Vorschriften für die Erbringung von Diensten für elektronische Attributsbescheinigungen, unter anderem zum Schutz personenbezogener Daten.

33 Erwägungsgrund 26 und 27 des Verordnungsentwurfs.
34 So bereits § 12 Abs. 1 Nr. 1-3 VDG.

4. Digitale Identitäten im Kontext des neuen europäischen Datenrechts

Als neues Rechtsgebiet hat das Datenrecht mittlerweile schon sehr konkrete Konturen angenommen. Data Governance Act (DGA), Digital Services Act (DSA), Digital Markets Act (DMA), Artificial Intelligence Act (AIA) und Data Act (DA) bestimmen zukünftig neben der Datenschutz-Grundverordnung (DSGVO) über Austausch, Nutzung und Dienste um Daten. Diese Rechtsakte hängen auf verschiedene Art und Weise zusammen und greifen ausdrücklich und indirekt ineinander.[35] Diese (geplanten) Rechtsakte der Europäischen Union zum Datenrecht sind direkt und indirekt mit der eIDAS-VO verzahnt und verlangen zum Beispiel eine rechtssichere Identifizierung. Diese darf die Nutzenden jedoch nicht in ihren grundrechtlich gewährleisteten Rechten einschränken. Aus den verfassungsrechtlich garantierten Rechten auf Schutz personenbezogener Daten aus Art. 8 Grundrechtecharta (GrCh) sowie dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 iVm Art. 1 Abs. 1 Grundgesetz (GG), aber auch dem Recht auf freie Meinungsäußerung aus Art. 11 GrCh sowie Art. 5 GG, erwächst das Recht von Nutzenden, das Internet anonym oder unter Pseudonym zu nutzen.[36] Daraus erwächst zwar kein absolutes Recht auf Anonymität, ein Eingriff in diese Grundrechte ist aber nur möglich, wenn dieser verhältnismäßig ist.

Im Rechts- und Geschäftsverkehr gibt es Vorgaben, die ein Anonymbleiben verhindern. Bei Bankgeschäften und im Versicherungswesen gibt es Vorschriften, die eine Identitätsprüfung zwingend voraussetzen, etwa im Geldwäschegesetz. Auch die Durchführung von Verwaltungsangelegenheiten setzt eine Identitätsprüfung voraus. Und schließlich bedarf es für eine effektive Strafverfolgung der Möglichkeit, die Personalien einer Person festzustellen. Für Online-Plattformen gibt es keine gesetzlich vorgeschriebene Prüfung zur Feststellung der Identität bei Erstellung eines Accounts. Gerade auf Social-Media-Plattformen besteht jedoch eine erhebliche Gefahr für die Verbreitung von Desinformationen[37] und sogar die Begehung von Straf-

35 Ausführlich *Geminn/Johannes (*Hrsg.), Europäisches Datenrecht, 2023, passim.

36 Z.B. *Jarass*, in: Jarass/Pieroth (Hrsg.), Grundgesetz, 2022, Art. 5 GG, Rn. 13, 110; *Polenz*, in: Taeger/Pohle (Hrsg.), Computerrechts-Handbuch, 2022, Teil 13, Kap. 130 Rn. 59. S. auch das Urteil des EuGH zum Verstoß der deutschen Vorratsdatenspeicherung gegen Unionsrecht, EuGH (Große Kammer), Urt. v. 20.9.2022 – C-793/19, C-794/19 (Bundesrepublik Deutschland/SpaceNet AG ua), Rn. 54.

37 Dazu *Steinebach u.a.* (Hrsg.): Desinformation aufdecken und bekämpfen, 2020, passim.

taten, Urheberrechtsverletzungen und Hasskriminalität, die dadurch nur schwer verfolgbar ist.[38] Häufig wird daher darüber diskutiert, ob eine Identifizierung der Nutzenden notwendig ist, um Straftaten besser verfolgen zu können. Die sogenannte Klarnamenpflicht sollte zur Konsequenz haben, dass alle Nutzenden einer Online-Plattform sich immer dem Plattformbetreiber gegenüber eindeutig identifizieren müssten und eine anonyme oder pseudonyme Nutzung faktisch ausgeschlossen wäre. Für die informationelle Selbstbestimmung und die Meinungsfreiheit stellt eine Verpflichtung aller Nutzenden zur Identifizierung gegenüber dem Plattformbetreiber in Abwägung mit Strafverfolgungsinteressen der Allgemeinheit und anderer schwerwiegender Risiken[39] aber einen unverhältnismäßigen Eingriff dar.[40]

Möglicherweise ließe sich die EUid-Brieftasche hier interessenausgleichend und grundrechtschonend nutzbar machen. Grundsätzlich wäre es möglich, dass eine Online-Plattform, z.B. ein Kurznachrichtendienst, eine Authentifizierung eines Nutzenden anstößt, die darauf beschränkt ist festzustellen, dass diese eine eineindeutige eID verwendet.[41] Auf diese Weise könnte die Plattform versuchen sicherzustellen, dass hinter jedem Nutzenden auch tatsächliche eine natürliche Person steht. So könnte sie sog. Trollfabriken und -netzwerken sowie Fake-Accounts entgegenwirken. Denkbar wäre aber auch, ein Pseudonym zu generieren, das in Form eines Attributs im Sinne des Art. 3 Nr. 43 eIDAS-VO-E in der EUid-Brieftasche hinterlegt ist. Dieses Pseudonym müsste von einem Treuhänder, etwa einem Vermittlungsdienst nach Art. 10 lit. a DGA, vergeben und verwaltet werden. Im Falle einer möglichen Strafverfolgung wegen krimineller Handlungen auf Online-Plattformen kann der Treuhänder die Identifizierung der Person gegenüber den Strafverfolgungsbehörden ermöglichen. Wirkungsvoll wäre diese Lösung nur, wenn Nutzende verpflichtet wären, sich mit der EUid-Brieftasche zu identifizieren – wenn auch nur mit Pseudonym. Dies widerspricht aber dem Ansatz des Art. 12b Abs. 3 eIDAS-VO-E, dass der Einsatz der EUid-Brieftasche alleinig auf Verlangen der Nutzenden geschehen soll.

38 Dies ist außerdem ein immer wieder bemühtes Argument für die Vorratsdatenspeicherung, die der EuGH zum Schutz der Anonymität im Netz nur für sehr eingeschränkt unionsrechtsmäßig hält, EuGH (Große Kammer), Urt. v. 20.9.2022 – C-793/19, C-794/19 (Bundesrepublik Deutschland/SpaceNet AG ua). Siehe dazu ausführlich *Roßnagel*, ZD 2022, 650.

39 ZB *Schmierer*, Klarnamenpflicht als Risiko für marginalisierte Gruppen, 2023.

40 Ausführlich zur Klarnamenpflicht *Nebel*, K&R 2019, 148 sowie *dies.*, ZD-Aktuell 2022, 01077.

41 Zero Knowledge Proof, s.a. Art. 6a Abs. 4 (a) (vi) eIDAS-VO-E-Parl.

Hier obliegt es dem Gesetzgeber, die Voraussetzungen dafür zu schaffen, dass der Einsatz der EUid-Brieftasche größere Bedeutung erlangt.

Auch jenseits der Diskussion um die mögliche Identifikation von Personen für Zwecke der Strafverfolgung stellt sich die Frage, ob die EUid-Funktion im restlichen europäischen Datenrecht nutzbar zu machen ist bzw. welchen Beitrag die EUid-Brieftasche zur effektiven Umsetzung der Vorgaben in den jeweiligen Gesetz(-entwürf)en leisten kann.

4.1 eIDAS-VO-E

Der eIDAS-VO-E selbst verweist nur an einer Stelle explizit auf den DSA. Gemäß Art. 12b Abs. 3 eIDAS-VO-E sowie Erwägungsgrund 28 werden sehr große Online-Plattformen im Sinne des Art. 33 DSA[42] verpflichtet, die EUid-Brieftasche zu akzeptieren, wenn diese von ihren Nutzenden für den Zugang zu Online-Diensten eine Authentifizierung verlangen. Die Online-Plattformen dürfen die Nutzung der EUid-Brieftasche jedoch nicht einfordern, da es allein dem Nutzenden obliegt, ob er sich mit der EUid-Brieftasche authentifizieren möchte oder den Nachweis anders erbringt.

4.2 Digital Services Act (DSA)

Die Verordnung über einen Binnenmarkt für digitale Dienste trat am 16. November 2022 in Kraft und gilt ab dem 17. Februar 2024 unmittelbar in allen Mitgliedstaaten.[43] Der DSA richtet sich an Anbieter von Vermittlungsdiensten, zum Beispiel Internetdienstleister, Cloud-Anbieter, Suchmaschinen, Social Networks und andere Online-Plattformen sowie Online-Marktplätze. Er deckt eine Reihe von Fragen ab, unter anderem ein Verbot von gezielter Werbung, die sich an Minderjährige richtet oder auf besonderen Datenkategorien beruht; ein Verbot irreführender Praktiken und Schnittstellen; die Sorge für mehr Transparenz bei den Parametern für die Empfehlung, Kuratierung oder Priorisierung von Inhalten für Nut-

42 Der für diese Ausarbeitung zugrunde liegende eIDAS-VO-E spricht noch von Art. 25 DSA. In der rechtsgültigen Fassung des DSA (Verordnung (EU) 2022/2065) handelt es sich dabei aber um Art. 33 DSA.

43 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste), ABl. EU vom 27.10.2022, L 277, 1.

zende; die Pflicht zu „Notice and Action"-Verfahren, um die Meldung und Entfernung illegaler Online-Inhalte zu ermöglichen, und die Pflicht zu „Know your business customer"-Anforderungen für Online-Marktplätze, um die Zuverlässigkeit von Händlern zu gewährleisten.[44]

Der DSA beinhaltet zwei Vorschriften, die für die EUid-Brieftasche von Bedeutung sein könnten. Gemäß Art. 23 Abs. 1 DSA setzen Anbieter von Online-Plattformen die Erbringung ihrer Dienste für Nutzende aus, die häufig und offensichtlich rechtswidrige Inhalte bereitstellen. Um diese Vorgabe effektiv umzusetzen und um zu verhindern, dass sich der betreffende Nutzende nicht unter falschem Namen als anderer Nutzender ausgibt, müsste jeder Nutzende eindeutig identifizierbar sein. Dies ließe sich grundsätzlich mit der EUid-Brieftasche bewerkstelligen. Um zu verhindern, dass jeder Vermittlungsdienst Kenntnis über die Identifikation seiner Nutzenden erlangt, könnte auch hier – wie im Zusammenhang mit der Klarnamenpflicht diskutiert – ein Rückgriff auf durch Treuhänder verwaltete Pseudonyme hilfreich sein.

Art. 30 DSA belegt Anbieter von Online-Plattformen, die Verbrauchern den Abschluss von Fernabsatzverträgen mit Unternehmern ermöglichen, mit der Pflicht, die Nachverfolgbarkeit dieser Unternehmer sicherzustellen. Hierzu müssen die Unternehmer dem Anbieter der Online-Plattform bestimmte Informationen zur Verfügung stellen, die in Abs. 1 lit. a bis e näher aufgezählt sind. Hierzu zählen neben dem Namen und Kontaktdaten des Unternehmers (lit. a) die Kopie des Identitätsdokuments oder eine elektronische Identifizierung im Sinne des Art. 3 eIDAS-VO (lit. b), Angaben zum Zahlungskonto des Unternehmers (lit. c), sofern zutreffend Handelsregisternummer oder eine gleichwertige Kennung aus einem öffentlichen Register (lit. d) sowie eine Selbstbescheinigung des Unternehmers, in der sich dieser verpflichtet, nur Produkte oder Dienstleistungen anzubieten, die den geltenden Vorschriften des Unionsrechts entsprechen (lit. e). Hier kann die EUid-Brieftasche erhebliche Vereinfachungen bringen, da bis auf lit. e alle geforderten Angaben grundsätzlich als elektronische Attribute in der EUid-Brieftasche des Unternehmers hinterlegt und so rechtssicher und einfach nachgewiesen werden könnten. Voraussetzung ist lediglich, dass Informationen wie Kennungen aus öffentlichen Registern als elektronisches Attribut verfügbar gemacht werden. Gemäß Abs. 2 obliegt dem Anbieter der Online-Plattform die Pflicht zur Überprüfung dieser Informationen.

44 *Johannes*, ZD-Aktuell 2022, 01166.

Der Einsatz der EUid-Brieftasche würde dieses Verfahren erheblich vereinfachen.

4.3 Data Governance Act (DGA)

Der DGA[45] zielt darauf ab, das Vertrauen in die gemeinsame Nutzung von Daten zu stärken. Er soll neue EU-Regeln für die Neutralität von Datenmarktplätzen schaffen und die Wiederverwendung bestimmter Daten im Besitz des öffentlichen Sektors erleichtern.[46] Der DGA ist am 23. Juni 2022 in Kraft getreten und ist ab dem 24. September 2023 anwendbar.

Einer der zentralen Regelungsbereiche des DGA ist die Etablierung so genannter Datenvermittlungsdienste. Dabei handelt es sich gemäß Art. 2 Nr. 11 DGA um „einen Dienst, mit dem durch technische, rechtliche oder sonstige Mittel Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und Datennutzern andererseits hergestellt werden sollen, um die gemeinsame Datennutzung, auch für die Zwecke der Ausübung der Rechte betroffener Personen in Bezug auf personenbezogene Daten, zu ermöglichen". Anbieter von Datenvermittlungsdiensten müssen diese Tätigkeit gemäß Art. 11 DGA bei der zuständigen Behörde anmelden. Die Anmeldung muss gemäß Abs. 6 lit. a bis g bestimmte Informationen zum Anbieter enthalten, wie Name, Kontaktangaben, Rechtsform, Vertreter und einiges mehr. Hier könnte die EUid-Brieftaschen-Infrastruktur gut nutzbar gemacht werden, da viele der verlangten Angaben typische Attribute sind, die in einer EUid-Brieftasche hinterlegt werden könnten. Die Übermittlung der Anmeldedaten per EUid-Brieftasche könnte das Verfahren deutlich beschleunigen.

Ein weiterer zentraler Regelungsbereich im DGA ist der Datenaltruismus. Dabei handelt es sich um eine freiwillige Zurverfügungstellung von personenbezogenen und nicht-personenbezogenen Daten, um diese für Ziele von allgemeinem Interesse zu nutzen, wie die Gesundheitsversorgung, die Bekämpfung des Klimawandels, die Verbesserung der Mobilität, die einfachere Entwicklung, Erstellung und Verbreitung amtlicher Statistiken, die Verbesserung der Erbringung öffentlicher Dienstleistungen, die

45 Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt), ABl. EU vom 3.6.2022, L 152, 1.

46 *Johannes*, ZD-Aktuell 2022, 01166.

staatliche Entscheidungsfindung oder die wissenschaftliche Forschung.[47] Die Datenspende basiert auf der Einwilligung der spendenden Personen, so dass die nach Art. 17 ff. DGA zuständigen anerkannten datenaltruistischen Organisationen zum Einwilligungsmanagement verpflichtet sind. Art. 25 DGA sieht hierfür die Entwicklung eines Europäischen Einwilligungsformulars vor, um Datenspenden europaweit zu vereinfachen. Die Einbindung der EUid-Brieftasche könnte das Einwilligungsmanagement in jedem Fall vereinfachen, insbesondere hinsichtlich der Authentizität des Einwilligenden.

4.4 Data Act-Entwurf (DA-E)

Der Vorschlag für eine Verordnung über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz) – im öffentlichen Diskurs vorrangig als Data Act bekannt – wurde am 24. Februar 2022 durch die Europäische Kommission in das offizielle Gesetzgebungsverfahren der EU eingebracht.[48] Der DA-E enthält u. a. Regelungen für ein Recht auf Zugang von bei der Nutzung von Produkten oder verbundenen Diensten erzeugten Daten; ein Verbot unfairer Vertragsklauseln in standardisierten Datenlizenzverträgen; ein Recht auf Datenzugang und -nutzung durch öffentliche Stellen; eine Erleichterung des Wechsels von Datenverarbeitungsdiensten (insbesondere Cloud- und Edge-Anbieter) sowie Anforderungen an die Interoperabilität von Datenverarbeitungsdiensten sowie an die internationale Datenübertragung.[49] Am 20. Juni 2023 erzielten das Europäische Parlament und der Rat im Trilogverfahren eine politische Einigung über den Data Act. Diese Version war bis Anfang August 2023 noch nicht veröffentlicht. Allseits erwartet eird, dass der Data Act noch in 2023 offiziel verabschiedet wird.

Da der DA-E bisher nur als Vorschlag vorlag, können sich im Laufe des Gesetzgebungsprozesses noch Änderungen ergeben. Anknüpfungspunkte für die eIDAS-VO bieten insbesondere zwei Aspekte. Gemäß Erwägungsgrund 20 DA-E sollen „Nutzer von Produkten, die Daten erzeugen, […] in der Regel ein Nutzerkonto einrichten. Dies ermöglicht die Identifizierung des Nutzers durch den Hersteller sowie die Kommunikation zur Ausfüh-

47 *Geminn/Johannes/Müller/Nebel*, Is that even legal? A guide for builders experimenting with data governance in Germany, 2023.
48 Vorgang 2022/0047/COD.
49 *Johannes*, ZD-Aktuell 2022, 01166.

rung und Bearbeitung von Datenzugangsverlangen" im Sinne des Art. 4 DA-E. Erwägungsgrund 27 DA-E stellt zugunsten des Dateninhabers klar, dass dieser eine geeignete Nutzeridentifizierung verlangen kann, um die Berechtigung des Nutzenden auf Zugang zu den Daten zu überprüfen. Hier könnte die EUid-Brieftasche zum Einsatz kommen, und zwar sowohl zur Identifizierung mittels des Namens als auch möglicherweise mittels Pseudonyms, wenn dieses als elektronisches Attribut hinterlegt ist.

Zweiter Anknüpfungspunkt sind „intelligente Verträge". Dabei handelt es sich gemäß Art. 2 Nr. 16 DA-E um ein in einem elektronischen Vorgangsregistersystem gespeichertes Computerprogramm, bei dem das Ergebnis der Programmausführung in dem elektronischen Vorgangsregister aufgezeichnet wird. Elektronische Vorgangsregister sind gemäß Art. 2 Nr. 17 DA-E solche im Sinne des Art. 3 Nr. 53 eIDAS-VO. Diese Computerprogramme in elektronischen Vorgangsregistern sorgen dafür, Transaktionen zu vorab festgelegten Bedingungen auszuführen und abzuwickeln. Sie haben das Potenzial, Dateninhabern und Datenempfängern Garantien dafür zu bieten, dass die Bedingungen für die gemeinsame Nutzung von Daten eingehalten werden.[50] Art. 30 DA-E nennt des Weiteren wesentliche Anforderungen an intelligente Verträge für die gemeinsame Datennutzung.

5. Kritik und Vorschläge zur Rechtsfortbildung

Die EUid-Brieftasche ist konzipiert als Lösung für elektronische Identitäten, die sowohl im öffentlichen als auch im privaten Sektor nutzbar gemacht werden kann, die flexibel genug für viele verschiedene Anwendungsszenarien ist und einen sicheren grenzüberschreitenden Austausch von Informationen zur Identität einer Person zulässt. Eine flächendeckende Einführung einer EUid-Lösung ist begrüßenswert, um mehr Verfahren und Dienste, insbesondere in der öffentlichen Verwaltung, zukünftig rein digital rechtssicher durchführen zu können und sollte zum Anlass genommen werden, noch mehr Angebote hierfür zu schaffen.[51] Dennoch gibt es eine Reihe von Punkten, die aus Sicht des Schutzes der informationellen Selbstbestimmung und des Rechts auf Datenschutz bedenklich sind. Im Laufe des

50 Begründung zum Kommissionsvorschlag 2022/0047/COD, S. 4.

51 Allgemein zu Akzeptanzproblemen der derzeitigen deutschen eID-Lösung durch den neuen Personalausweis (nPA) *Seegebart*, DuD 2022, 5; *Skierka/Parycek*, HMD Praxis der Wirtschaftsinformatik, 1.

Gesetzgebungsverfahrens wurden einige dieser Punkte durch den für das Europäische Parlament federführenden Ausschuss für Industrie, Forschung und Energie (ITRE-Ausschuss) adressiert.[52] Ob und wie diese Eingang in die finale Fassung finden, bleibt jedoch abzuwarten. Im Folgenden werden die kritischen Punkte daher noch einmal zusammengefasst und Vorschläge zur Rechtsfortbildung gemacht.

5.1 Identifizierungskennziffer

Zunächst muss die Erforderlichkeit einer eindeutigen Identifizierungskennziffer bezweifelt werden. Zwar soll dies nach Art. 11a Abs. 2 eIDAS-VO-E „im Einklang mit dem Unionsrecht", also auch unter Zugrundelegung der Grundsätze der DSGVO erfolgen. Allerdings widerspricht es dem Zweck der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO, dem „Mindestsatz von Personenidentifizierungsdaten", die für sich genommen die Identifizierung der Person ermöglichen müssen, eine zusätzliche Kennziffer hinzuzufügen, die dauerhaft mit der Person des Nutzenden verknüpft ist. Die eindeutige dauerhafte Kennung zur Identifizierung des Nutzenden der EUid-Brieftasche birgt gleich eines „Super-Cookies"[53] erhebliche Risiken für die betroffene Person. Wird eine solche Kennung bereichsübergreifend von Behörden bis Onlineplattformen für digitale Services verwendet, könnten über alle Dienste hinweg umfassende Persönlichkeitsprofile erstellt werden.[54] Diese Gefahr wird noch dadurch verstärkt, dass jeder Mitgliedstaat selbst eine gesetzliche Identifizierung vorschreiben kann. So wäre es ein Leichtes, zum Beispiel eine Klarnamenpflicht in Social Media vorzuschreiben, die nur durch eine persönliche Identifizierung mit der EUid-Brieftasche durchgesetzt werden kann.[55] Privaten Online-Diensten würde die eigene umfassende Profilbildung durch eine staatlich verifizierte Kennziffer einfach gemacht werden. Auch die Entwurfsfassung des Rates vom

52 Konsolidierter Vorschlag des Europäischen Parlaments: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/ITRE/DV/2023/02-09/05_CA_eIDAS_EN.pdf; *Greis*, Elektronische Identität: Europaparlament will lebenslange Personenkennziffer stoppen.

53 Offener Brief von Epicenter.works, weiteren NGOs und Datenschützern vom 1. Februar 2023, https://epicenter.works/sites/default/files/open_letter_eidas_2023-01_0.pdf.

54 So auch *Wölbert*, c't 09/2022, 144.

55 Zur Kritik an Art. 11a eIDAS-VO-E *Wölbert*, c't 9/2022, 144; s.a. *Nebel*, K&R 2019, 148; *dies.*, ZD-Aktuell 2022, 01077.

6. Dezember 2022 nimmt von der Kennziffer keinen Abstand.[56] Das Europäische Parlament möchte die Nutzung einer solchen Kennziffer zumindest erheblich einschränken und nur für grenzüberschreitende Transaktionen vorsehen, schließt eine solche aber nicht grundsätzlich aus (vgl. Art. 11a Abs. 2 eIDAS-VO-E-Parl). Aus datenschutzrechtlicher Sicht ist die Vergabe einer solcher Kennziffern grundsätzlich äußerst risikobehaftet. Eine dauerhafte, also lebenslang bestehende, eindeutige Kennung ist zur Identifizierung einer Person ist in der Regel nicht zwingend erforderlich, da der Abgleich des Namens und Geburtsdatums ggf. mit weiteren Attributen zur eindeutigen Identifizierung einer Person zumeist ausreichen wird. Daher liegt ein Verstoß gegen das Prinzip der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO nahe und sollte zum Anlass genommen werden, Art. 11a eIDAS-VO-E insgesamt zu streichen.

Problematisch ist zudem, dass keine einheitlichen Vorgaben gemacht werden, für welche Zwecke eine Identifizierung samt eindeutiger dauerhafter Kennung notwendig sein soll. Vielmehr kann jeder einzelne Mitgliedstaat über die Zwecke der Identifizierung bestimmen. Dies lässt nicht nur einen Flickenteppich befürchten, sondern könnte darüber hinaus dazu führen, dass die Ausweispflicht online wie offline deutlich ausgeweitet wird. Wenn Mitgliedstaaten beispielsweise festlegen, dass jede Registrierung auf einer Online-Plattform mit Namen und eindeutiger Kennung zu erfolgen hat,[57] käme dies der Einführung einer Klarnamenpflicht durch die Hintertür gleich. Daher sollte klar geregelt werden, für welche Zwecke eine Identifizierung notwendig ist und wer welche Daten abfragen darf. Technische Vorkehrungen sollten unterstützen, dass nicht mehr Informationen abgefragt werden als rechtlich zulässig.

Zwar legt der Reformvorschlag der Kommission fest, dass die alleinige Kontrolle über die Daten beim Nutzenden verbleibt. Es steht jedoch zu befürchten, dass sich am Machtgefälle zwischen Nutzenden einerseits und großen Online-Plattformen andererseits nicht grundsätzlich etwas ändern wird. Der Datenschatz der EUid-Brieftasche könnte Begehrlichkeiten wecken und insbesondere private Anbieter dazu bringen, Nutzende durch Dark Patterns oder Versprechungen dazu zu verleiten, mehr Daten preiszugeben als nötig. An dieser Stelle müsste etwa durch gesetzlich vorgeschriebene restriktive Voreinstellungen sichergestellt werden, dass Nutzende

56 Vgl. Erwägungsgründe 17a und 17aa des Ratsentwurfs.
57 *Wölbert*, c't 9/2022, 144.

nicht etwa aus Unwissenheit oder Bequemlichkeit mehr Daten übermitteln als erforderlich.[58] Der Parlamentsentwurf sieht entsprechend eindeutig in Art. 6a Abs. 7a vor, dass die Nutzung der Europäischen digitalen Brieftasche freiwillig sei. Der Zugang zu öffentlichen und privaten Dienstleistungen und die Berufsfreiheit dürften in keiner Weise eingeschränkt werden für Personen, die keine EUid-Brieftasche verwenden. Kritisch hervorzuheben sind auch die fehlenden ausdrücklichen Möglichkeiten pseudonymer Nutzung.[59] Zwar sieht Art. 5 eIDAS-VO-E vor, dass die pseudonyme Nutzung bei elektronischen Transaktionen nicht untersagt werden darf. Wünschenswert, weil datenschutzfreundlich, wäre darüber hinaus aber die explizite Verpflichtung auf Ermöglichung der pseudonymen Identifizierung, auch und gerade gegenüber großen Online-Plattformen. Hierin würde ein großer Gewinn für die alltägliche Nutzung der Wallet liegen, um Straftaten im Internet leichter verfolgbar zu machen, ohne die wahre Identität aller Nutzenden in die Hände von einzelnen Online-Plattformen zu legen.

5.2 Verlust oder Missbrauch der EUid-Brieftasche

Bisher nur unzureichend geregelt ist zudem das Vorgehen bei Verlust oder Missbrauch der EUid-Brieftasche. Der Kommissionsentwurf sieht keine Regelungen für die Sperrung vor. Hier hat der Ratsentwurf zwar nachgebessert, weil Art. 6 Abs. 4a des Ratsentwurfs die Mitgliedstaaten verpflichten, entsprechende Regelungen für die Meldung des Verlusts oder Missbrauchs der EUid-Brieftasche oder Beantragung des Widerrufs vorzusehen. Auch der Parlamentsentwurf sieht in Art. 6a Abs. 5a vor, dass es möglich sein muss die Gültigkeit der EUid-Brieftasche zu widerrufen, und zwar entweder auf ausdrücklichen Antrag des Nutzenden, wenn die Sicherheit der Brieftasche beeinträchtigt wurde, beim Tod des Nutzenden oder bei Einstellung der Tätigkeit der juristischen Person. Dennoch bleibt weiter unklar, wie sichergestellt werden soll, dass eine Person nur die eigene EUid-Brieftasche sperrt oder widerruft und nicht die einer beliebigen anderen Person.

58 Die Regelung geht über Art. 25 DSGVO hinaus, da sie sich an die Entwickler der EUid-Brieftasche richtet und die Pflicht zu Privacy by Design und Default für die EUid-Brieftasche konkretisiert.

59 Der Parlamentsentwurf bessert hier nach, siehe insbesondere Art. 5.

5.3 Dezentrale Speicherung

Grundsätzlich begrüßenswert ist der Ansatz, dass die EUid-Brieftasche dezentral auf den Endgeräten der Nutzenden gespeichert wird und nicht zentral in einer einzigen Datenbank. Dennoch bleiben Bedenken hinsichtlich einer ausreichenden Datensicherheit. Die Speicherung auf den persönlichen Endgeräten der Nutzenden hat zur Folge, dass ihnen auch die große Verantwortung obliegt, für ausreichende Datensicherheit ihrer Endgeräte zu sorgen. Hier sind neben der grundsätzlich vorauszusetzenden Sicherheit und Verlässlichkeit der Software weitere Maßnahmen notwendig, die Nutzende niedrigschwellig dazu bringen, ein möglichst hohes Maß an Datensicherheit zu gewährleisten. Dies beginnt mit einer ausreichenden Zugangssperre zur EUid-Brieftasche (Passwort), Vermeiden von Spähsoftware auf dem Endgerät und hört bei konkreten automatisierten Hinweisen auf mögliche Gefahren auf dem Endgerät nicht auf.

Wichtige Aspekte der technischen Umsetzung der EUid-Brieftasche obliegen Durchführungsrechtsakten der Kommission, beispielsweise Art. 6a Abs. 11 und Art. 6b Abs. 4 eIDAS-VO-E. Dass konkrete technische Vorgaben nicht im Gesetz selbst spezifiziert sind, ist nicht ungewöhnlich und hat den Vorteil, dass sie sich bei schnellem technischem Wandel leichter anpassen lassen. Es wäre jedoch wünschenswert, konkrete Anforderungen an die Technik wie Interoperabilität, dezentrale Speicherung und die Verwendung offener Standards explizit im Gesetz zu normieren, um einen umfassenden Grundrechtsschutz zu gewährleisten und einen hohen technischen Standard zu gewährleisten. Insbesondere der Vorschlag des Parlaments ist hinsichtlich der Nennung technischer Zielvorgaben konkreter.

5.4 Bedeutung im Datenrecht erhöhen

Neben den konkreten Kritikpunkten zur EUid-Brieftasche, die sich aus dem eIDAS-VO-E ergeben, bleibt zu überlegen, wie deren Bedeutung im restlichen Datenrecht der Union intensiviert werden kann. Möglicherweise wäre eine explizite Bezugnahme auf die EUid-Brieftasche in anderen Rechtsakten oder eine Privilegierung ihres Einsatzes sinnvoll, um deren Verbreitung voranzutreiben. Denkbar wäre dies beispielsweise bei Art. 11 Abs. 6 DGA[60] im Rahmen der Anmeldung der Anbieter von Datenvermitt-

60 S. Kapitel 4.3.

lungsdiensten, bei Art. 25 DGA[61] im Rahmen des Europäischen Einwilligungsformulars oder bei der Durchsetzung der Sperrung solcher Nutzenden nach Art. 23 DSA[62], die rechtswidrige Inhalte auf Online-Plattformen bereitstellen.

6. Fazit

Die EUid-Brieftasche verspricht eine deutliche Vereinfachung bei der Nutzung elektronischer Dienste – unabhängig davon, ob diese grenzüberschreitend sind oder nicht. Auch das neue europäische Datenrecht bietet genügend Anknüpfungspunkte, um der EUid-Brieftasche zu noch mehr Bedeutung zu verhelfen. Einige der Vorschläge zur Umsetzung sind jedoch durchaus bedenklich und sollten der Legislative Anlass geben, auf eine datenschutzfreundliche Umsetzung hinzuarbeiten. Die Verhandlungen über die Kernelemte sind wohl abgeschlossen.[63] Die fachlichen Arbeiten zur Vervollständigung des Rechtstextes dauerten Anfang August 2023 noch an. Es bleibt abzuwarten, ob die Trilogverhandlungen die Interessen der Nutzenden der EUid-Brieftasche besser in den Blick genommen haben und insbesondere Aspekte wie die eindeutige lebenslange Kennziffer überdenken sowie Möglichkeiten pseudonymen Handelns, dezentrale Speicherung und ausreichende Datensicherheit im Gesetz verankern werden. Wenigstens Letzteres deutet das vorläufige Trilogergebnis an.

Literaturverzeichnis

Geminn, Christian L. und Johannes, Paul C. (Hrsg.): (2023): *Europäisches Datenrecht*. Baden-Baden: Nomos (in Vorbereitung).

Geminn, Christian L.; Johannes, Paul C.; Müller, Johannes und Nebel, Maxi (2023): *Is that even legal? A guide for builders experimenting with data governance in Germany*. Berlin: Mozilla Foundation. URL: https://foundation.mozilla.org/en/research/library/is-that-even-legal/germany/.

Granc, Franziska und Fiedler, Arno (2022): Nationale und europäische Sicht auf eIDAS 2.0 – Aufwand und Nutzen. *Datenschutz und Datensicherheit (DuD),* S. 27-31.

Greis, Friedhelm (9. Feb. 2023): Elektronische Identität: Europaparlament will lebenslange Personenkennziffer stoppen. URL: https://glm.io/171792.

61 S. Kapitel 4.3.
62 Kapitel 4.2.
63 PM Rat der EU vom 29. Juni 2023 (siehe oben Fn. 16).

Jarass, Hans D. und Kment, Martin (Hrsg.) (2022): *Grundgesetz für die Bundesrepublik Deutschland, Kommentar,* 17. Aufl. München: Beck. Zitiert als Jarass/Pieroth (Begr.).

Johannes, Paul C. (2020): Vertrauensdienste oder Bärendienste? Rechtssicherheit von Kundenportalen Blockchain & Co durch oder neben der eIDAS-VO. In: Hentschel, Anja; Hornung, Gerrit und Jandt, Silke (Hrsg.): *Mensch – Technik – Umwelt: Verantwortung für eine sozialverträgliche Zukunft*. Baden-Baden: Nomos, S. 587-602.

Johannes, Paul C. (2022): Europäisches Datenrecht – ein Spickzettel. *ZD-Aktuell*, 01166.

Kudra, Andre; Seegebart, Christian und Schwalm, Steffen (2022): Ein digitaler Vertrauensraum für Identitäten und Dienste – Europa ist auf dem richtigen Weg. *Datenschutz und Datensicherheit (DuD)*, Heft 1, S. 9-11.

Liptak, Patrick (2022): Ein neuer Rahmen für eine europäische digitale Identität. *Datenschutz und Datensicherheit (DuD)*, Heft 1, S. 18-21.

Nebel, Maxi (2019): Die Zulässigkeit der Erhebung des Klarnamens nach den Vorgaben der Datenschutz-Grundverordnung. *Kommunikation und Recht (K&R)*, Heft 3, S. 148-152.

Nebel, Maxi (2022): Klarnamenpflicht nach DS-GVO und TTDSG. *ZD-Aktuell*, 01077.

Roßnagel, Alexander (2015): Der Anwendungsvorrang der eIDAS-Verordnung – Welche Regelungen des deutschen Rechts sind weiterhin für elektronische Signaturen anwendbar? *Multimedia und Recht (MMR)*, Heft 6, S. 359-364.

Roßnagel, Alexander (2022): Vorratsdatenspeicherung – was geht noch und was nicht mehr? *Zeitschrift für Datenschutz (ZD)*, Heft 12, 650-655.

Roßnagel, Alexander; Geminn, Christian L.; Johannes, Paul C.; Müller, Johannes (2022): Auswirkungen ausländischer Gesetzgebung auf die deutsche Cybersicherheit. *Datenschutz und Datensicherheit (DuD)*, Heft 3, S. 156-163.

Roßnagel, Alexander und Johannes, Paul C. (2013): Entwurf einer EU-Verordnung über elektronische Identifizierung und Vertrauensdienste – Neue Regeln für elektronische Sicherheitsdienste. *Zeitschrift für Datenschutz (ZD)*, Heft 2, S. 65-72.

Schmierer, Anna-Lena (14. April 2023): Klarnamenpflicht als Risiko für marginalisierte Gruppen. URL: https://netzpolitik.org/2023/meta-verified-klarnamenpflicht-als-risiko-fuer-marginalisierte-gruppen/.

Seegebart, Christian (2022): eIDAS-Novellierung 2021 – erste Analyse des Proposals. *Datenschutz und Datensicherheit (DuD)*, Heft 1, S. 5-8.

Skierka, Isabel und Parycek, Peter (2023): Einwurf – Kann Deutschland seine eID noch retten? HMD Praxis der Wirtschaftsinformatik (8. März 2023), S. 1-6, https://doi.org/10.1365/s40702-023-00958-0.

Spindler, Gerald und Rockenbauch, Matti (2013): Die elektronische Identifizierung – Kritische Analyse des EU-Verordnungsentwurfs über elektronische Identifizierung und Vertrauensdienste. *Multimedia und Recht (MMR)*, Heft 3, S. 139-148.

Steinebach, Martin; Bader, Katarina; Rinsdorf, Lars; Krämer, Nicole und Roßnagel, Alexander (Hrsg.): (2020): *Desinformation aufdecken und bekämpfen. Interdisziplinäre Ansätze gegen Desinformationskampagnen und für Meinungspluralität.* Baden-Baden: Nomos.

Taeger, Jürgen und Pohle Jan (Hrsg.) (2022): *Computerrechts-Handbuch*, 37. Ed. München: Beck.

Wölbert, Christian (2022): Orwells Brieftasche. Die umstrittenen Pläne für eine europäische digitale Identität. *c't Magazin*, Heft 9, S. 144.

„Data Free Flow with Trust“ - Auf der Suche nach dem Vertrauen

Marie-Louise Gächter

Zusammenfassung

Am Weltwirtschaftsforum 2019 in Davos kündigte der damalige japanische Premierminister Shinzō Abe an, eine internationale Ordnung für freien und auf gegenseitigem Vertrauen basierenden Datenfluss (*Data Free Flow with Trust*) schaffen zu wollen. Das ehrgeizige Projekt möchte mit dem Schlüsselbegriff „Vertrauen“ eine Grundlage schaffen, welche die Interoperabilität zwischen den vielfältigen und verschiedenartigen Datenschutzsystemen weltweit gewährleisten soll. Die Suche nach dieser Vertrauensbasis gestaltet sich aber schwieriger als erwartet, denn die Haltung der Staaten bzw. Regierungen gegenüber dem Schutz personenbezogener Daten ist von sehr unterschiedlichen Wertevorstellungen und Traditionen geprägt. Zudem wird die Interoperabilität im Sinne einer gleichberechtigten Kooperation dadurch erschwert, dass insbesondere die europäische Datenschutz-Grundverordnung Anspruch auf Geltung auch außerhalb der Grenzen des Europäischen Wirtschaftsraums (EWR) erhebt und mit ihren strengen Regelungen wenig Spielraum lässt für andere Systeme, was den Datentransfer aus dem EWR in einen Drittstaat betrifft.

Der Beitrag beleuchtet die Chancen und Hindernisse für einen *Data Free Flow with Trust* und kommt zum kritischen Schluss, dass derzeit vor allem noch die Hindernisse überwiegen und eine auf Vertrauen basierende Interoperabilität aktuell wenig Chancen hat, Realität zu werden.

1. Einleitung

Das Weltwirtschaftsforum in Davos war 2019 Schauplatz einer ambitionierten Ankündigung des japanischen Premierministers Shinzō Abe, wonach es an der Zeit sei, eine internationale Ordnung für freien und vertrauens-

würdigen Datenfluss (*Data Free Flow with Trust*) zu schaffen.[1] Die Ankündigung erfolgte zeitgleich mit der Annahme des Angemessenheitsbeschlusses für Japan unter Art. 45 der Datenschutz-Grundverordnung (DSGVO) durch die Europäische Kommission.

In diesem Vorhaben wird Vertrauen prominent als Schlüsselbegriff in den Mittelpunkt gestellt. Die beteiligten Staaten bzw. Regierungen wollen damit auf der Grundlage des Vertrauens nach langer Suche endlich einen Rahmen für einen globalen Datenfluss schaffen. Der Begriff Vertrauen bleibt aber unklar, und es stellt sich die Frage, ob er nicht eher politischer Rhetorik denn einer veritablen gemeinsamen und tragfähigen Basis entspricht.

Dieser Beitrag macht sich auf die Suche nach dem Vertrauen und geht der Frage nach, ob Vertrauen tatsächlich das entscheidende Element sein kann, das einen globalen Datenfluss legitimieren kann. Dies vor allem deshalb, weil die aktuellen Entwicklungen in der Frage des internationalen Datentransfers zwischen der EU und den USA nicht nur vertrauensfördernd sind. Insbesondere ist zu klären, wer wem vertrauen soll und auf welcher Grundlage dieses Vertrauen basieren kann.

Ähnliche Ungewissheit besteht im Hinblick auf den Begriff der (personenbezogenen) Daten. Der Begriff personenbezogen wird unterschiedlich ausgelegt, und selbst wenn sich der Data Free Flow with Trust aus Sicht der Initiatoren grundsätzlich nur auf nicht personenbezogene Daten beziehen soll, so stellen die unterschiedlichen Verständnisse dazu das Vorhaben auf eine weitere schwierige Probe. Was für die eine Seite personenbezogen ist, fällt für die andere Seite nicht darunter und das anzuwendende Regelwerk ändert sich je nach Perspektive. Erschwerend kommt hinzu, dass personenbezogene Daten in Europa zu einem Schlüsselbegriff für Selbstbestimmung und Privatsphäre geworden sind, sehr weit ausgelegt werden und auch grundrechtlich geschützt sind. Außerhalb Europas ist dies aber noch lange nicht zum Standard geworden, und es zeichnet sich hier auch aktuell kein Paradigmenwechsel ab.

1 *Abe*, Toward a New Era of "Hope-Driven Economy": The Prime Minister's Keynote Speech at the World Economic Forum Annual Meeting, 2019.

2. Der bisherige Weg zu einem Data Free Flow with Trust

Nach der Ankündigung in Davos 2019 wurde die Idee des Data Free Flow with Trust am G20 Gipfel im Sommer 2019 im japanischen Osaka im Rahmen des Themenschwerpunkts „Innovation" vertieft behandelt. Premierminister Abe unterstrich erneut die immense Bedeutung eines globalen Datenflusses für die zunehmende Digitalisierung, für die er internationale Regelungen insbesondere im Zusammenhang mit E-Commerce im Rahmen der WTO als wesentlich erachtete. Diese Bekenntnisse fanden ihren Niederschlag in den beiden Deklarationen des Gipfels, der „G20 Osaka Leaders' Declaration"[2] sowie der „Osaka Declaration on Digital Economy"[3].

Die G20 Osaka Leaders' Declaration sieht den globalen Datenfluss als große Chance für eine Steigerung der Produktivität und Innovation sowie die nachhaltige Entwicklung, anerkennt aber gleichzeitig, dass damit etliche Herausforderungen verbunden sind, darunter vor allem das Recht auf Privatsphäre und der Schutz personenbezogener Daten. Durch die Bewältigung dieser Herausforderungen soll der freie Datenfluss erleichtert und das Vertrauen der Konsumenten und der Wirtschaft gestärkt werden.[4] Privatsphäre, Datenschutz, geistiges Eigentum und Sicherheit sollen zudem mittels normativer Regelungen gewährleistet werden. Der explizite Hinweis auf den Datenschutz macht deutlich, dass personenbezogene Daten sehr wohl eine Rolle in dem Projekt spielen. Datenschutz wird in dem Dokument nicht nur als Herausforderung, sondern sogar als Grundlage des Vertrauens qualifiziert, wodurch der Ansatz weitgehend dem europäischen Kurs zu folgen scheint. Es ist aber freilich unklar, ob dies auch tatsächlich dem Bestreben der Initiatoren entspricht.

Als weitere, essentielle Voraussetzung wird zudem auf die Notwendigkeit der Interoperabilität der unterschiedlichen rechtlichen Rahmenbedingungen hingewiesen. Damit lässt sich als erster Anhaltspunkt für die Suche nach dem Vertrauen festhalten, dass gesetzlich normierter Datenschutz eine Grundlage für das Vertrauen der Konsumenten und der Wirtschaft bieten kann. Die Brücke zwischen den unterschiedlichen Ausprägungen der ge-

2 https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html

3 https://www.wto.org/english/news_e/news19_e/osaka_declration_on_digital_economy_e.pdf

4 Der Originaltext in Rz. 11 der G20 Osaka Leaders' Declaration lautet: "By continuing to address these challenges, we can further facilitate data free flow and strengthen consumer and business trust."

setzlichen Normierungen soll mittels Interoperabilität hergestellt werden und eine zusätzliche Vertrauensbasis bieten.

Das zweite Dokument, die Osaka Declaration on Digital Economy, wurde von 78 Staaten unterzeichnet und fokussiert gänzlich auf das große Potenzial des Datenflusses. Das Verständnis für die Rolle des Vertrauens vertieft sie nicht weiter. In der Erklärung wird vielmehr der Grundstein gelegt für den sogenannten „Osaka Track", der den Weg ebnen soll für Verhandlungen im Rahmen der WTO über globale Regelungen zum E-Commerce. Indien, Indonesien, Ägypten und Südafrika haben auf eine Unterzeichnung der Erklärung verzichtet.[5] Insbesondere Indien begründete dies damit, dass Daten als eine neue Form des Wohlstands als nationales Gut zu betrachten seien. Folglich sollten bei der Frage eines Data Free Flow with Trust auch die Interessen von Entwicklungsländern berücksichtigt werden, denn Daten dürften nicht nur dem Wirtschaftswachstum dienen, sondern auch der Entwicklung.[6] Verhandlungen zur Frage eines globalen Datenflusses müssten daher auf globaler Ebene stattfinden und sollten nicht in die Hände einer ausgewählten wirtschaftsorientierten Staatengruppe gelegt werden.

Im Januar 2023 folgten weitere Präzisierungen im Briefing Paper des Weltwirtschaftsforums zum Thema „Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows" (World Economic Forum 2023). In diesem Papier wird wiederholt festgehalten, dass die unterschiedlichen nationalen Regelungen zur Wirtschaftsentwicklung, zum Schutz von personenbezogenen Daten sowie zu Grundrechten und nationalen Sicherheitsbedenken zu einer geopolitischen Fragmentierung führen und den Data Free Flow vor große Herausforderungen stellen. Als zusätzliche Hürde werden die zunehmenden gesetzlichen Verpflichtungen zur lokalen Datenspeicherung in vielen Ländern identifiziert. Der Lösungsvorschlag, wie mit diesen vielfältigen nationalen Regelungen umzugehen ist, und vor allem, wie ihrem bedeutenden Einfluss auf den internationalen Datenfluss begegnet werden kann, wird auch hier in der Herstellung von Interoperabilität gesehen. Dabei wird erneut das Vertrauen ins Spiel gebracht, das Bestandteil dieser Interoperabilität sein soll.

Interoperabilität wird allgemein definiert als die „Fähigkeit unterschiedlicher Systeme, möglichst nahtlos zusammenzuarbeiten".[7] Um die Leistungsfähigkeit der Interoperabilität beurteilen zu können, braucht es aber zuerst

5 *Greenleaf*, Privacy Laws & Business International Report 2019, 18 (19).
6 Ibid.
7 Definition gemäß Duden online.

eine Auseinandersetzung mit den Systemen, für welche eine Zusammenarbeit gewährleistet werden soll. Je weiter deren zugrundeliegende Konzepte voneinander entfernt sind, desto schwieriger wird ihre nahtlose Zusammenarbeit und umso weniger Platz bleibt für das Vertrauen. Eines dieser grundlegenden Konzepte ist der Begriff der Daten und dabei vor allem die Unterscheidung und Definition von personenbezogenen und nicht-personenbezogenen Daten. Diese Grundsatzfrage wird in den unterschiedlichen Rechtskreisen sehr individuell beantwortet und hängt ab von den zugrundeliegenden Werten und Traditionen.

3. Der Begriff der Daten

In Davos betonte Premierminister Abe, dass seine Initiative des Data Free Flow with Trust selbstverständlich nur nicht-personenbezogene Daten umfassen sollte, während personenbezogene Daten, Daten in Bezug auf Geistiges Eigentum und nationale Geheimdienstinformationen eines besonderen Schutzes bedürften. Entgegen dieser scheinbar klaren Abgrenzung lassen die auf Abes Ankündigung folgenden Debatten und Dokumente keine eindeutige Schlussfolgerung zu, welche Arten von Daten tatsächlich von dem Projekt erfasst sein sollen. Die zahlreichen Hinweise auf Datenschutzbestimmungen, Privatsphäre und Grundrechte lassen eher vermuten, dass sich die Initiatoren sehr wohl bewusst sind, dass das Projekt nicht isoliert von den Fragen rund um personenbezogene Daten realisiert werden kann. Die große Frage betrifft vor allem die Unterscheidung zwischen personenbezogenen und nicht-personenbezogenen Daten bzw. die Definition dieser beiden Begriffe in den unterschiedlichen Rechtsordnungen. Das Briefing Paper des Weltwirtschaftsforums (World Economic Forum 2023) nennt die Unsicherheiten in Bezug auf die Definition des Begriffs „personenbezogene Daten" erstmals unmissverständlich als Hürde für den Data Free Flow with Trust, geht allerdings in Folge nicht näher darauf ein. Ohne dass es explizit in den Diskussionen zum Ausdruck gebracht wird, dürfte damit wohl vor allem die Diskrepanz zwischen der Europäischen Union (EU) bzw. dem Europäischen Wirtschaftsraum (EWR) und den USA, aber auch zahlreichen anderen Staaten außerhalb des EWR, gemeint sein.

Aber selbst wenn es gelingen sollte, sich auf einheitliche Definitionen zu einigen, wäre eine Trennung von personenbezogenen und nicht-personenbezogenen Daten für den Data Free Flow with Trust sowohl für den

privaten wie auch öffentlichen Sektor mit hohen bis sehr hohen Kosten verbunden und wohl kaum durchgängig zu erreichen.[8] Der Schutz der personenbezogenen Daten wird demnach immer ein wesentliches Element im Projekt bleiben.

3.1 Daten und Datenschutz in Europa

Im EWR wird nur die Kategorie der personenbezogenen Daten vom Datenschutzrecht, sprich der DSGVO erfasst.[9] Für nicht-personenbezogene Daten gilt eine eigene Verordnung.[10] Zur Gewährleistung eines besseren Verständnisses des nicht immer einfachen Verhältnisses zwischen den beiden Rechtstexten und Datenkategorien hat die Europäische Kommission Leitlinien erlassen.[11] Einer der Grundsätze lautet, dass in dem Falle, dass sich eine Trennung der Kategorien nicht herstellen lässt, die Bestimmungen für die personenbezogenen Daten auf das gesamte Datenkonglomerat Anwendung finden. Zusätzlich regeln weitere europäische Rechtstexte die Verarbeitung von (nicht-)personenbezogenen Daten im EWR bzw. der EU.[12]

8 *Casalini/López*, Trade Policy Paper 2019, 34.

9 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

10 Verordnung (EU) 2018/1807 des Europäischen Parlaments und des Rates vom 14. November 2018 über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union (ABl. L 303 vom 28.11.2018, S. 59).

11 Leitlinien zur Verordnung über einen Rahmen für den freien Verkehr nicht-personenbezogener Daten in der Europäischen Union vom 29. Mai 2019, COM(2019) 250 final.

12 So etwa die Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39); Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89); Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37).

Zur Beurteilung der Frage, welche Daten als personenbezogen gelten, hat zudem der Gerichtshof der Europäischen Union (EuGH) eine reichhaltige Rechtsprechung zur Verfügung gestellt, deren Tendenz klar dahin geht, im Zweifel Daten der Kategorie der personenbezogenen Daten zuzuordnen.[13] Getragen wird diese weite Auslegung vom europäischen Grundverständnis, dass Datenschutz ein eigenständiges Grundrecht ist.[14] In Nicht-EU-Staaten, die dem Europarat angehören, gilt, dass der Schutz personenbezogener Daten zumindest vom Recht auf Privatsphäre in Art. 8 der Europäischen Menschenrechtskonvention (EMRK) mitumfasst ist,[15] sofern die nationalen Verfassungen nicht ebenfalls ein explizites Grundrecht auf Datenschutz vorsehen.[16] Der Ehrgeiz der EU geht aber darüber noch hinaus, indem dieses sehr weitreichende Grundrechtsverständnis über die Grenzen der territorialen Jurisdiktion ausgeweitet wird und Anspruch erhebt auf eine extraterritoriale Anwendung, wenn bestimmte Anknüpfungspunkte zum EWR vorhanden sind. Diese folgen einerseits aus Art. 3 Abs. 2 DSGVO und andererseits aus Kapitel V DSGVO betreffend internationalen Daten-

13 Vgl. EuGH, *Patrick Breyer gegen Bundesrepublik Deutschland*, Urteil vom 19. Oktober 2016, C-582/14, ECLI:EU:C:2016:779; EuGH, *YS gegen Minister voor Immigratie, Integratie en Asiel und Minister voor Immigratie, Integratie en Asiel gegen M und S.*, Urteil vom 17. Juli 2014, C-141/12 und C-372/12, ECLI:EU:C:2014:2081. Vgl. näher dazu: *Zuiderveen Borgesius*, Eur. Data Prot. L. Rev. 2017; *Tracol*, Computer Law & Security Review 2015; *Lynskey*, Modern Law Review 2018; *Purtova*, Law, Innovation and Technology 2018; *Finck/Pallas*, International Data Privacy Law 2020.

14 Art. 8 der Charta der Grundrechte der Europäischen Union (ABl. C 326 vom 26.10.2012, S. 391) sieht den „Schutz personenbezogener Daten" als eigenständiges Grundrecht vor.

15 Art. 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten gewährleistet das Recht auf Achtung des Privat- und Familienlebens, das gemäss ständiger Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte auch das Recht auf Schutz personenbezogener Daten umfasst. Vgl. beispielsweise EGMR, *Drelon gegen Frankreich*, Urteil vom 8. September 2022, Nr. 3153/16 und 27758/18 oder EGMR, *Big Brother Watch and Others gegen das Vereinigte Königreich*, Urteil der Grossen Kammer vom 25. Mai 2021, Nr. 58170/13, 62322/14 and 24969/15.

16 So bestimmt etwa Art. 13 Abs. 2 der Bundesverfassung der Schweizerischen Eidgenossenschaft, dass jede Person Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten hat. Wenngleich Art. 13 selbst den Titel „Schutz der Privatsphäre" trägt, wird der Schutz vor Missbrauch der Daten nicht in den Schutz der Privatsphäre integriert, sondern als eigenes Schutzobjekt in Abs. 2 explizit erwähnt. Art. 35 der albanischen Verfassung sieht wiederum einen klaren Schutz personenbezogener Daten vor und hebt sogar explizit einige der Rechte der betroffenen Personen auf Verfassungsstufe. Ähnlich weitreichend regelt auch Art. 34 der armenischen Verfassung den Schutz personenbezogener Daten.

transfer. Im Zusammenhang mit Letzterem hatte der EuGH in seinem Schrems-II Urteil im Juli 2020 festgestellt, dass die Datenübermittlung in die USA in zwei Punkten aus europäischer Sicht nicht rechtskonform ist.[17] Dies ist zum einen der fehlende Rechtsschutz für die betroffenen Personen und zum anderen der Zugriff US-amerikanischer Behörden auf Daten aus dem EWR, welcher die (am europäischen Grundrechtsstandard gemessenen) Kriterien der Erforderlichkeit und Verhältnismäßigkeit nicht einhält.[18]

3.2 Daten und Datenschutz in den USA

Außerhalb Europas wird der Begriff „personenbezogene Daten" vor allem im Konsumentenrecht angesiedelt und nicht als Element verstanden, das grundrechtlichen Schutz genießt. Zugegeben, auch in Europa treten die beiden Rechtsbereiche in eine zunehmend enger werdende Beziehung,[19] wenngleich nur einem Bereich Grundrechtscharakter zugestanden wird, während der andere unter dem Titel Verbraucherschutz als Ziel in Art. 169 des Vertrags über die Arbeitsweise der Europäischen Union aufgelistet ist.

In den USA, wo Datenschutz nicht auf gesamtstaatlicher Ebene, sondern bislang nur in einzelnen Bundesstaaten gesetzlich geregelt ist, werden personenbezogene Daten und Konsumentenrecht als Einheit betrachtet.[20] Dies ist vor allem daran ersichtlich, dass es der Federal Trade Commission obliegt, Grundsätze für die faire Nutzung von personenbezogenen Daten auf Basis des Konsumentenrechts zu entwickeln.[21] Die mannigfachen gesetzlichen Regelungen in den USA bringen es zudem mit sich, dass einzelne Fragen unterschiedliche Lösungen erfahren, unter anderem die Definition des Begriffs „personenbezogene Daten".[22] Der Unterschied zeigt sich bei der Frage, ob sich personenbezogene Daten auf eine identifizierte oder direkt identifizierbare Person beziehen müssen, oder ob es sich auch um Daten handeln kann, die erst in Verbindung mit zusätzlichen Informationen, die

17 EuGH, *Data Protection Commissioner gegen Facebook Ireland Ltd, Maximillian Schrems,* Urteil vom 16. Juli 2020, C-311/18, ECLI:EU:C:2020:559.

18 Für eine detaillierte Analyse dieser Entscheidung vgl. etwa: *Sury,* Informatik Spektrum 2020, 354; *Heper*, Jahrbuch für Vergleichende Staats-und Rechtswissenschaften 2022, 125.

19 *Helberger* u.a., Common Market Law Review 2017, 1427.

20 *Solove/Hartzog*, Columbia Law Review 2014, 584; *Schwartz/Solove*, California Law Review 2014, 877.

21 *Rustad/Koenig*, Florida Law Review 2019, 365 (381).

22 *Schwartz/Solove*, California Law Review 2014, 877 (888f.).

eventuell nur bei einer dritten Stelle verfügbar sind, die Identifizierung einer natürlichen Person ermöglichen. Von wenigen Ausnahmen abgesehen ist der erste Ansatz in den USA vorherrschend.[23] Daraus ergeben sich Diskrepanzen zwischen der DSGVO und amerikanischem Recht vor allem bei den Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die ein Gerät oder Software-Anwendungen und Tools oder Protokolle liefern, oder sonstigen Kennungen wie Funkfrequenzkennzeichnungen. Diese können gemäß Erwägungsgrund 30 der DSGVO „Spuren" hinterlassen, die letztlich in Kombination mit anderen Kennungen und Informationen dazu dienen können, Personen zu identifizieren. Der California Consumer Privacy Act (CCPA) sowie der California Privacy Rights Act (CPRA), als erstes umfassendes US-Gesetz in Bezug auf die Verarbeitung personenbezogener Daten, erkennen zwar Online-Kennungen ebenso wie Informationen, welche durch die Interaktion mit dem Internet oder einem anderen elektronischen Netzwerk generiert werden, als personenbezogene Daten an, wenn diese Information „identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[24] Weder diese Legaldefinition noch die Rechtsprechung in den USA beantworten aber die Frage, ob damit eine Online-Kennung, vor allem die IP-Adresse, eindeutig als personenbezogenes Datum eingestuft wird oder nicht.[25] Anders der EuGH, der hier eine klare Meinung vertritt und IP-Adressen einschließlich dynamischer IP-Adressen als personenbezogene Daten qualifiziert.[26]

Die Debatten rund um Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die Geräte oder Software-Anwendungen und -Tools oder Protokolle liefern und die Frage von deren Personenbezug haben einen erheblichen Einfluss auf den internationalen Datentransfer. Nachdem diese Daten aus EWR-Sicht der DSGVO unterfallen, wird aktuell – nach dem Wegfall des Angemessenheitsbeschlusses für die USA – der Nutzung unterschiedlicher Tools wie Google Analytics[27] etc. im EWR die unkomplizier-

23 Zu den Ausnahmen zählt Children's Online Privacy Protection Rule (COPPA), 78 Fed. Reg. 3972 (Jan. 17, 2013). Eventuell lässt sich der hier gewählte strengere Schutz damit begründen, dass es in dem Gesetz explizit um den Schutz von Kindern geht.

24 Cal. Civ. Code § 1798.140 (v).

25 *Zetoony*, Loyola University Chicago Journal of Regulatory Compliance 2022, 1 (4).

26 EuGH, *Patrick Breyer gegen Bundesrepublik Deutschland*, Urteil vom 19. Oktober 2016, C-582/14, ECLI:EU:C:2016:779.

27 Das Beispiel von Google Analytics erlangte deshalb besondere Bedeutung, als die Organisation NOYB nach dem EuGH-Urteil Schrems II eine Reihe von Beschwerden

teste Rechtsgrundlage entzogen. Die Hürden, einen alternativen Weg für Datenübermittlungen in die USA zu finden, sind in der Praxis so groß, dass der transatlantische Datentransfer einen bedeutenden Rückgang erfahren müsste, würden alle EWR Datenexporteure der strengen Auslegung des EuGH Folge zu leisten versuchen.

Aber nicht nur bei der Frage, was unter personenbezogenen Daten zu verstehen ist, gibt es Unterschiede. Ebenso finden sich unterschiedliche Sichtweisen in Bezug auf die zu schützenden Individuen und die verantwortlichen Stellen. Unter der DSGVO sind dies sämtliche natürliche Personen im EWR, während die einschlägigen US-Gesetze die Betonung auf Konsumenten legen. Auch wenn der Begriff Konsument im jeweiligen Gesetzestext dann konkret mit „Bürger" eines bestimmten Staates definiert wird und damit zumindest im Wortlaut dem EWR-System angeglichen wird, hat der Grundgedanke des „Konsumentenschutzes" weitere Auswirkungen, nämlich auf die verantwortlichen Stellen. Nachdem Datenschutz gemäß diesem Verständnis nur Konsumenten als Schutzobjekte hat, werden die verantwortlichen Stellen auf Unternehmen eingeschränkt. Vor allem Behörden werden nicht verpflichtet. Im Gegenteil, ihnen kommen sogar weitreichende Befugnisse zu, auf Daten von in- und ausländischen Bürgern zuzugreifen. Aber auch bei den Unternehmen gelten die Datenschutzbestimmungen nicht umfassend, denn auch hier bestehen ergänzende Kriterien, etwa die Bedingung im CCPA/CRPA, dass es sich um Unternehmen handeln muss, die einen bestimmten Mindestumsatz erreichen und die jährlich Daten von mindestens 100'000 Konsumenten oder Haushalten kaufen, erhalten, verkaufen oder teilen, oder einen bestimmten Prozentsatz des Umsatzes mit dem Verkauf oder Teilen von Daten generieren.[28] Im Vergleich zu diesem stark sektoral ausgeprägten Datenschutzsystem der USA konnten sich bislang die Befürworter eines gesamtstaatlichen Datenschutzgesetzes (noch) nicht durchsetzen.

3.3 Daten und Datenschutz im asiatisch-pazifischen Raum

Die USA ist keine Ausnahme, was die fehlende Verbindung von Datenschutz zu den Grundrechten betrifft. Auch wenn es Ausnahmen wie etwa

gemäss Art. 77 DSGVO einreichte, die fast gleichlautend entschieden wurden und die Rechtsgrundlage für die Nutzung dieses Tools in Frage stellten.

28 Ähnlich auch der Virginia Consumer Data Protection Act (VCDPA), der etwas niedrigere Hürden ansetzt und das Mindestmaß mit 25'000 Konsumenten bestimmt.

Japan gibt, werden in zahlreichen Staaten im asiatisch-pazifischen Raum Daten häufig als „Beiwerk" von gehandelten Waren oder Dienstleistungen betrachtet. Ähnlich wie in den US-Gesetzen werden auch hier Definitionen von personenbezogenen Daten sehr offen formuliert. So folgt etwa aus dem südkoreanischen Gesetz, dass personenbezogene Daten nicht notwendigerweise Online-Kennungen, Geräte- oder verhaltensbezogene Informationen, Informationen zum Surfverhalten sowie User-Interaktionen (advertising information, inference information, Internet browsing and search records, and information about Internet websites/ application programs/advertisements and user interactions) umfassen.[29] Ebenso zeigt sich hier die Tendenz, Pseudonymisierung in die Nähe der Anonymisierung zu bringen und somit zumindest teilweise aus dem Bereich der personenbezogenen Daten auszuklammern.[30] Ähnliche Tendenzen sind auch in der 2020 erfolgten Reform des japanischen Datenschutzgesetzes sichtbar. Die neue Kategorie von „in pseudonymisierter Form verarbeiteten Daten" bleibt zwar weiterhin Teil der personenbezogenen Daten, wird aber von einzelnen Betroffenenrechten ausgenommen.[31] Etliche Gesetze erlauben den Unternehmen, diese Daten etwa für interne Zwecke, wie Unternehmensanalysen oder die Entwicklung von Berechnungsmodellen zu verwenden. Auch sind pseudonymisierte Daten nicht verpflichtend zu löschen, selbst wenn die personenbezogenen Daten für den ursprünglich erhobenen Zweck nicht mehr erforderlich sind. Für zukünftige statistische Analysen dürfen sie weiterhin gespeichert bleiben. Die Begriffe Unternehmensanalysen, Statistiken oder Berechnungsmodelle sind vage gehalten und gewinnorientierte Zwecke scheinen dabei nicht überall ausgeschlossen.

Andererseits haben sich Indien, China, Malaysia, Vietnam und zahlreiche weitere Staaten für verstärkte Verpflichtungen zur lokalen Datenspeicherung ausgesprochen, die vor allem den E-Commerce bzw. Finanzbereich betreffen und etwa Zahlungsdienstleister verpflichten, die Daten von Kunden aus den jeweiligen Staaten national zu speichern.[32] Dies stößt wiederum vor allem bei den USA auf großes Unverständnis.

29 *Park* u.a., Asian Journal of Innovation and Policy 2020, 339 (353).

30 Ibid., 339 (342); vgl. auch die diesbezüglichen Bestimmungen im Angemessenheitsbeschluss für Südkorea, Rz. 82.

31 *Joo/Kwon*, Government Information Quarterly 2023, 1 (5f.); vgl. auch den Angemessenheitsbeschluss für Japan, Rz. 30-32.

32 Vgl. etwa Reserve Bank of India, Statement on Developmental and Regulatory Policies vom 5. April 2018, wo unter Pkt. 4 folgende Anweisung erfolgt: „It is observed that at present only certain payment system operators and their outsourcing

In Bezug auf das Grundverständnis des Schutzes personenbezogener Daten lautet das Argument häufig, dass „asiatische Werte" nicht vereinbar seien mit dem westlichen Grundrechtsverständnis, das bisweilen aus asiatischer Sicht sogar als eine moderne Erweiterung des Imperialismus betrachtet wird.[33] Aus Grundrechtsdokumenten, politischen Debatten und auch der Literatur lässt sich ableiten, dass das Individuum gegenüber dem Kollektiv in Asien oft eine nachrangige Bedeutung einnimmt. Damit wird auch erklärt, warum in der politischen Agenda vieler asiatischer Staaten wirtschaftliche Entwicklung und politische Stabilität (in welcher Form diese auch immer gewährleistet wird) höher gewertet werden als zivile und politische Rechte einschließlich des Rechts auf Privatsphäre und des Schutzes personenbezogener Daten.[34]

Auch wenn diese Aussagen einen Hang zum Klischee haben und der Vereinfachung dienen, sind sie in Bezug auf die Wertung des Schutzes personenbezogener Daten nicht ganz von der Hand zu weisen und erklären viele staatliche Entscheidungen, aber auch die Haltung vieler Menschen in Staaten wie beispielsweise Indien in Bezug auf die Verarbeitung ihrer personenbezogenen Daten.[35] Sie lassen deshalb auch Rückschlüsse auf das unterschiedliche Verständnis des im Rahmen des Data Free Flow with Trust aufgeworfene Konzept des Vertrauens zu. Europa hat nach dem zweiten Weltkrieg unmissverständlich den Weg eingeschlagen, dass Grundrechte und entsprechende Mechanismen zu ihrer Durchsetzung die Grundlage eines friedlichen Zusammenlebens sind. Entsprechend vertrauen die Menschen darauf, dass durch diese Mechanismen, die auf staatlicher wie internationaler bzw. regionaler Ebene angesiedelt sind, eine Kontrolle gegenüber

partners store the payment system data either partly or completely in the country. In order to have unfettered access to all payment data for supervisory purposes, it has been decided that all payment system operators will ensure that data related to payment systems operated by them are stored only inside the country within a period of 6 months". URL: https://rbidocs.rbi.org.in/rdocs/PressRelease/PDFs/PR264270719E5CB28249D7BCE07C5B3196C904.PDF. Vgl. allgemein zur zunehmenden Tendenz der Datenlokalisierung: *Basu*, The retreat of the data localization brigade: India, Indonesia and Vietnam.

33 Vgl. *Freeman*, The Pacific Review 1996, 352 (364); *Rustad/Koenig*, Florida Law Review 2019, 365 (387).

34 Vgl. unter anderem *Ghai*, Hong Kong Law Journal 1993; *Chan*, in: Tuck-Hong (Hrsg.), Human Rights and International Relations in the Asia Pacific Region, 2017, 25 (35).

35 *Chatterjee*, International Journal of Law and Management 2019, (170) 177.

dem Staat und zunehmend auch gegenüber nicht-staatlichen Akteuren entstanden ist.

Asiatische Wertvorstellungen sind hingegen stark vom Kommunitarismus geprägt, dem der westliche Individualismus gegenübersteht. Die individuelle Freiheit, Privatsphäre und (informationelle) Selbstbestimmung, die Grundlage des europäischen Datenschutzes ist, trifft bei vielen Regierungen im asiatischen Raum oft auf Unverständnis.[36] Und selbst wenn diese oder ähnliche Konzepte vorhanden sind, wie etwa in Japan, ist ihr Verständnis nicht unbedingt identisch mit demjenigen in Europa.[37]

3.4 Sonderfall China hinsichtlich Daten und Datenschutz

In der staatlichen *State Informatization Development Strategy 2006–2020* betont China die immense Bedeutung von Daten, insbesondere deren Rolle als zentraler Produktionsfaktor und Garant für den Wohlstand der Gesellschaft. Die nationale Big Data-Strategie steht darin ebenso wie die staatlich organisierten Big Data-Zentren im Mittelpunkt. Die Grund- und Freiheitsrechte der Bürgerinnen und Bürger sollen demgegenüber einen „realistischen" Schutz erhalten und der Schutz personenbezogener Daten gestärkt werden. Eine gesetzliche Regelung zum Datenschutz findet sich entsprechend in dem am 1. November 2021 in Kraft getretenen *Personal Information Protection Law* (PIPL). Die darin enthaltene Definition personenbezogener Daten basiert auf der Vorlage der DSGVO und umfasst „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen lassen und in elektronischem oder anderem Format gespeichert werden".[38] Einer der Hauptunterschiede zur DSGVO liegt jedoch in den strengen Vorschriften zur verpflichtenden Datenspeicherung in China. Genaue Kriterien oder Vorgaben dafür finden sich im Gesetz allerdings nicht. Beachtlich sind auch die Einschränkungen und Hürden für den Datentransfer außerhalb Chinas. Trotz der stellenweisen Orientierung am Text der DSGVO wurde der entsprechende Regelungsgehalt der DSGVO nicht übernommen. Insgesamt ist festzustellen, dass China mit dem neuen Datenschutzgesetz trotz formeller und teilweise inhaltlicher Anlehnung an das DSGVO-Modell keineswegs einem Grundrecht zur Durch-

36 *de Vries/Meijknecht*, International Journal on Minority and Group Rights 2010, 75 (86).
37 *Beer*, Asian Survey, 437 (439f.).
38 *Wang Han/Munir*, European Data Protection Law Review 2018, 535; *Geller*, GRUR International 2020, 1191 (1193).

setzung verhelfen will, sondern auf soziale Kontrolle, gesamtgesellschaftliche Interessen und natürlich die nationale Sicherheit als zu erreichende Ziele setzt.[39]

Dies bringt ein chinesischer Autor folgendermaßen zum Ausdruck: „Asian values [put] emphasis on a quest for consensual solutions, communitarianism rather than individualism, social order and harmony, respect for elders, discipline, a paternalistic state, and the primary role of government in economic development."[40]

3.5 Zwischenfazit

Die Beispiele der unterschiedlichen staatlichen und regionalen Lösungsansätze für den Umgang mit personenbezogenen Daten könnten noch beliebig fortgesetzt werden, was aber den Umfang dieses Beitrags sprengen würde. Die genannten Beispiele reichen aus, um auf ein grundlegendes Problem hinzuweisen. Der Umgang mit Daten ist weit mehr als eine Frage der Gesetzgebung, es geht um wesentlich tiefer liegende gesellschaftliche Konzepte und Werte, auf denen die jeweiligen rechtlichen Lösungsansätze beruhen. Im Grunde geht es um die Frage, ob personenbezogene Daten als Werte und Interessen zu qualifizieren sind, welche durch die Grund- und Menschenrechte geschützt werden sollen, oder ob sie im Dienst der Gemeinschaft, der Wirtschaft und/oder der nationalen Sicherheit stehen. Und damit geht es letztlich auch um die Frage, worauf Menschen wirklich vertrauen, wenn es um die Verarbeitung bzw. Übermittlung ihrer Daten geht.

In Europa steht das Menschenrecht auf Privatsphäre bzw. des Schutzes personenbezogener Daten im Mittelpunkt der Frage der Verarbeitung von Daten. Damit einhergehend ist die weite Auslegung des Begriffs „personenbezogene Daten" und die vor allem vom EuGH festgelegte, niedrige Schwelle für die Identifizierbarkeit von Personen. Hinzu kommt, dass sowohl der EuGH[41] als auch der Europäische Gerichtshof für Menschenrechte (EGMR)[42] dem Zugang zu einer gerichtlichen Überprüfung der Rechtmäßigkeit einer Datenverarbeitung einen immens hohen Stellenwert

39 *Geller*, GRUR International 2020, 1191 (1192).

40 Zitiert in *Tomuschat*, Human Rights. Between Idealism and Realism 2003, 70.

41 EuGH, *Schrems II*, Rz. 95.

42 EGMR, *Roman Zakharov gegen Russland,* Urteil der Grossen Kammer vom 4. Dezember 2015, Nr. 47143/06, Rz. 234: "There is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the

einräumen. Ebenso zeigen die beiden Gerichtshöfe auf, dass sie für einen Zugriff staatlicher Stellen auf personenbezogene Daten strenge Maßstäbe ansetzen und dabei vor allem die Erforderlichkeit und Verhältnismäßigkeit genau überprüfen und auch von Drittstaaten einfordern, soweit Daten aus dem EWR betroffen sind.

Ein zweiter Ansatz in Bezug auf den Schutz personenbezogener Daten, der vor allem in den USA dominiert, ist die starke Verknüpfung der Verarbeitung von Daten mit der Wirtschaft und den Unternehmen. Vereinfacht dargestellt, sind Daten bei diesem Ansatz Teil des Trade-offs einer Konsumentenbeziehung und Konsumenten sollen selbst entscheiden, welchen Wert sie ihren personenbezogenen Daten dabei zumessen. Daten nehmen damit die Rolle eines Wirtschaftsgutes ein, das ebenso wie Produkte und Dienstleistungen Teil des freien Marktes ist. Auf der anderen Seite stehen US-Behörden weitreichende Möglichkeiten für einen Zugriff auf personenbezogene Daten für Zwecke der nationalen Sicherheit zur Verfügung.

In Asien hingegen lässt sich ein anderer Ansatz finden. In der politischen Agenda der meisten asiatischen Regierungen werden die wirtschaftliche Entwicklung, das Interesse der Gemeinschaft und die politische Stabilität sowie die nationale Sicherheit höher gewertet als zivile und politische Rechte des Individuums. Neben der politischen Agenda spielt hier auch die Wertvorstellung der Gesellschaft, in der die Gemeinschaft einen hohen Stellenwert einnimmt, eine Rolle und lässt somit das Recht des Individuums auf Privatsphäre in den Hintergrund treten. Nicht eindeutig geklärt ist damit aber die Frage, ob die Menschen bezüglich ihrer personenbezogenen Daten entgegen der hohen Wertschätzung der Gemeinschaft doch einen erweiterten Schutz als wünschenswert erachten.

Eine zusätzliche Komponente wurde von Indien ins Spiel gebracht, das dem Osaka Track unter anderem mit der Begründung ferngeblieben ist, dass Daten als eine neue Form des Wohlstands und entsprechend als nationales Gut zu betrachten seien. Folglich sollten bei der Frage eines Free Flow of Data auch die bislang vernachlässigten Interessen von Entwicklungsländern berücksichtigt werden.[43]

---

measures taken without his or her knowledge and thus able to challenge their legality retrospectively … or, in the alternative, unless any person who suspects that his or her communications are being or have been intercepted can apply to courts, so that the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his communications".

43 *Greenleaf*, Privacy Laws & Business International Report 2019.

Schließlich sind auch noch jene Staaten in die Debatte miteinzubeziehen, denen Datenschutzbestimmungen ganz oder fast gänzlich unbekannt sind, wie etwa Indonesien, Pakistan oder viele Staaten im mittleren Osten und in Ozeanien. Auch wenn internationale Datentransfers aus Sicht dieser Staaten unproblematisch sind, findet nur sehr wenig Datenimport in diese Länder statt.

Die aufgezeigten Ansätze sind in den meisten Fällen nicht ausschließlich aufzufinden, sondern oft in Kombination vorhanden. Viele staatliche Lösungsansätze befinden sich auch irgendwo dazwischen, so kann der australische Ansatz beispielsweise zwischen Europa und den USA angesiedelt werden.

4. Interoperabilität der Systeme

Das Ziel der Interoperabilität ist es, zu gewährleisten, dass unterschiedliche Systeme nahtlos zusammenarbeiten und, im Falle des Data Free Flow with Trust, Mechanismen geschaffen werden, die es erlauben, dass „systems, regulatory frameworks, technologies or standards interact, communicate and function with those of other operators or countries".[44] Der Osaka Track will diese Interoperabilität vor allem im Bereich des E-Commerce sicherstellen.

Zu den größten Hürden, die der Interoperabilitäts-Mechanismus neben der Frage seiner generellen Anwendbarkeit abhängig von der Definition der personenbezogenen Daten überbrücken muss, gehören die in den nationalen bzw. regionalen Datenschutzgesetzen vorzufindenden Bestimmungen für den Datentransfer außerhalb der eigenen Jurisdiktion sowie Verpflichtungen zur lokalen Datenspeicherung. Für ersteres stellt zweifelsfrei die DSGVO die beträchtlichste Herausforderung dar, denn mit ihrem Kapitel V zur Übermittlung personenbezogener Daten in Drittländer oder an internationale Organisationen hat sie ein eigenes, sehr straffes Regime geschaffen, mit dem sie das Schutzniveau der Daten auch in Drittstaaten angemessen aufrechterhalten will. Mit dieser spezifischen Regelung macht Europa klar, dass der internationale Transfer von Daten als autonomes Prozedere zu werten ist, das zwar einen praktischen Bezug haben kann zum Austausch von Wirtschaftsgütern, aber nicht dessen Regelungen folgt. Obwohl Kapitel V DSGVO prima facie keine extraterritoriale Anwendung der DSGVO zum Ziel hat, sondern nur Datenexporteuren im EWR Aufla-

44 *Casalini/López*, Trade Policy Paper 2019, 6.

gen für ihren Datentransfer in einen Drittstaat auferlegt, hat das System eine weitreichende Wirkung auf Drittstaaten und deren Rechtsordnungen, wie die aktuellen Diskussionen rund um die Ausgestaltung des EU-US Data Privacy Framework als Nachfolger des EU-US Privacy-Shields zeigen. Gemäß EuGH sind nämlich an einen Datentransfer unter anderem die Bedingungen geknüpft, dass einerseits betroffenen Bürgern in den jeweiligen Drittstaaten die Möglichkeit einer gerichtlichen Überprüfung der Datenverarbeitung zur Verfügung steht und andererseits der Zugriff staatlicher Behörden auf diese Daten nur in verhältnismäßigem und erforderlichem Ausmaß erfolgt – gemessen aus europäischer Sicht selbstverständlich am europäischen Grundrechtsstandard.

Angesichts dieses engen Korsetts stellt sich die Frage, ob die DSGVO überhaupt Platz lässt für eine Interoperabilität im Sinne einer *Kooperation* mit anderen Rechtssystemen oder ob sie vielmehr den (nicht verhandelbaren) Maßstab vorgibt, der erreicht werden muss, wenn Datenexporteure in EWR-Staaten in einen Free Flow of Data involviert sind. Bereits heute sieht sich der europäische Maßstab bisweilen der Kritik eines neuen „Imperialismus" ausgesetzt.[45] Diese Kritik wendet sich insbesondere gegen den Trend, dass zahleiche Staaten außerhalb des EWR-Raums die DSGVO als Modell für ihre nationalen Datenschutzgesetze verwenden, ohne dass dies immer ihren Rechtstraditionen entspricht.

Zwischenzeitlich wurde 14 Staaten von der Europäischen Kommission mit einem Angemessenheitsbeschluss attestiert, dass sie über ein dem EWR-Standard angemessenes Datenschutzniveau verfügen. Art. 45 sowie Erwägungsgrund 104 der DSGVO geben die Kriterien für den Angemessenheitsbeschluss vor und machen kein Geheimnis aus ihrer Orientierung am europäischen bzw. internationalen Menschenrechtsstandard. Ebenfalls zu berücksichtigen sind Vorschriften über die öffentliche Sicherheit, die Landesverteidigung und die nationale Sicherheit sowie die öffentliche Ordnung und das Strafrecht. Diese Bereiche sind gemäß Art. 2 Abs. 2 DSGVO nicht einmal vom Anwendungsbereich der DSGVO umfasst, finden aber trotzdem Beachtung, wenn es um die Frage der Angemessenheit von Drittstaaten geht. Zudem ist nicht zu vergessen, dass auch die Richtlinie (EU) 2016/680 für den Datenschutz bei Polizei und Justiz die Möglichkeit eines

45 *Fabbrini/Celeste*, German Law Journal 2020, 55 (56). In dieselbe Richtung geht die Aussage: „Be ready for the Brussels Effect — It's coming to Data and AI" - vgl. dazu *Rzeszucinski*, Forbes v. 26. Mai 2022.

Angemessenheitsbeschlusses enthält. 2021 erhielt Großbritannien als erster Drittstaat einen solchen Angemessenheitsbeschluss.

Das Beispiel der aktuellen Verhandlungen zum EU-US Data Privacy Framework wirft die Frage auf, ob der mit dem Angemessenheitsbeschluss zu regelnde Datenfluss zwischen den beiden Jurisdiktionen tatsächlich als „nahtlose" Kooperation zweier Systeme gedacht ist, oder die Vorgaben EU-seitig gemacht werden. Grundbedingung für den Datentransfer ist gemäß Entwurf des Angemessenheitsbeschlusses die Gewährleistung von „privacy rights and their effective implementation, supervision and enforcement"[46] sowie von „rules intended to limit interferences with the fundamental rights of the persons whose data is transferred from the Union, which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security, and provides effective legal protection against interferences of that kind".[47] Auch die Frage der Definition personenbezogener Daten (einschließlich besonderer Kategorien) wird im Sinne Europas gelöst, indem die Definition der DSGVO übernommen wird und auch pseudonymisierte Daten für Forschungszwecke mitumfasst sind, selbst wenn der Schlüssel in Europa verbleibt.[48] Ebenso ist die Zweckbestimmung des Art. 5 Abs. 1 Bst. b DSGVO Teil der Bedingungen[49] und konterkariert somit die allgemein zu beobachtende Tendenz, über die Pseudonymisierung einzelne Datenschutzbestimmungen wie die Zweckbestimmung und vor allem die Betroffenenrechte einzuschränken.

Europa macht damit zweifelsfrei die strengsten Vorgaben, aber auch andere Jurisdiktionen, wie Australien, sehen Bedingungen für den Datentransfer in Drittstaaten vor. China hingegen versucht, mit Verpflichtungen zur Speicherung im Inland, wofür als Gründe die Cyberspace Sovereignty und Netzwerksicherheit angegeben werden, Datentransfers in Drittstaaten stark zu reduzieren.[50] Selbst in Fällen, wo ein internationaler Datentransfer gesetzlich nicht ausgeschlossen ist, ist ein solcher Transfer von zahlreichen, meist schwierig zu erfüllenden Voraussetzungen abhängig, für die zudem wenig Rechtssicherheit besteht.

46 Draft Commission Implementing Decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework, Dezember 2022, Rz. 4.
47 Ibid., Rz. 4.
48 Ibid., Rz. 11.
49 Ibid., Rz. 14.
50 *Geller*, GRUR International 2020, 1191 (1200); *Feng*, Asia Pacific Law Review 2019, 62 (72).

Die aktuelle Situation zeigt, dass es zumindest in naher Zukunft wohl kaum möglich sein wird, im Dialog systemübergreifende Gemeinsamkeiten zu identifizieren, die schließlich als tragfähige Basis bzw. Interoperabilitäts-Mechanismus für ein globales digitales Ökosystem zum Einsatz kommen können. Neben dem Dialog fehlt es aktuell auch an einer internationalen Institution, die für die Etablierung der Interoperabilität verantwortlich zeichnen könnte. Die Bemühungen auf Ebene der WTO und der OECD gehen kaum über Leitlinien oder Briefing Papers hinaus. Praktische Schritte setzt, wie ausgeführt, lediglich die EU, allerdings nicht im Dialog und nicht immer mit einer Suche nach Gemeinsamkeiten und nahtloser Zusammenarbeit, sondern mit klaren Bedingungen, unter denen ein internationaler Datentransfer aus ihrer Sicht, und gemessen am europäischen Grundrechtsstandard, rechtmäßig erfolgt. Immerhin erlauben so aktuell 30 EWR-Staaten und 14 Drittstaaten mit Angemessenheitsbeschluss einen Data Free Flow with Trust in einem Datenraum, der ein Viertel der Staaten weltweit umfasst. Prozentual betrachtet sind dies ca. 820 Millionen Menschen, allerdings nur gut 10% der Weltbevölkerung. Darüber hinaus wird es aber schwierig, vor allem auch mit Blick auf die zunehmenden gesetzlichen Verpflichtungen zur lokalen Datenspeicherung.

5. Fazit zur Suche nach dem Vertrauen

Diese Entwicklungen lassen darauf schließen, dass Interoperabilität vor schwierigen Herausforderungen steht. Somit fällt sie auch als Grundlage für das Vertrauen in ungehinderte internationale Datentransfers weg. Dies ist bedauerlich, denn die Grundidee ist nicht zu unterschätzen, kann Vertrauen im weitesten Sinn doch einen wesentlichen Beitrag zum Gelingen internationaler Kooperation leisten.[51] Zurzeit allerdings scheint es eher so zu sein, dass zwar die meisten Regierungen mit dem Element Vertrauen argumentieren und den Menschen die jeweiligen nationalen oder regionalen Lösungsansätze als Vertrauensbasis anbieten, was in vielen Fällen auch recht gut gelingt. So vertrauen Menschen in Europa auf den Grundrechtsschutz. In den USA vertrauen sie auf den freien Markt, auf dem sie ihre Daten als handelbares Gut in eine Kundenbeziehung einbringen. Im asiatisch-pazifischen Raum vertrauen sie darauf, dass ihre Daten einem höheren Gut, vor allem der Gemeinschaft, dem Wirtschaftswachstum und

51 *Brugger* u.a., Zeitschrift für Internationale Beziehungen 2013.

der nationalen Sicherheit dienen. In China speziell werden Daten vertrauensvoll dem Staat überlassen, der für gesellschaftliches Wohlergehen und soziale und nationale Sicherheit und Kontrolle sorgen soll. In Entwicklungsländern schließlich wird darauf vertraut, dass Daten der Entwicklung dienen. Nicht vergessen werden darf bei dieser Kategorisierung, dass die einzelnen Systeme natürlich unterschiedliche Ausprägungen erfahren und Elemente kombinieren können. Auch ist das Vertrauen der Bevölkerung nicht immer vollumfänglich zu gewinnen, und es gibt sowohl in Europa Stimmen, die bereit sind, ihre Daten als Wirtschaftsgut einzubringen wie es in Asien und den USA diejenigen gibt, die dem Weg, den die Regierungen beschreiten, kritisch gegenüberstehen.

Für einen Data Free Flow (with Trust) scheint Vertrauen allerdings derzeitig nicht wirklich eine tragfähige Basis zu sein. Der europäische Ansatz in dieser Frage ist eindeutig und in einer Anpassung des nationalen Rechtsrahmens der Drittstaaten an die europäische Lösung zu finden. Vertrauen muss damit allerdings nicht notwendigerweise verbunden sein, kann es aber natürlich werden, wenn die Drittstaaten mit der Anpassung an die DSGVO auch das Vertrauen in den Grundrechtsschutz übernehmen. Dies scheint im Moment allerdings eher unrealistisch und somit wird der Data Free Flow wohl noch eine längere Zeit eine Gemengelage unterschiedlicher Lösungsansätze bleiben. Abzuwarten bleibt außerdem, welche Rolle künftig die Konvention 108+ des Europarates in dieser Frage spielen wird. Auch sie hat ihre Wurzeln in der europäischen Grundrechtstradition, ist aber explizit auch offen für Drittstaaten außerhalb Europas und bietet Hoffnung für eine neue grenzüberschreitende Vertrauensbasis.

Literatur

Abe, Shinzō (2020): Toward a New Era of "Hope-Driven Economy": the Prime Minister's Keynote Speech at the World Economic Forum Annual Meeting. URL: https://japan.kantei.go.jp/98_abe/statement/201901/_00003.html (besucht am 16. 02. 2023).

Basu, Arindrajit (2020): The retreat of the data localization brigade: India, Indonesia and Vietnam. *The Diplomat* vom 10. Jan. 2020. URL: https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/ (besucht am 19. 02. 2023).

Beer, Lawrence W. (1981) Group Rights and Individual Rights in Japan. *Asian Survey* 21(4), S. 437–53.

Brugger, Philipp; Hasenclever, Andreas; Kasten, Lukas (2013): Vertrauen Lohnt Sich: Über Gegenstand und Potential eines vernachlässigten Konzepts in den internationalen Beziehungen. *Zeitschrift für Internationale Beziehungen*, 20(2), S. 65-104.

Casalini, Francesca und López, González Javier (2019): Trade and Cross-Border Data Flows. *OECD Trade Policy Papers*, No. 220, Paris: OECD Publishing.

Chan, Joseph (1995): The Asian Challenge to Universal Human Rights: A Philosophical Appraisal. In: Tuck-Hong Tang, James (Hrsg.): *Human Rights and International Relations in the Asia Pacific Region*. London: Pinter, S. 25-38.

Chatterjee, Sheshadri (2019): Is data privacy a fundamental right in India? An analysis and recommendations from policy and legal perspective. *International Journal of Law and Management*, 61(1), S. 170-190.

de Vries, Byung Sook und Meijknecht, Anna (2010): Is There a Place for Minorities' and Indigenous Peoples' Rights within ASEAN?: Asian Values, ASEAN Values and the Protection of Southeast Asian Minorities and Indigenous Peoples. *International Journal on Minority and Group Rights*, 17(1), S. 75-110.

Fabbrini, Federico und Celeste, Edoardo (2020): The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders. *German Law Journal*, 21(S1), S. 55-65.

Feng, Yang (2019): The future of China's personal data protection law: challenges and prospects. *Asia Pacific Law Review*, 27(1), S. 62-82.

Finck, Michèle und Pallas, Frank (2020): They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), S. 11-36.

Freeman, Michael (1996): Human rights, democracy and 'Asian values'. *The Pacific Review*, 9(3), S. 352-366.

Geller, Anja (2020): How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective. *GRUR International*, 69(12), S. 1191-1203.

Ghai, Yash (1993), Asian Perspectives on Human Rights. *Hong Kong Law Journal*, 23(3), S. 342-357.

Greenleaf, Graham (2019): G20 Makes Declaration of 'Data Free Flow With Trust': Support and Dissent. *Privacy Laws & Business International Report*, 160, S. 18-19.

Helberger, Natali; Zuiderveen Borgesius, Frederik; Reyna, Agustin (2017): The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law. *Common Market Law Review*, 54(5), S. 1427-1465.

Heper, Joshua (2022): Schrems als Handlungsauftrag: die Zukunft internationaler Datentransfers aus europäischer Perspektive. *Jahrbuch für Vergleichende Staats-und Rechtswissenschaften*, S. 125-154.

Joo, Moon-Ho und Kwon, Hun-Yeong (2023): Comparison of personal information de-identification policies and laws within the EU, the US, Japan, and South Korea. *Government Information Quarterly*, S. 1-12.

Lynskey, Orla (2018): Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez. *Modern Law Review*, 78(3), S. 522-534.

Park, Sung-Uk; Park, Moon-Soo; Park, Soo-Hyun; Yun, Young-Mi (2020): Keywords Analysis on the Personal Information Protection Act: Focusing on South Korea, the European Union and the United States. *Asian Journal of Innovation and Policy*, 9(3), S. 339-359.

Purtova, Nadezhda (2018): The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 10(1), S. 40-81.

Rustad, Michael L. und Koenig, Thomas H. (2019): Towards a Global Data Privacy Standard. *Florida Law Review* 71(2), S. 365-454.

Rzeszucinski, Pawel (26. Mai 2022): Be Ready For The Brussels Effect — It's Coming To Data And AI, Forbes. URL: https://www.forbes.com/sites/forbestechcouncil/2022/05/26/be-ready-for-the-brussels-effect---its-coming-to-data-and-ai/?sh=3d23f7bf3036 (besucht am 16. 02. 2023).

Schwartz, Paul M. und Solove, Daniel J. (2014): Reconciling Personal Information in the United States and European Union. *California Law Review,* 102(4), S. 877-916.

Solove, Daniel J. und Hartzog, Woodrow (2014): The FTC and the new common law of privacy. *Columbia Law Review*, 114(3), S. 584-676.

Sury, Ursula (2020): Die Auswirkungen des EuGH-Urteils C-311/18 „Schrems-II" auf den Datenaustausch mit den USA. *Informatik Spektrum*, 43, S. 354-355.

Tomuschat, Chrisitan (2003): Human Rights. Between Idealism and Realism. Oxford: Oxford University Press.

Tracol, Xavier (2015): Back to basics: The European Court of Justice further defined the concept of personal data and the scope of the right of data subjects to access it. *Computer Law & Security Review*, 31(1), S. 112-119.

Wang Han, Sarah und Bakar Munir, Abu (2018): Information Security Technology – Personal Information Security Specification: China's Version of the GDPR? *European Data Protection Law Review,* 4, S. 535-541.

World Economic Forum (WEF) (2023): Data Free Flow with Trust: Overcoming Barriers to Cross-Border Data Flows, Briefing Paper. URL: https://www3.weforum.org/docs/WEF_Data_Free_Flow_with_Trust_2022.pdf (besucht am 17. 02. 2023).

Zetoony, David (2022): Navigating the Chaos of the CCPA: The Most Frequently Asked Questions When Implementing Privacy Programs. *Loyola University Chicago Journal of Regulatory Compliance (JRC)*, 8, S. 1-17.

Zuiderveen Borgesius, Frederik (2017): The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition. *European Data Protection Law Review (Eur. Data Prot. L. Rev.)*, 3(1), S. 130-137.

Informiertheit und Transparenz im Kontext digitaler Selbstvermessung

Fabiola Böning, Stefanie Astfalk, Rachelle Sellung und Uwe Laufs

Zusammenfassung

Der folgende Beitrag ordnet sich in das vom BMBF geförderte Projekt TESTER – „Digitale Selbstvermessung selbstbestimmt gestalten" ein und stellt zunächst die Ergebnisse einer halbstrukturierten, qualitativen Interviewstudie vor, bevor er auf einige sich daraus ergebende Fragen im Hinblick auf die Transparenzvorgaben der Datenschutz-Grundverordnung eingeht.

Anhand der Ergebnisse der Interviewstudie wurden verschiedene Personas erstellt, die aus unterschiedlichen Gründen Selbstvermessung betreiben und einen unterschiedlichen Umgang mit Privatsphäreeinstellungen pflegen. Gemein ist ihnen jedoch, dass sie grundsätzlich anhand weniger Informationen umfassend informiert werden wollen und die Wichtigkeit von Transparenz höher eingeschätzt wird als die Wichtigkeit von Intervenierbarkeit. Der Beitrag stellt Fragen nach den Gründen für die Einschätzungen der SelbstvermesserInnen und wirft rechtliche Fragen auf, die sich aus den Ergebnissen der Interviewstudie und insbesondere im Hinblick auf den Umgang mit dem Strukturprinzip der Transparenz einerseits und den Informationspflichten andererseits ergeben.

Zuletzt wird die in TESTER erforschte Möglichkeit zur technischen Umsetzung von Transparenzvorgaben in Form eines Privacy Assistenten als einem interaktiven System zur Personalisierung der Informationsver- und -übermittlung vorgestellt.

1. Einleitung

Zu den zentralen Grundsätzen des Datenschutzrechts gehört der Transparenzgrundsatz, der in Art. 5 Abs. 1 lit. a Alt. 3 DS-GVO als Strukturprinzip[1]

1 *Pötter*, in: Gola/Heckmann (Hrsg.), DS-GVO/BDSG, Art. 5 DS-GVO, Rn. 11; s. zur Bedeutung der Strukturprinzipien z.B. auch *Roßnagel*, ZD 2018, 339.

der Datenschutz-Grundverordnung allgemein normiert und in zahlreichen weiteren Vorschriften weiter ausgeformt wird. Dieser Grundsatz steht in einem Spannungsverhältnis zu der Informationsflut, der sich auch die NutzerInnen von Selbstvermessungs-Apps und Wearables zum Zwecke der Selbstvermessung ausgesetzt sehen und aus der sie kaum diejenigen Informationen im Sinne der Artt. 13 und 14 DS-GVO herausfiltern können, an denen sie tatsächlich Interesse haben.[2] Selbstvermessung, auch bekannt als Self-Tracking, Self-Monitoring, Lifelogging oder Personal Informatics ist der Einsatz digitaler Technologie zur Aufzeichnung und Umwandlung täglicher Erfahrungen und Gewohnheiten in Daten. Die Datafizierung des Körpers der NutzerInnen ist in der Gesundheitsförderung und -pflege inzwischen gängige Praxis.[3] So wichtig wie der Transparenzgrundsatz aufgrund zunehmender Informations- und Machtasymmetrien auch im privatwirtschaftlichen Bereich[4] geworden ist, so schwierig gestaltet sich zuweilen seine praktische Umsetzung.[5] Umso wichtiger sind innovative Ansätze, die die Bedürfnisse der betroffenen Personen mit den Anforderungen der Datenschutz-Grundverordnung vereinen. Ein solcher Ansatz kann die Implementierung eines Privacy Assistenten als einem interaktiven System sein, das einen Abgleich der NutzerInnenpräferenzen hinsichtlich des Umgangs der Anbieter mit (besonderen) personenbezogenen Daten mit dem tatsächlich zu erwartenden Umgang ermöglicht.[6] Der genannte Privacy Assistent wird im Projekt TESTER „Digitale Selbstvermessung selbstbestimmt gestalten"[7] entwickelt und erforscht.

2 S. zur schwankenden Qualität verschiedener Datenschutzerklärungen von Gesundheits-Apps *Freye*, DuD 2022, 762.

3 *Lupton*, Economy and Society 2016, 101.

4 S. dazu zum Beispiel auch *Breuer*, in: Heselhaus/Nowak (Hrsg.), Handbuch der Europäischen Grundrechte, 2020, § 25, Rn. 1.

5 S. dazu *Freye*, DuD 2022, 762; s. zum Zeitaufwand beim vollständigen Lesen von Datenschutzerklärungen großer Internethändler auch *Gerpott/Mikolas*, MMR 2021, 936.

6 S. dazu auch die Ausführungen unter 8.

7 Förderung im Rahmen der BMBF-Förderrichtlinie „Forschung Agil" mit dem Förderkennzeichen KIS6AGSE022 und einer Forschungsdauer von drei Jahren bis August 2024.

2. Entwicklung der Selbstvermessung

Die wachsende Beliebtheit und Entwicklung der Selbstvermessung wurde vor allem durch den zunehmenden technischen Fortschritt erreicht, welcher die Geräte zur Selbstvermessung für NutzerInnen erschwinglicher und zugänglicher gemacht hat. Beispielsweise sind die für die Selbstvermessung erforderlichen Sensoren über die letzten Jahre besser tragbar und handhabbar geworden, und die Kosten für deren Herstellung sind ebenfalls gesunken, sodass die intelligente Sensortechnologie rasch in das tägliche Leben der NutzerInnen eindringen konnte.[8] Darüber hinaus wird mit der zunehmenden Verbreitung des Internets der Dinge die Datenerfassung und -weitergabe weiter zunehmen, da die Technologien immer intelligenter, allgegenwärtiger und autonomer werden.[9] Insgesamt verändern die vollständige Digitalisierung sowie Echtzeitverarbeitung die Interaktion der Menschen mit der Welt sowie die Art und Weise, wie sie ihren Körper und ihre Gesundheit wahrnehmen.[10] Denn die Selbstvermessungs-Technologie liefert wertvolle Informationen.[11] Sie kann so dazu führen, dass die Menschen mehr Verantwortung für das eigene Wohlbefinden und die eigene Gesundheit übernehmen und damit eine aktive Rolle einnehmen.[12] Damit fördert die Selbstvermessung einen Wandel hin zu einer präventiven, personalisierten Gesundheitsversorgung,[13] bei der die Individuen und ihre Daten im Mittelpunkt stehen.[14] Dies kann – obwohl Selbstvermessung zum Empowerment der SelbstvermesserInnen beitragen kann – jedoch auch zu negativen Effekten führen, etwa einer gesundheitsschädlichen Übersteigerung

8 *Ajana*, Digital Health 2017; *Ajana*, Metric Culture: Ontologies of Self-Tracking Practices, 2020; *Van Hoof* u.a., Science 2004, 986.

9 *Filkins* u.a., American journal of translational research 2016, 1560; *Swan*, Journal of Sensor and Actuator Networks 2012, 217.

10 *Berry* u.a., Sex Roles 2020, 1; *Brătucu* u.a., Sustainability 2020, 10349; *Šmahel* u.a., in: Šmahel, u.a. (Hrsg.), Digital Technology, Eating Behaviors, and Eating Disorders, 2018, 65.

11 *Vitak*, u.a., Transforming Digital Worlds 2018, 229.

12 *Kahana/Kahana,* in: Kronefeld (Hrsg.), Changing consumers and changing technology in healthcare and health care delivery, 2001, 21; *Sharon*, Philosophy and Technology 2017, 93.

13 *Europäische Kommission*, Green Paper on mobile health ("mHealth"), 2014; *Sharon*, Philosophy and Technology 2017, 93.

14 *Swan*, Journal of Sensor and Actuator Networks 2012, 217.

vermeintlich gesundheitsfördernden Verhaltens bis hin zum Selbstzwang.[15] Abgesehen davon entstehen mit der zunehmenden Verfügbarkeit und Zugänglichkeit digitaler Gesundheitstechnologien auch neue Datenschutzbedenken und -risiken.[16] Beispielsweise können restriktive Einstellungen aus Sicht der NutzerInnen wünschenswert sein, wenn sie eine Datenweitergabe gegen ihren Willen befürchten. Daher untersucht die im Rahmen des Projekts TESTER durchgeführte Interviewstudie die Gründe, weshalb NutzerInnen sich selbst vermessen, sowie etwaige Datenschutzbedenken.

3. Empirische Erkenntnisse

Für die Erfassung der Gründe für die Selbstvermessung sowie vorliegenden Datenschutzbedenken wurde eine qualitative, halbstrukturierte Interviewstudie mit N = 11 Personen (55 % weiblich, 45 % männlich) im Alter zwischen 24 und 38 Jahren durchgeführt.

3.1 Methodik der qualitativen Interviewstudie

Der Leitfaden der qualitativen Interviewstudie gliederte sich in die vier Inhaltsblöcke der Motivation zur Selbstvermessung, der NutzerInnenpräferenzen hinsichtlich Transparenz und Intervenierbarkeit hinsichtlich des Datenschutzes, den technischen und funktionalen Detailanforderungen an einen Privacy Assistenten sowie demografische Daten.

Die Auswertung der qualitativen Interviewstudie erfolgte anhand einer qualitativen Inhaltsanalyse nach Mayring, welche als systematische und regelbasierte Methode ein hohes Maß an Nachvollziehbarkeit gewährleistet.[17] Kern dieser Methode ist das Kategoriensystem, in dem alle relevanten Textpassagen als inhaltsanalytische Kategorien abgebildet werden.[18] Dieses wird im Laufe des Verfahrens angepasst und kann deduktiv, d. h. basierend auf bereits vorhandenen Theorien und Forschungsergebnissen, oder induktiv,

15 *Stiglbauer* u.a., Computers in Human Behaviour 2019, 94; *Wieczorek* u.a., Ethics & Behaviour 2023, 239.
16 *Filkins* u.a., American journal of translational research 2016, 1560.
17 *Mayring*, Qualitative Inhaltsanalyse: Grundlagen und Techniken, 2015.
18 *Hussy* u.a., Forschungsmethoden in Psychologie und Sozialwissenschaften für Bachelor, 2013.

d. h. aus dem zu erstellenden Datenmaterial, erfolgen.[19] In der vorliegenden Arbeit wurde eine Kombination aus beiden Ansätzen gewählt. Als unterstützende Software und zur besseren Übersicht über die Kategorien und kodierten Textpassagen wurde MAXQDA für die Auswertung eingesetzt.[20] Hierbei wurden die Kategorien Selbstvermessung, Motive, Datenweitergabe, Privatsphäre, Transparenz, Intervenierbarkeit und Bereitschaft zur Nutzung eines Privacy Assistenten sowohl induktiv als auch deduktiv gebildet.

3.2 Ergebnisse der qualitativen Interviewstudie: Motive der Selbstvermessung und Privatsphärebedenken

Insgesamt umfassen die Motive zur Selbstvermessung vor allem die Motive der Selbstverbesserung, des Lebensstils und der Achtsamkeit, der Statistik und Gamifizierung, der sportlichen Leistung und deren Überwachung sowie der Gesundheit. Die Interviewten haben in den letzten sechs Jahren mit der Selbstvermessung begonnen und verwenden eine Smart Watch mit dazugehöriger App sowie zum Teil weitere Apps für Fitnessstudios, Sportvereine oder zum Vergleich mit anderen Personen. Hierbei beinhaltet die Routine der Selbstvermessung, dass ein dauerhaftes Tracken der Schritte, des Kalorienverbrauchs sowie des Schlafes stattfindet und ein gesondertes Aktivieren des Trackings von Trainingseinheiten. Ein Abnehmen der Uhr findet nur bei besonderen Anlässen statt.

Bezüglich der Bedenken hinsichtlich der Privatsphäre liegt bei allen Interviewten ein mittleres bis hohes Vertrauenslevel vor. Hierbei zeigen sich zwei Tendenzen: Entweder wird von den Interviewten eine sehr hohe Privatsphäreneinstellung vorgenommen oder es liegt wenig Wissen bzw. Interesse seitens der Interviewten zum Thema Privatsphäre vor. Insgesamt wird Transparenz über alle InterviewpartnerInnen hinweg höher priorisiert als Intervenierbarkeit.[21]

19 *Mayring*, Qualitative Inhaltsanalyse: Grundlagen und Techniken, 2015.
20 *Kuckartz*, Einführung in die computergestützte Analyse qualitativer Daten, 2010.
21 S. zum Verständnis der InterviewpartnerInnen von Transparenz auch die Ausführungen unter 6.3.

3.3 Ergebnisse der qualitativen Interviewstudie: Ableitung von Personas

Insgesamt wurden aus diesen Ergebnissen anhand einer narrativen Nutzungskontextbeschreibung[22] folgende vier Personas erstellt, welche die verschiedenen Ausprägungen der Kategorien abdecken: „Sporty-Sam", „Healthy-Henry", „Techy-Tina" und „Balanced-Beth". Diese vier Personas zeigen unterschiedliche Ausprägungen hinsichtlich der Motivation zur Selbstvermessung, der Sensibilität bezüglich der Datenweitergabe sowie der Bedenken bezüglich der Privatsphäre und der Nutzung des Privacy Assistenten.[23] Sporty-Sam priorisiert die Selbstverbesserung und sportliche Leistung und zeigt die Motivatoren Selbstverbesserung, Lebensstil und Achtsamkeit, Statistik und Gamifizierung, sportliche Leistung und deren Überwachung sowie Gesundheit. Das Vertrauen in den Schutz der Privatsphäre durch den Anbieter ist hoch, eine personalisierte Anpassung der Privatsphäreeinstellungen wie beispielsweise Einstellungen bezüglich der Sichtbarkeit der verarbeiteten Daten für andere NutzerInnen auf der einen Seite und für die Anbieter auf der anderen Seite, ist nicht vorhanden. Ein Privacy Assistent würde verwendet werden, wenn dieser einfach zu bedienen ist. Die Wichtigkeit von Transparenz wird hoch bewertet, diejenige von Intervenierbarkeit hingegen nur gering.

Die Persona Healthy-Henry sieht eine Smart-Watch als Erweiterung ihrer Selbst zur dauernden Selbstvermessung an und weist die Motivatoren Selbstverbesserung, Lebensstil und Achtsamkeit sowie Gesundheit auf. Das Vertrauen in den Schutz der Privatsphäre durch den Anbieter ist mittelhoch und es liegt zum Teil eine Personalisierung der Privatsphäreeinstellungen vor. Die Wichtigkeit von Transparenz wird hoch bewertet, diejenige von Intervenierbarkeit hingegen nur gering. Ein Privacy Assistent würde genutzt werden, da eine Privatsphäreverletzung im Vorhinein abgewendet werden könnte.

Für Techy-Tina stehen bei der Selbstvermessung die mit der Bewegung verbundenen Zahlen im Vordergrund. Entsprechend sind die Motivatoren der Statistik und Gamifizierung sowie sportliche Leistung und deren Überwachung vorhanden. Das Vertrauen in den Schutz der Privatsphäre durch den Anbieter ist hoch. Dennoch findet eine sensible personalisierte Anpassung der Privatsphäreeinstellungen statt. Die Wichtigkeit von Transparenz wird hoch bewertet und diejenige von Intervenierbarkeit mittelhoch. Ein

22 *Geis* u.a., Basiswissen Usability und User Experience, 2020.

23 S. zur Funktionsweise des Privacy Assistenten die Ausführungen unter 8.

Privacy Assistent würde auf jeden Fall verwendet werden, da dieser mehr Überblick und Statistiken zur Selbstvermessung anbietet.

Für Balanced-Beth stehen bei der Selbstvermessung der Lebensstil und die Achtsamkeit im Vordergrund. Als Motivatoren sind die Selbstverbesserung, der Lebensstil und die Achtsamkeit sowie die Gesundheit vorzufinden. Das Vertrauen in den Schutz der Privatsphäre durch den Anbieter ist mittelhoch und es liegt zum Teil eine Personalisierung der Privatsphäreeinstellungen vor. Die Wichtigkeit von Transparenz wird hoch bewertet, diejenige von Intervenierbarkeit hingegen nur gering. Ein Privacy Assistent würde genutzt werden.

3.4 Einordnung der Interviewergebnisse

Aus der Interviewstudie lässt sich entnehmen, dass die Wichtigkeit des Vorliegens von Transparenz über die Personas hinweg als grundsätzlich hoch bewertet wird, und zwar unabhängig von den durchaus unterschiedlichen Privatsphäreeinstellungen. Interessant ist für die weitere Einbettung der Interviewergebnisse in den juristischen Kontext auch, dass die Herstellung von Transparenz immer auch eine Gradwanderung zwischen einem „zu viel" an Informationen, das schlimmstenfalls in einem „information overload" endet, und einem „zu wenig" an Informationen ist.[24]

4. Die Entwicklung des Transparenzgrundsatzes

Durch die unmittelbare Geltung der Verordnung in allen Mitgliedstaaten der Europäischen Union[25] haben der Transparenzgrundsatz als in Art. 5 Abs. 1 lit. a Alt. 3 DS-GVO normiertes Strukturprinzip und die konkreten Informationspflichten der Artt. 13 und 14 DS-GVO eine besondere Bedeutung sowohl für die Verantwortlichen als auch für die betroffenen Personen erlangt. Die Ursprünge des Transparenzgrundsatzes sind aber viel älter.

Bereits 1983 entschied das Bundesverfassungsgericht im Volkszählungsurteil,[26] dass für die BürgerInnen transparent sein müsse, welche Informa-

24 S. *Art. 29-Gruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, 2018, S. 21 f.; *Voigt*, Die datenschutzrechtliche Einwilligung, 2020, 92.
25 Art. 288 Abs. 2 AEUV.
26 *BVerfG*, NJW 1984, 419.

tionen über sie in welchem Kontext bekannt sind. Informationsasymmetrien zwischen BürgerInnen und Staat seien untragbar, weil sie dazu führen könnten, dass erstere in der Ausübung ihrer Grundrechte insgesamt gehemmt werden.[27] Die Verwirklichung der individuellen Selbstbestimmung setze voraus, dass jeder/jede BürgerIn wissen könne, „wer was wann und bei welcher Gelegenheit" über ihn/sie weiß.[28] Das Recht auf informationelle Selbstbestimmung als Konkretisierung des in Art. 2 Abs. 1 GG und Art. 1 Abs. 1 GG verankerten allgemeinen Persönlichkeitsrechts[29] sollte den „Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten" schützen.[30] Dafür bedarf es jedoch einer Kenntlichmachung, dass Daten bei Dritten oder durch heimliches Beobachten erhoben worden sind. Die Datenverarbeitung muss also für die BürgerInnen transparent sein.

Auf europäischer Ebene ist der Schutz personenbezogener Daten und der Privatsphäre im Rahmen eigenständiger Gemeinschaftsgrundrechte durch die Schutzgehalte der Artt. 7 und 8 der Charta der Grundrechte der Europäischen Union (GRCh) garantiert,[31] wenngleich diese zunächst nur die Union und die Mitgliedstaaten im Falle der Durchführung von Unionsrecht verpflichten.[32] Aus beiden Grundrechten lässt sich – insbesondere auch vor dem Hintergrund der Rechtsprechung zu Art. 8 EMRK – die Verpflichtung der Normadressaten zur Herstellung von Transparenz ableiten.

Der Schutz des Privatlebens, wie er in Art. 7 Abs. 1 Var. 1 GRCh als ein Teilbereich des „Grundrechts auf Privatheit" normiert ist, entspricht dem aus Art. 2 Abs. 1 GG und Art. 1 Abs. 1 GG abgeleiteten Recht auf informationelle Selbstbestimmung.[33] Der Schutzbereich umfasst in sachlicher Hinsicht das Recht des Grundrechtsträgers, über die eigene Lebensführung zu bestimmen,[34] das Recht, über die Darstellung der eigenen Person in der Öf-

27 S. *BVerfG*, NJW 1984, 419 (422).
28 *BVerfG*, NJW 1984, 419 (422).
29 *BVerfG*, NJW 1984, 419; *Roßnagel*, NJW 2019, 1.
30 *BVerfG*, NJW 1984, 419 (422).
31 S. z.B. *Roßnagel*, NJW 2019, 1 (2), allerdings in Bezug auf die Schutzgehalte differenzierend.
32 S. *Jarass*, in: Jarass (Hrsg.), Charta der Grundrechte der EU, Einleitung, Rn. 34 m.w.N.
33 S. *Roßnagel*, NJW 2019, 1 (2).
34 S. *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, Art. 7 GRCharta, Rn. 4.

fentlichkeit zu entscheiden[35] und das Recht darauf, sich von seiner Umwelt abzuschirmen und sich zurückzuziehen,[36] worunter auch das Recht einer Person fällt, ihren Gesundheitszustand geheim zu halten.[37] Grundrechtsträger sind alle natürlichen Personen.[38] Bei der Erhebung von Daten diverser Vitalparameter wie zum Beispiel Gewicht, Puls und Blutdruck ist regelmäßig der Schutzbereich des Rechts auf den Schutz des Privatlebens betroffen. Durch die Verarbeitung von Standortdaten einer Person, nachvollziehbar z. B. über GPS, wie sie regelmäßig bei der Aufzeichnung einer Joggingstrecke vorkommen wird, kann sowohl das Recht auf Selbstbewahrung als auch das Recht auf Selbstdarstellung betroffen sein. Die betroffene Person kann einerseits ein Interesse daran haben, Standortdaten nicht mit Dritten zu teilen. Sie kann aber andererseits gerade ein Interesse daran haben, besonders herausragende Leistungen mit Dritten zu teilen, sich diesen gegenüber also selbst darzustellen.

In Art. 8 GRCh ist der Schutz personenbezogener Daten geregelt. Dabei wird in Absatz 1 das generelle Recht ein jeder Person auf den Schutz der sie betreffenden personenbezogenen Daten festgelegt, während in Absatz 2 weitere Grundsätze für die Verarbeitung personenbezogener Daten normiert sind. Interessant ist dabei in Bezug auf das Ziel einer transparenten Datenverarbeitung insbesondere das Auskunftsrecht aus Art. 8 Abs. 2 S. 2 Alt. 1 GRCh, welches die Kontrolle der betroffenen Person über den sie betreffenden Datenverarbeitungsvorgang erleichtern soll.

Daten, die die betroffene Person eingibt, oder die an ihrem Körper mittels Wearables gemessen werden, sind personenbezogene Daten,[39] da es sich dabei regelmäßig um Daten handelt, die eine natürliche Person[40] identifizierbar machen.[41] Sie weisen somit einen ausreichenden Personenbezug

35 S. *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, Art. 7 GRCharta, Rn. 6.
36 S. *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, Art. 7 GRCharta, Rn. 5.
37 S. *Jarass*, in: Jarass, (Hrsg.), Charta der Grundrechte der EU, Art. 7 GRCh, Rn. 15.
38 S. zum Diskussionsstand und zur Grundrechtsfähigkeit juristischer Personen unter anderem *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, Art. 8 GRCharta, Rn. 12.
39 S. zur Wechselwirkung zwischen GRCh und DS-GVO *Jarass*, in: Jarass (Hrsg.), Charta der Grundrechte der EU, Art. 8 GRCh, Rn. 6.
40 S. zu der Eigenschaft von natürlichen Personen und der teilweisen Eigenschaft von juristischen Personen als Grundrechtsträger *Jarass*, Art. 8 GRCh, Rn. 8 und *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, Art. 8 GRCh, Rn. 12 mit Kritik an der unklaren Rechtsprechung des EuGH.
41 S. zur Anlehnung an Begriffe aus der DS-GVO z.B. *Kingreen*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, Art. 8 GRCh, Rn. 10.

auf,[42] sodass im Regelfall der Schutzbereich des Art. 8 GRCh eröffnet ist. Ein Eingriff in den Schutzbereich von Art. 8 GRCh liegt bei der Verarbeitung personenbezogener Daten vor, und zwar unabhängig von möglichen Folgen für die betroffene Person.[43] Damit ein Eingriffsausschluss nach Art. 8 Abs. 2 S. 1 GRCh in Betracht kommt, muss die betroffene Person in die Datenverarbeitung einwilligen und die Datenverarbeitung muss den Grundsätzen von „Treu und Glauben" entsprechen, was die Transparenz der Datenverarbeitung einschließt.[44] Damit die Einwilligung den Eingriffsausschluss herbeiführt, muss die betroffene Person ausreichend informiert werden.[45] Letztendich spiegelt sich der Transparenzgrundsatz also bereits in Art. 8 Abs. 2 S. 1 GRCh wider.

Die Gewährleistungen des Art. 8 GRCh gehen über die des Art. 7 GRCh insofern hinaus, als der Datenschutz durch Art. 8 GRCh auch dann gewährleistet wird, wenn die in Art. 7 GRCh geschützte Privatsphäre nicht tangiert wird.[46] Tatsächlich kommt es im Kontext digitaler Selbstvermessung aber wohl nicht auf das Verhältnis von Art. 7 GRCh und Art. 8 GRCh an, da es bei der Datenerhebung mittels Sensoren und Wearables am Körper der betroffenen Person unerheblich ist, ob Art. 8 GRCh lex specialis zu Art. 7 GRCh[47] oder parallel anzuwenden ist,[48] Darüber hinaus ist insbesondere der in Art. 8 Abs. 2 S. 2 GRCh normierte Auskunftsanspruch, in dem sich Grundsätze aus der Datenschutz-Richtlinie wiederfinden,[49] die

42 S. zum Personenbezug *Jarass*, in: Jarass (Hrsg.), Charta der Grundrechte der EU, Art. 8 GRCh, Rn. 7.

43 S. *Jarass*, in: Jarass (Hrsg.), Charta der Grundrechte der EU, Art. 8 GRCh, Rn. 9; *Kingreen*, in: Calliess/Ruffert (Hrsg.) EUV/AEUV, Art. 8 GRCh, Rn. 13.

44 S. *Jarass*, in: Jarass (Hrsg.), Charta der Grundrechte der EU, Art. 8 GRCh, Rn. 10 f..

45 S. *Jarass*, in: Jarass (Hrsg.), Charta der Grundrechte der EU, Art. 8 GRCh, Rn. 10 m.w.N.

46 S. *Roßnagel*, NJW 2019, 1 (2).

47 S. unter anderem *Jarass*, in: Jarass (Hrsg.), Charta der Grundrechte der EU, Art. 8 GRCh, Rn. 4, der einen Anwendungsvorrang von Art. 8 GRCh vor Art. 7 GRCh im Überschneidungsbereich annimmt und zugleich auf die weniger differenzierte Rechtsprechung des EuGH verweist.

48 S. nur *EuGH*, Urteil vom 9.11.2010 C-92/09 und C-93/09, Rn.47, 52 und *EuGH*, Urteil vom 24.11.20122 C-468/10 und C-469/10, Rn. 41 f; *Jarass*, in: Jarass (Hrsg.), Charta der Grundrechte der EU, Art. 8 GRCh, Rn. 4; kritisch zur EuGH Rechtsprechung *Breuer*, in: Heselhaus/Nowak (Hrsg.), Handbuch der Europäischen Grundrechte, § 25, Rn. 24; zum Verhältnis der Vorschriften insgesamt ausführlich *Michl*, DuD 2017, 353.

49 S. *Bernsdorff,* in: Meyer/Hölscheidt (Hrsg.), Charta der Grundrechte der EU, Art. 8 GRCh, Rn. 30; *Breuer,* in: Heselhaus/Nowak (Hrsg.), Handbuch der Europäischen

primärrechtliche Absicherung des Transparenzgrundsatzes,[50] der über die Verpflichtung der Unionsorgane und der Mitgliedstaaten auch Wirkung für Privatpersonen entfaltet.[51] Der Auskunftsanspruch bezieht sich auf die Frage, ob Daten des Grundrechtsträgers verarbeitet worden sind und kann auch bei der bloßen Möglichkeit der Datenverarbeitung geltend gemacht werden.[52] Er bezieht sich auf den „gesamten Inhalt der gespeicherten Daten"[53] und dient nicht nur der Kenntniserlangung von einer Datenverarbeitung, sondern insbesondere auch der Möglichkeit, die Richtigkeit der Daten sowie die Rechtmäßigkeit der Datenverarbeitung zu überprüfen[54] und damit letztendlich der Kontrollmöglichkeit der betroffenen Person. Art. 7 GRCh ist mit im Grunde unerheblichen Änderungen an den Wortlaut des Art. 8 EMRK[55] angelehnt, sodass nach Art. 52 Abs. 3 GRCh auf die entsprechende Rechtsprechung des EGMR zurückzugreifen ist. Wenngleich in dieser der Transparenzgrundsatz nicht explizit erwähnt wird, ist die Transparenz über Datenverarbeitungsvorgänge schon eine Voraussetzung dafür, dass überhaupt Beschwerden beim EGMR erhoben werden können.[56] Darüber hinaus gleicht der EGMR fehlende oder mangelhafte Transparenz dadurch aus, dass er strengere Anforderungen an die Rechtmäßigkeit der verdeckten Datenverarbeitung stellt.[57] Insgesamt ist Transparenz somit zwar kein Hauptaugenmerk des EGMR, wird jedoch für eine wirksame Rechtsdurchsetzung vorausgesetzt, sodass sie kontextunabhängig relevant ist.

Grundrechte, § 25, Rn. 37, dieser auch zur Abgrenzung gegenüber der Rechtsprechung des EGMR.

50 *Roßnagel,* in: Simitis u.a. (Hrsg.), Datenschutzrecht, Art. 5 DS-GVO, Rn. 49; s. auch *Manthey*, Das datenschutzrechtliche Transparenzgebot, 2020, 102.

51 S. *Streinz/Michl*, EuZW 2011, 384 (385); *Kingreen*, in: Calliess/Ruffert (Hrsg.) EUV/AEUV, Art. 8 GRCh, Rn. 11.

52 S. *Jarass*, in: Jarass (Hrsg.), Charta der Grundrechte der EU, Art. 8 GRCh, Rn. 20.

53 *Jarass*, in: Jarass (Hrsg.), Charta der Grundrechte der EU, Art. 8 GRCh, Rn. 20.

54 *Jarass*, in: Jarass (Hrsg.), Charta der Grundrechte der EU, Art. 8 GRCh, Rn. 20 mit Verweis auf EuGH, Urteil vom 17.07.2014 – C-141/12, Rn. 60.

55 S. zur Rechtsnatur der EMRK *Manthey*, Das datenschutzrechtliche Transparenzgebot, 2020, 56 ff.

56 S. *Manthey*, Das datenschutzrechtliche Transparenzgebot, 2020, 81.

57 S. *Manthey*, Das datenschutzrechtliche Transparenzgebot, 2020, 82.

5. Transparenz bei der Verarbeitung von Gesundheitsdaten vor dem Hintergrund zunehmender Vernetzung

Bereits 1994 entschied der EuGH, dass es einer Person unbenommen sein muss, sich gegen eine ärztliche Untersuchung und die Veröffentlichung der Ergebnisse einer ärztlichen Untersuchung zu entscheiden.[58] Das Recht auf die Achtung des Privatlebens umfasse das Recht einer Person, ihren Gesundheitszustand geheim zu halten.[59] Interessant ist im vorliegenden Kontext, dass es den SelbstvermesserInnen ja gerade darauf ankommt, Daten über den eigenen Gesundheitszustand zu erheben und Erkenntnisse aus der Kombination verschiedener Daten zu ziehen. Um die Dienste der Anbieter diesbezüglich in Anspruch nehmen zu können, ist es notwendig, die entsprechenden Daten auch an diese zu übermitteln.

Interessant wäre auch zu wissen, inwiefern sich die Bereitschaft zur Datenfreigabe gegenüber privaten Anbietern von Selbstvermessungs-Tools von derjenigen gegenüber öffentlichen Stellen unterscheidet. Zu erwarten ist eine Zunahme der Vernetzung im Gesundheitsbereich, bei der die Grenzen zwischen der Datenverarbeitung im Freizeitbereich und die Datenverarbeitung zum Zwecke der Versorgung und der Forschung aufgeweicht werden könnten. Insofern ist es für die betroffene Person umso wichtiger, transparent über Datenverarbeitungsvorgänge informiert zu werden, um weiterhin Kontrolle über die eigene Privatsphäre und die die betroffene Person betreffenden personenbezogenen Daten ausüben zu können. Die Bedeutung von Gesundheitsdaten als besondere personenbezogene Daten zeigt sich auch in der Vorschrift des Art. 9 DS-GVO, in der besondere Voraussetzungen für die Verarbeitung von Gesundheitsdaten normiert sind. Es stellt sich die Frage, ob bei der Verarbeitung besonderer personenbezogener Daten nicht höhere Anforderungen an die Herstellung von Transparenz zu stellen sind.

6. Transparenz in der Datenschutz-Grundverordnung

Besonders relevant sind für den Rechtsanwender die Vorgaben der Datenschutz-Grundverordnung. Die Bedeutung des Transparenzgrundsatzes zeigt sich dabei einerseits in der Tatsache, dass die betroffene Person einen

58 EuGH, Urteil vom 05.10.1994 – C-404/92; *Jarass*, in: Jarass (Hrsg.), Charta der Grundrechte der EU, Art. 7 GRCh, Rn. 15.

59 EuGH, Urteil vom 05.10.1994 – C-404/92.

direkten Anspruch auf dessen Einhaltung hat, die auch durch die mögliche Verhängung eines Bußgeldes gewährleistet werden soll. Sie zeigt sich aber auch ganz praktisch in den zahlreichen Informationspflichten und den Vorgaben zur Übermittlung der entsprechenden Informationen, die den datenschutzrechtlichen Verantwortlichen treffen.

6.1 Transparenz als zentrales Strukturprinzip

Das Bundesverfassungsgericht hob in dem Volkszählungsurteil die Bedeutung der Transparenz und anderer Grundsätze der Verarbeitung personenbezogener Daten zwar hervor, jedoch folgten daraus keine einklagbaren Individualrechte oder eine Katalogisierung durch den nationalen Gesetzgeber, die eine Vollziehbarkeit der Grundsätze zur Folge hätte.[60] Vielmehr wurden die Grundsätze bei der Gesetzgebung und zur Auslegung von Normen herangezogen.[61] Dies wurde durch den europäischen Verordnungs- und Richtliniengeber schon durch die Einführung der Datenschutzgrundsätze – infolge des Katalogs von Grundsätzen zur „Qualität der Daten" in der Konvention 108[62] – in Art. 6 Abs. 1 der DS-RL[63] anders gehandhabt, was sich in den in Art. 5 DS-GVO festgesetzten Grundsätzen fortsetzt.[64] Bemerkenswert ist dabei, dass der Grundsatz der Transparenz in Art. 5 Abs. 1 lit. a Alt. 3 DS-GVO erstmals ausdrücklich erwähnt ist,[65] während er zuvor in die in Art. 6 DS-RL enthaltene Voraussetzung der Verarbeitung nach den Grundsätzen von Treu und Glauben hereingelesen wurde.[66]

Ein Blick auf die inhaltliche Ausgestaltung und Bedeutung von Art. 5 Abs. 1 lit. a Alt. 3 DS-GVO lohnt sich auch, weil ein Verstoß gegen dieses Prinzip bußgeldbewehrt ist. Nach Art. 83 Abs. 5 lit. a DS-GVO drohen dem datenschutzrechtlich Verantwortlichen auch bei einem Ver-

60 S. *Roßnagel*, ZD 2018, 339.
61 S. *Roßnagel*, ZD 2018, 339.
62 Übereinkommen zu Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, Straßburg 28.1.1981, BGBl. II S. 539; s. zu deren Bedeutung auch *Simitis* u.a., in: Simitis u.a. (Hrsg.), Datenschutzrecht, Einleitung, Rn. 78 f.
63 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 23.11.1995, ABl.. L 281, 31.
64 S. *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 5 DS-GVO, Rn. 5.
65 S. *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 5 DS-GVO, Rn. 5f.
66 S. *Jaspers* u.a., in: Schwartmann u.a. (Hrsg.), DS-GVO/BDSG, Art. 5 DS-GVO, Rn. 8.

stoß gegen die Grundsätze der Verarbeitung Geldbußen von bis zu 20.000.000,00 € bzw. 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres eines Unternehmens. Bemerkenswert ist dabei, dass ein Verstoß gegen die Pflichten aus Artt. 12 ff. DS-GVO gesondert bußgeldbewehrt ist (Art. 83 Abs. 5 lit. b DS-GVO), wenngleich aufgrund des in Art. 83 Abs. 3 DS-GVO normierten „Nichtakkumulationsprinzip"[67] die Höhe der Geldbuße insgesamt begrenzt ist.[68] Indes stellt sich die Frage, was bei Einhaltung der Übermittlungserfordernisse und Informationspflichten der Artt. 12 ff. DS-GVO inhaltlich für das Strukturprinzip der Transparenz noch übrigbleibt und inwiefern ihm eine eigenständige Bedeutung zukommt.

Konkret ist ausweislich des EG 39 DS-GVO unter dem in Art. 5 Abs. 1 lit. a Alt. 3 DS-GVO normierten Strukturprinzip der Transparenz zu verstehen, dass „alle Informationen und Mitteilungen zur Verarbeitung [der] personenbezogenen Daten leicht zugänglich, verständlich sowie in klarer und einfacher Sprache abgefasst sind".[69] Diese Anforderungen werden – neben anderen – auch in Art. 12 Abs. 1 DS-GVO formuliert, sodass wiederum unklar ist, inwiefern Art. 5 Abs. 1 lit. a Alt. 3 DS-GVO inhaltlich über Art. 12 Abs. 1 DS-GVO hinausgeht. Die Verarbeitung personenbezogener Daten muss nach Art. 5 Abs. 1 lit. a Alt. 3 DS-GVO in einer „nachvollziehbaren" Weise geschehen. Trotzdem ist der Begriff der Transparenz nicht mit dem Begriff der Nachvollziehbarkeit gleichzusetzen. Das Prinzip der Transparenz geht über die bloße Herstellung der Nachvollziehbarkeit von Datenverarbeitungsvorgängen hinaus.[70] Das Transparenzprinzip bezieht sich beispielsweise nicht nur auf vergangene, sondern auch auf zukünftige Datenverarbeitungsvorgänge,[71] was sich unter anderem aus EG 39 S. 2 DS-GVO ergibt und sich auch vor dem Hintergrund des EG 7 S. 2 DS-GVO erschließt.[72] Diese zukunftsorientierte Ausrichtung ist

67 *Holländer,* in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 83 DS-GVO, Rn. 46.

68 S. *Holländer,* in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 83 DS-GVO, Rn. 46; s. *Boehm,* in: Simitis u.a. (Hrsg.), Datenschutzrecht, Art. 83 DS-GVO, Rn. 36 mit dem Verweis auf mehrere Verarbeitungsvorgänge bei Fitness-Trackern.

69 S. *Pötters,* in: Gola/Heckmann (Hrsg.) DS-GVO/BDSG, Art. 5 DS-GVO, Rn. 11 mit dem Verweis auf weitere Erwägungsgründe.

70 S. *Frenzel,* in: Paal/Pauly (Hrsg.) DS-GVO/BDSG, Art. 5 DS-GVO Rn. 21.

71 S. *Frenzel,* in: Paal/Pauly (Hrsg.) DS-GVO/BDSG, Art. 5 DS-GVO, Rn. 21; *Schantz,* in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 5 DS-GVO, Rn. 11.

72 S. *Pötters,* in: Gola/Heckmann (Hrsg.), DS-GVO/BDSG, Art. 5 DS-GVO, Rn. 12; *Schantz*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 5 DS-GVO, Rn. 11.

insbesondere im Zusammenhang mit der digitalen Selbstvermessung interessant, weil es den SelbstvermesserInnen ja gerade darauf ankommt, dass über einen langen Zeitraum und damit auch in der Zukunft große Mengen an personenbezogenen Daten verarbeitet werden.

Während die InterviewpartnerInnen der im Rahmen von TESTER durchgeführten Interviewstudie das Wissen über die Verwendung der über sie erhobenen Daten als ein Zeichen von Respekt des Verantwortlichen ihnen gegenüber werten, dient der Transparenzgrundsatz aus Sicht des Verordnungsgebers in erster Linie der Wahrung der Rechte der betroffenen Person.[73] Dass der Transparenzgrundsatz kein Selbstzweck ist und durch die Einhaltung desselben nicht die eine Person betreffenden Daten, sondern vielmehr deren Grundfreiheiten und Grundrechte geschützt werden sollen, ergibt sich auch aus Art. 1 Abs. 2 DS-GVO. Dort wird klargestellt, dass zwar „insbesondere [das] Recht [natürlicher Personen] auf Schutz personenbezogener Daten" geschützt werden soll, jedoch auch der Schutz der übrigen Rechte und Freiheiten natürlicher Personen Ziel der Verordnung ist. Gleichzeitig kann nur die angemessene Übermittlung von Informationen über den Prozess der Datenverarbeitung, deren Zusammenhang und die Konsequenzen die betroffene Person in die Lage versetzen, sich im Zweifel und nach eigener Abwägung auch gegen den unbedingten Datenschutz zu entscheiden.[74] Dies ist insbesondere im Kontext der Selbstvermessung eine wichtige Erkenntnis, da es den SelbstvermesserInnen ja darauf ankommt, dass über sie in umfassender Weise Daten verarbeitet werden, die dann für sie einsehbar sind. Dabei scheint es den Personen, die Selbstvermessung betreiben, nicht auf Transparenz zum Zwecke der Ermöglichung von Intervenierbarkeit anzukommen. Vielmehr geht es Sporty-Sam, Healthy-Henry, Techy-Tina und Balanced-Beth grundsätzlich eher darum, dass überhaupt Transparenz hergestellt wird, wenngleich lediglich Sporty-Sam grundsätzlich keine individuellen Privatsphäreeinstellungen vorgenommen hat. Fraglich ist, ob diese personalisierten Privatsphäreeinstellungen zu Beginn bzw. vor der Datenverarbeitung schon für das Gefühl von Kontrolle über die eigenen Daten ausreichend sind und in inwiefern

73 S. *Roßnagel,* in: Simitis u.a. (Hrsg.), Datenschutzrecht, Art. 5 DS-GVO, Rn. 50 mit Verweis auf das Volkszählungsurteil.

74 S. *Frenzel,* in: Paal/Pauly (Hrsg.) DS-GVO/BDSG, Art. 5 DS-GVO, Rn. 21; so im Ergebnis wohl auch *Hermann* u.a., in: Schwartmann u.a., DS-GVO/BDSG, Art. 5 DS-GVO, Rn. 34, die auf die Gefahr der transparency fatigue verweisen.

tatsächlich mehr Kontrolle der SelbstvermesserInnen besteht.[75] Spannend ist überdies die Frage, warum die Wichtigkeit von Transparenz höher eingeschätzt wird und inwiefern der Transparenz ein intrinsischer Wert zukommt.

6.2 Vermeidung eines „Information Overload"

Transparenz bedeutet indes nicht, dass den betroffenen Personen alle denkbaren Informationen zu einem Datenverarbeitungsvorgang übermittelt werden. Vielmehr müssen die Informationen „situationsgerecht" und in der jeweils gewünschten Tiefe übermittelt werden.[76] Dies entspricht auch den Ergebnissen der qualitativen und halbstrukturierten Interviewstudie, bei der die InterviewpartnerInnen überwiegend angaben, dass sie unter dem Begriff Transparenz die eigene Informiertheit anhand sehr weniger Informationen verstehen. Dieses Begriffsverständnis lässt sogleich an den Begriff des „information overload" denken, der das Problem beschreibt, dass der betroffenen Person mehr Informationen gegeben werden, als sie verarbeiten kann oder will.[77]

Einer „Informationsüberlastung" bzw. „Informationsermüdung"[78] soll vor allem durch die Vorgaben des Art. 12 Abs. 1 DS-GVO entgegengewirkt werden, wonach die Informationen zunächst in präziser, also auf die Situation zugeschnittener,[79] inhaltlich richtiger und vollständiger[80] und abgrenzbarer [81] Weise, übermittelt werden sollen. Das in Art. 12 Abs. 1 DS-GVO

75 S. ausführlich *Hermstrüwer*, Informationelle Selbstgefährdung, 2016, 309 f.; *Voigt*, Die datenschutzrechtliche Einwilligung, 2020, 91.

76 *Roßnagel,* in: Simitis u.a. (Hrsg.), Datenschutzrecht, Art. 5 DS-GVO, Rn. 60.

77 S. *Paal/Hennemann*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 12 DS-GVO, Rn. 5; s. weitergehend zum möglichen "information overload" im Kontext weiterer Informationspflichten z.B. auch *Ebner*, ZD 2022, 364.

78 *Art. 29-Gruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679 2018, S. 7, Rn. 8.

79 S. *Eßer*, in: Auernhammer, Art. 12 DS-GVO, Rn. 6; *Franck*, in: Gola/Heckmann (Hrsg.), DS-GVO/BDSG, Art. 12 DS-GVO, Rn. 18; *Heckmann/Paschke*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, Art. 12, Rn. 12; *Quaas*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 12 DS-GVO, Rn. 13.

80 S. *Paal/Hennemann*, in: Paal/Pauly (Hrsg.) DS-GVO/BDSG, Art. 12 DS-GVO, Rn. 28; *Heckmann/Paschke*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, Art. 12, Rn. 12.

81 S. *Art. 29-Gruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679 2018, S. 7, Rn. 8; *Franck*, in: Gola/Heckmann (Hrsg.), DS-GVO/BDSG, Art. 12 DS-GVO, Rn. 18; *Pohle/Spittka*, in: Taeger/Gabel (Hrsg.), DSGVO - BDSG - TTDSG, Art. 12

ebenfalls aufgegriffene Erfordernis der Transparenz wirft Schwierigkeiten auf, weil sich für den Verantwortlichen im Ergebnis so erhebliche Gestaltungsspielräume ergeben,[82] dass die Voraussetzung der transparenten Übermittlung nur bei „grob ungenauen oder unverständlichen Informationen"[83] nicht vorliegt. Fraglich ist, ob nicht gerade dieser weite Gestaltungsspielraum in der Praxis dazu führt, dass bei den InterviewpartnerInnen eine überwiegende Unzufriedenheit in Bezug auf die Transparenz im Rahmen der Selbstvermessung vorliegt.[84]

Von der Voraussetzung der Transparenz nur schwer abgrenzbar ist das Kriterium der Verständlichkeit, wonach jedenfalls die "richtige Sprache" ausgewählt werden muss[85] und die allgemeinen kognitiven Fähigkeiten des Durchschnittsadressaten ausreichen müssen, um die Informationen und Mitteilungen inhaltlich zu erfassen.[86] Wenngleich Selbstvermessung derzeit noch überwiegend von jüngeren und gebildeten Personen betrieben wird,[87] kann davon ausgegangen werden, dass sich dies aufgrund von verbesserter Sensorik, sinkenden Kosten[88] und dem Wandel hin zu einer präventiven Gesundheitsversorgung[89] in Zukunft ändern wird, sodass eine Anpassung der Informationen erforderlich ist. Dies könnte einerseits dafürsprechen, Informationen auf eine möglichst generische Weise zu übermitteln. Andererseits könnte dies aber auch dafürsprechen, dass eine konsequent

DS-GVO, Rn. 10; *Quaas*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 12 DS-GVO, Rn. 13.

82 S. zu den erheblichen Gestaltungsspielräumen bei der informierten Einwilligung *EDSA*, Leitlinien zur Einwilligung, S. 18, Rn. 66.

83 *Bäcker*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, Art. 12 DS-GVO, Rn. 12 mit dem Hinweis auf die Folgen einer etwaigen Verletzung.

84 S. bzgl. der Einzelheiten die Ausführungen unter 6.3.

85 S. *Franck*, in: Gola/Heckmann (Hrsg.), DS-GVO/BDSG, Art. 12 DS-GVO, Rn. 20; *Greve*, in: Sydow/Marsch (Hrsg.), DS-GVO/BDSG, Art. 12 DS-GVO, Rn. 15 leitet diesen Aspekt der Verständlichkeit indes aus dem Transparenzgebot ab.

86 S. *Bäcker*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, Art. 12 DS-GVO, Rn. 11: „ohne übermäßigen kognitiven oder zeitlichen Aufwand"; *Quaas*, in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 12 DS-GVO, Rn. 15: „Inhalt visuell wie begrifflich erfassen"; *Paal/Hennemann*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 12 DS-GVO, Rn. 30, die darauf verweisen, dass durchaus eine gewisse geistige Anstrengung gefordert werden kann.

87 *Bol* u.a., The Information Society 2018, 183; *Lupton*, Economy and Society 2016, 101.

88 *Ajana*, Digital Health 2017; *Ajana*, Metric Culture: Ontologies of Self-tracking Practices, 2020; *Van Hoof* u.a., Science 2004, 986.

89 *European Commission*, Green Paper on mobile health ("mHealth"), 2014; *Sharon*, Philosophy and Technology 2017, 93.

adressatenbezogene Informationsübermittlung nur individualisiert erfolgen kann.

Zur verständlichen Darstellung von Informationen bzgl. Datenverarbeitungsvorgängen über den ganzen Zeitraum der Selbstvermessung hinweg kommt der Einsatz einer Datenschutz-Ampel bzw. eines Datenschutz-Dashboards in Betracht, wie es für den Privacy Assistenten TESTER geplant ist. Ein Vorteil kann dabei unter anderem die im Laufe der Zeit zunehmende Personalisierung des Privacy Assistenten sein, die eine auf die entsprechende Person zugeschnittene Informationsübermittlung ermöglicht.

6.3 (Gewünschter) Umfang der Informationen

Die InterviewpartnerInnen stellen sich unter Transparenz zwar einerseits überwiegend vor, dass sie anhand sehr weniger Informationen informiert werden, möchten aber andererseits über alles informiert werden, was mit den erhobenen Daten zusammenhängt, bis hin zu den verwendeten Servern, dem Speicherort und der Speicherdauer.

Diesem Bedürfnis kommen die Informationspflichten der Artt. 13 und 14 DS-GVO zumindest weitgehend entgegen, wobei es im Kontext der digitalen Selbstvermessung vor allem auf die Informationspflichten aus Art. 13 DS-GVO ankommt, da die Datenerhebung direkt bei der betroffenen Person erfolgt, wenn sie mittels einer Applikation auf dem Smartphone oder mittels eines Wearables erfolgt und die Daten auf dem Server des Verantwortlichen und nicht nur lokal bei der betroffenen Person gespeichert werden.[90]

Zwar muss die betroffene Person von dem Verantwortlichen ausweislich des Art. 13 Abs. 2 lit. a DS-GVO tatsächlich auch über die Speicherdauer informiert werden, allerdings gehen die Informationspflichten in Teilen weit über das hinaus, was die SelbstvermesserInnen sich wünschen und vorstellen, wenngleich die SelbstvermesserInnen sich andererseits mehr Informationen wünschen, als der Verantwortliche ihnen ausweislich des Art. 13 DS-GVO geben müsste. Dabei stellt sich die Frage, ob für den Fall der Selbstvermessung nicht zugunsten der Transparenz auf die Einhaltung aller Informationspflichten aus Artt. 13 und 14 DS-GVO verzichtet werden müsste, um dem Willen der betroffenen Personen zu entsprechen. Dies wäre allerdings nur möglich, wenn man unter Berufung auf

90 S. *Dix*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, Art. 13 DS-GVO, Rn. 5.

Art. 5 Abs. 1 lit. a Alt. 3 DS-GVO die Informationspflichten aus Art. 13 DS-GVO einschränken könnte, was methodisch zweifelhaft erscheint. Überdies könnte man andererseits man die These in dem Raum stellen, dass die SelbstvermesserInnen sich keine Informationen über bestimmte Bereiche wünschen, weil sie zum Beispiel keine Vorstellung davon haben, wie die Datenverarbeitung genau vonstattengeht und welche Informationen wichtig sein könnten. In diesem Fall wäre es kontraproduktiv, den SelbstvermesserInnen nur genau die Informationen zu übermitteln, die sie sich explizit wünschen, weil sie so nie alle Informationen erhalten würden, die man eigentlich braucht, um selbstbestimmt über die Freigabe der eigenen Daten zu entscheiden. Um differenzierte Transparenzwünsche zu erfüllen, kommt schließlich die gestufte Darstellung der zu übermittelnden Informationen, beispielsweise mittels Mehrebenen-Datenschutzerklärungen, in Betracht. Dies erhöht zwar den Aufwand für die Verantwortlichen, eröffnet aber Chancen auf eine echte Information der Beteiligten. Ein Privacy Assistent kann bei der situationsgerechten, abgestuften Übermittlung von Informationen helfen und wesentlich zur Informiertheit der NutzerInnen beitragen.[91]

Schließlich ist wohl auch jeder/ jedem DurchschnittsnutzerIn und damit jeder der vorgestellten Personas klar, dass die Daten auf Servern – in Abhängigkeit zum jeweiligen Zweck – an einem bestimmten Ort für eine bestimmte Zeit gespeichert werden „müssen", weswegen in der Interviewstudie möglicherweise diese Informationen als solche genannt wurden, die man im Sinne der Transparenz gerne hätte.

Angesichts der Menge der Informationen, die nach Artt. 13 f. DS-GVO eigentlich übermittelt werden müssen, stellt sich die Frage, ob ein „information overload" wirklich durch die bloße Einhaltung der Vorgaben der Artt. 12 ff. DS-GVO verhindert werden kann, oder ob die genannten Vorschriften nicht grundsätzlich anders konzipiert werden müssten.[92] Eine Rechtspflicht zu einem gestuften Ansatz könnte ein Schritt in diese Richtung sein.

91 S. bzgl. der Einzelheiten die Ausführungen unter 8.

92 S. zur grundlegenden Kritik an den Informationspflichten der Artt. 13 f. *Ebner*, Weniger ist Mehr?, 2022 und *Roßnagel/Geminn*, Datenschutz-Grundverordnung verbessern, 2020, 62 ff., 121 ff.

7. Mögliche Reaktionen von SelbstvermesserInnen auf fehlende Transparenz

Die SelbstvermesserInnen wären dazu bereit, den Anbieter bei einem eingeführten Zwang zur Datenfreigabe zu wechseln. Ein anderer Anreiz den Anbieter zu wechseln, wäre ein Fehlverhalten des bisherigen Anbieters in dem Sinne, dass er Daten ohne die Einwilligung der betroffenen Person oder eine andere Rechtsgrundlage an Dritte weiterleitet, oder allgemein gegen die Datenschutz-Grundverordnung verstößt. Zu beachten ist jedoch, dass die InterviewpartnerInnen überwiegend nicht darauf vertrauen, dass sich die verschiedenen Anbieter auch im Umgang mit den verarbeiteten Daten unterscheiden. Ein Privacy Assistent kann auch insofern die SelbstvermesserInnen bei der Auswahl von zu ihren Datenschutzpräferenzen passenden Wearables und Selbstvermessungs-Apps unterstützen, sofern sich die Anbieter in ihren Praktiken im Hinblick auf den Datenschutz unterscheiden. Ein weiterer Grund, der nach Ansicht der SelbstvermesserInnen gegen einen Anbieterwechsel spricht, ist die Gewöhnung an das bereits verwendete Gerät bzw. die verwendete App.

8. Technische Umsetzungsmöglichkeiten

Eine Möglichkeit zur Schaffung von Transparenz bezüglich des Umgangs mit Selbstvermessungsdaten ist die Schaffung eines Privacy Assistenten, welcher die NutzerInnen hierbei durch eine geeignete Bereitstellung der benötigten Informationen unterstützt. Als Basis für die Umsetzung eines Privacy Assistenten wird ein Datenmodell benötigt, das die Eigenschaften der verschiedenen Selbstvermessungsgeräte abbildet und weitere Aspekte, etwa die rechtliche Einordnung der jeweiligen Daten oder Informationen hinsichtlich der NutzerInnenpräferenzen für eine adaptive Gestaltung der Nutzungsschnittstelle, beinhaltet. Für die Umsetzung solcher, stark vernetzter Datenstrukturen eignet sich z. B. die objektorientierte Modellierung, die auch von gängigen Standards unterstützt wird, etwa der visuellen Modellierungssprache UML.[93]

8.1 Schaffung von Transparenz

Bei der Untersuchung der Bedürfnisse von SelbstvermesserInnen zeigte sich, dass diesen Transparenz einerseits relativ wichtig ist und sie die der-

93 *OMG,* About the Unified Modelling Language Specification Version 2.5.1.

zeitige Gestaltung ihrer Selbstvermessungs-Apps und Wearables für nicht transparent halten, sie andererseits gleichzeitig nicht zu viele Informationen und diese in einer ansprechenden Weise dargestellt bekommen möchten.

Ein Lösungsansatz, um dies zu erreichen, ist die Entwicklung eines interaktiven Systems. Hierbei können interaktive Systeme Informationen zielgerichteter darstellen als z. B. ein langer statischer Text (Datenschutzerklärung), da es dem/der BenutzerIn ermöglicht wird, durch die Informationen zu navigieren und nur die Teile anzuzeigen, die auf die jeweilige Situation angepasst und für diese am relevantesten sind. Hierdurch werden die Informationen situationsgerecht sowie in der gewünschten Tiefe mitgeteilt. Insgesamt können interaktive Systeme dazu beitragen, dass BenutzerInnen Informationen schneller und effektiver aufnehmen und verarbeiten können. Daher bietet sich die Umsetzung des Privacy Assistenten als interaktives System an. Hierzu wurden im Projekt TESTER Methoden aus den Bereichen der Usability und User Experience verwendet, um Mock-Ups für die Gestaltung eines solchen interaktiven Systems zu erstellen.

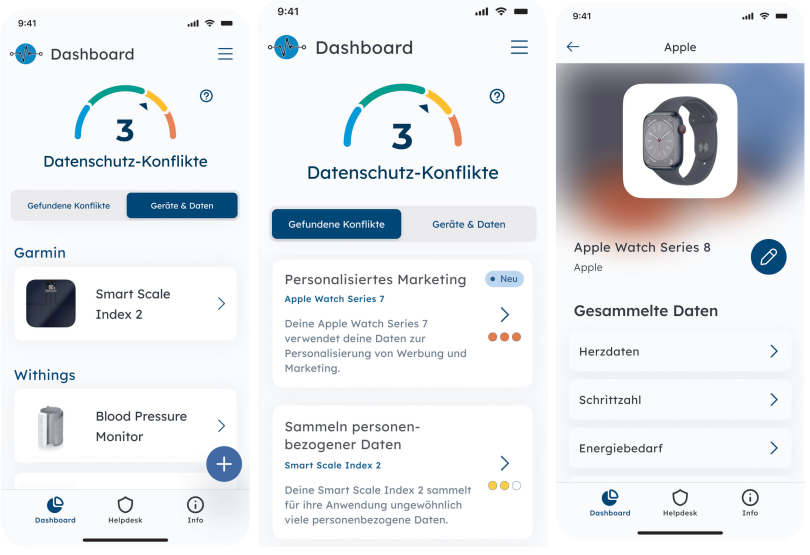

Abbildung 1: Screenshot Mock-Ups: Privacy Assistant

Grundprinzip bei der Gestaltung des Privacy Assistenten ist es, den Umgang eines verwendeten Selbstvermessungssystems mit den gewählten Präferenzen der NutzerInnen abzugleichen, und die Abweichungen von dem

erwarteten Umgang mit den Daten gezielt aufzuzeigen. Hierdurch soll ein kompakter sowie schneller Überblick geschaffen werden, welcher ohne großen Aufwand Transparenz für die NutzerInnen herstellen soll. Die Gestaltung der Nutzungsschnittstelle wird anhand der in Abbildung 1 exemplarisch dargestellten Mock-Ups in NutzerInnentests validiert. Im nächsten Schritt wird der Privacy Assistent als erster funktionaler Demonstrator umgesetzt werden, sodass weitere NutzerInnentests mit der vollen Funktionalität des Systems durchgeführt werden. Hiernach soll eine angepasste Variante des Privacy Assistenten in das Produkt eines Telemedizin-Anbieters integriert werden. Hierdurch können weitere Untersuchungen in einem realen Umfeld mit echten AnwenderInnen durchgeführt werden. Zudem stellt dieses Szenario eine Möglichkeit dar um aufzuzeigen, wie die Schaffung von Transparenz für Anbieter solcher Selbstvermessungssysteme zu realisieren ist.

8.2 Unterstützung von Intervention

Um neben der Schaffung von Transparenz auch die Wahrnehmung der Betroffenenrechte aus der Datenschutz-Grundverordnung zu erleichtern, verfolgt TESTER zwei Ansätze, die im Projekt validiert werden. Ein erster Ansatz ist die Schaffung einer Softwareschnittstelle, über welche es den NutzerInnen ermöglicht wird, bestimmte Betroffenenrechte, wie z. B. die Rechte auf Berichtigung, auf Löschung oder auf Auskunft auszuüben. Die Schnittstelle soll unter Nutzung gängiger Web-Standards umgesetzt werden und ebenfalls in das Produkt des am Projekt beteiligten Telemedizin-Anbieters integriert werden.

Da nicht davon ausgegangen werden kann, dass alle Anbieter von Selbstvermessungssystemen eine solche Schnittstelle in ihre Systeme integrieren werden, wird als zweite Variante ein Generator für Datenschutzanfragen auf klassischem Wege (z. B. per E-Mail) entwickelt und erprobt. Hierbei werden aufbauend auf den im Datenmodell hinterlegten Informationen über die Betroffenenrechte hinsichtlich der jeweiligen Daten und der NutzerInnenwünsche vorgefertigte Textblöcke mittels einer Template Engine[94] angepasst und kombiniert. Durch dieses Verfahren können auf das jeweilige datenschutzrechtliche Anliegen abgestimmte Anfragen generiert werden, um die entsprechende Reaktion seitens des Anbieters zu veranlassen.

94 *Apache*, The Apache Velocity Project.

9. Fazit und Ausblick

Zusammenfassend lässt sich zunächst feststellen, dass aufgrund sinkender Kosten und besserer Sensorik infolge des technischen Fortschritts insgesamt sowie der Verbreitung des Internets der Dinge mehr Möglichkeiten der Selbstvermessung für Privatpersonen bestehen. Die erhebliche Menge der dabei verarbeiteten Daten ermöglicht eine präventive, zunehmend personalisierte Gesundheitsversorgung, bei der auch die betroffenen Personen eine aktive Rolle einnehmen können, jedoch gleichzeitig datenschutzrechtlichen Herausforderungen ausgesetzt sind.

In der durchgeführten, halbstrukturierten Interviewstudie, die aus insgesamt vier Inhaltsblöcken bestand und anhand einer qualitativen Inhaltsanalyse nach Mayring ausgewertet wurde, zeigte sich, dass bei der Selbstvermessung die Motive der Selbstverbesserung, des Lebensstils, der Achtsamkeit, der Statistik und Gamifizierung, der sportlichen Leistung und deren Überwachung und der Gesundheit vorherrschend sind. Alle Interviewten haben ein mittleres bis hohes Vertrauenslevel bezüglich der Gewährleistung ihrer Privatsphäre durch die Anbieter und schätzen die Wichtigkeit von Transparenz insgesamt tendenziell höher ein als die der Intervenierbarkeit.

Aus den Ergebnissen der Interviewstudie wurden Personas erstellt, bei denen der Selbstvermessung unterschiedliche Motive zugrunde liegen und das Vertrauen in die Gewährleistung der eigenen Privatsphäre durch die Anbieter der genutzten Selbstvermessungs-Apps und Wearables variiert. Zum Teil erfolgten bereits personalisierte Privatsphäreeinstellungen, und alle Personas sind der Verwendung eines Privacy Assistenten gegenüber grundsätzlich aufgeschlossen.

Der Transparenzgrundsatz ist in deutschen und europäischen Grundrechten verankert und wurde erstmals ausdrücklich in Art. 5 Abs. 1 lit. a Alt. 3 DS-GVO als Strukturprinzip normiert. Daneben finden sich konkrete Informationspflichten sowie Vorgaben in Bezug auf die Art und Weise der Übermittlung der Anbieter als datenschutzrechtlich Verantwortliche in den Artt. 12 ff. DS-GVO. Dass Transparenz mehr sein muss als die bloße Übermittlung aller in den Artt. 13 f. DS-GVO aufgeführten Informationen zeigt sich schon daran, dass ein Verstoß gegen das Strukturprinzip der Transparenz einerseits und gegen die Informationspflichten andererseits jeweils bußgeldbewehrt ist, was die Frage nach deren Verhältnis aufwirft. Worin genau dieses „Mehr" besteht, ist indes bisher ebenso ungeklärt, wie die Frage, inwiefern Informationspflichten des Verantwort-

lichen von den Wünschen der SelbstvermesserInnen als betroffenen Personen abhängig gemacht werden können und sollten.

Eine Möglichkeit der Herstellung von Transparenz kann der Einsatz eines Privacy Assistenten als interaktives System sein, das die personalisierte und interaktive Ver- und Übermittlung von Informationen ermöglicht, die an die Bedürfnisse der NutzerInnen angepasst ist. Transparenz ist darüber hinaus auch eine Voraussetzung für die effektive Ausübung von Betroffenenrechten durch die SelbstvermesserInnen, weshalb der Privacy Assistent diese durch die Schaffung einer Softwareschnittstelle zur direkten Ausübung und alternativ durch die automatische Generierung von Textvorlagen unterstützen soll.

Da derzeit keine Indizien für eine Änderung der grundsätzlichen Konzeption der Transparenzinstrumente der Datenschutz-Grundverordnung erkennbar sind und die Datenverarbeitung im Alltag der SelbstvermesserInnen absehbar weiter zunehmen wird, werden technische Umsetzungsmöglichkeiten eine immer wichtigere Rolle spielen, um die gelebte Nutzungsrealität mit den Erwartungen der SelbstvermesserInnen und den Vorgaben der Datenschutz-Grundverordnung in Einklang zu bringen.

Literatur

Ajana, Btihaj (2017): Digital health and the biopolitics of the Quantified Self. *Digital Health*, 3, S. 1-18. https://doi.org/10.1177/2055207616689509.

Ajana, Btihaj (2020): *Metric Culture: Ontologies of Self-Tracking Practices*. Bingley: Emerald Publishing Ltd.

Apache (2023): The Apache Velocity Project. URL: https://velocity.apache.org/ (besucht am 28.02.2023).

Art-29-Datenschutzgruppe (2018): *Leitlinien für Transparenz gemäß der Verordnung 2016/679*. URL:https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html (besucht am 28.02.2023).

Berry, Rachel A.; Rodgers, Rachel F. und Campagna, Jenna (2021): Outperforming iBodies: A Conceptual Framework Integrating Body Performance Self-Tracking Technologies with Body Image and Eating Concers. *Sex Roles,* 85(1-2), S. 1-12.

Bol, Nadine; Helberger, Natali und Weert, Julia C. M. (2018): Differences in mobile health app use: A source of new digital inequalities? *The Information Society*, 34(3), 183–193. https://doi.org/10.1080/01972243.2018.1438550.

Brătucu, Gabriel; Tudor, Andra I. M.; Dovleac, Lavinia; Sumedrea, Silvia; Chitu, Ioana Bianca und Trifan, Adrian (2020): The Impact of New Technologies on Individuals' Health Perceptions in the European Union. *Sustainability*, 12(24), 10349. https://doi.org/10.3390/su122410349.

BVerfG (1984): Verfassungsrechtliche Überprüfung des Volkszählungsgesetzes 1983. *Neue Juristische Wochenschrift (NJW),* 37(8), S. 419-428.

Calliess, Christian und Ruffert, Matthias (Hrsg.) (2022): *Kommentar EUV/AEUV mit Europäischer Grundrechtecharta*. München: C.H.Beck.

DIN EN ISO (2020): *DIN EN ISO 9241-210, Ergonomie der Mensch-System-Interaktion – Teil 210: Menschzentrierte Gestaltung interaktiver Systeme*. Berlin: Beuth Verlag GmbH.

Ebner, Gordian K. (2022): Information Overload 2.0? Datenwirtschaftsrecht IV: Die Informationspflichten gem. Art. 3 Abs. 2 Data Act-Entwurf. *Zeitschrift für Datenschutz (ZD)*, 12(7), 364-369.

Ebner, Gordian K. (2022): *Weniger ist Mehr? Die Informationspflichten der DS-GVO – Eine kritische Analyse*. Baden-Baden: Nomos.

Ehmann, Eugen und Selmayr, Martin (Hrsg.) (2018): *Kommentar DS-GVO*. München: C.H.Beck.

Europäischer Datenschutzausschuss (2020): *Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679*. (Abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_de).

Europäische Kommission (2014): Greenpaper on mobile health („mHealth"). URL: https://digital-strategy.ec.europa.eu/en/library/green-paper-mobile-health-mhealth (besucht am 28.02.2023).

Eßer, Martin; Kramer, Philipp und von Lewinski, Kai (2020): *Auernhammer Kommentar DS-GVO/BDSG*. Köln: Carl Heymanns.

Filkins, Barbara. L.; Kim, Ju Young; Roberts, Bruce; Armstrong, Winston; Miller, Mark A.; Hultner, Michael L.; Castillo, Anthony P.; Ducom, Jean-Christophe; Topol, Eric J. und Steinhubl, Steven R. (2016): Privacy and security in the era of digital health: What should translational researchers know and do about it? *American journal of translational research*, 8(3), S. 1560-1580.

Freye, Merle (2022): Die Datenschutzerklärungen von Gesundheits-Apps. *Datenschutz und Datensicherheit (DuD),* 46(12), S. 762-766.

Geis, Thomas und Tesch, Guido (2019): *Basiswissen Usability und User Experience: Aus- und Weiterbildung zum UXQB® Certified Professional for Usability and User Experience (CPUX) – Foundation Level (CPUX-F).* Heidelberg: dpunkt.verlag.

Gerpott, Torsten J. und Mikolas, Tobias (2021): Lesbarkeit von Datenschutzerklärungen großer Internethändler in Deutschland Ergebnisse einer empirischen Studie. *MultiMedia und Recht (MMR)*, 24(12), S. 936-941.

Gola, Peter und Heckmann, Dirk (Hrsg.) (2022): *Kommentar DS-GVO/BDSG*. München: C.H.Beck.

Hermstrüwer, Yoan (2016): *Informationelle Selbstgefährdung Zur rechtsfunktionalen, spieltheoretischen und empirischen Rationalität der datenschutzrechtlichen Einwilligung und des Rechts auf informationelle Selbstbestimmung*. Tübingen: Mohr Siebeck.

Heselhaus, Sebastian und Nowak, Carsten (Hrsg.) (2020): *Handbuch der Europäischen Grundrechte*. München: C.H.Beck.

Hussy, Walter; Schreier, Margrit und Echterhoff, Gerald (2013): *Forschungsmethoden in Psychologie und Sozialwissenschaften für Bachelor*. Berlin und Heidelberg: Springer.

Jarass, Hans D. (Hrsg.) (2021): *Kommentar Charta der Grundrechte der Europäischen Union*. München: C.H. Beck.

Kahana, Eva und Kahana, Boaz (2001): On being a proactive health care consumer: Making an „unresponsive" system work for you. In: Kronefeld, Jennie J. (Hrsg.): *Changing Consumers and Changing Technology in Health Care and Health Care Delivery*. Bingley: Emerald Publishing Ltd, S. 21-44. https://doi.org/10.1016/S0275-4959(01)80005-3.

Kuckartz, Uda (2010): *Einführung in die computergestützte Analyse quantitativer Daten*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Kühling, Jürgen und Buchner, Benedikt (Hrsg.) (2020): *Datenschutz-Grundverordnung BDSG Kommentar*. München: C.H.Beck.

Lupton, Deborah (2016): The diverse domains of quantified selves: self-tracking modes and dataveilance. *Economy and Society*, 45(1), S. 101-122.

Manthey, Benjamin (2020): *Das datenschutzrechtliche Transparenzgebot Die Grenzen des individuellen Datenschutzes anhand verdeckter Datenverarbeitungen im Internet*. Baden-Baden: Nomos.

Mayring, Philipp (2015): *Qualitative Inhaltsanalyse*. Weinheim: Beltz.

Meyer, Jürgen und Hölscheidt, Sven (Hrsg.) (2019): *Kommentar Charta der Grundrechte der Europäischen Union*. Baden-Baden: Nomos.

Michl, Walther (2017): Das Verhältnis zwischen Art. 7 und Art. 8 GRCh zur Bestimmung der Grundlage des Datenschutzgrundrechts im EU-Recht. *Datenschutz und Datensicherheit (DuD)*, 41(6), S. 349-353.

OMG (2023): About the Unified Modelling Language Specification Version 2.5.1. URL: https://www.omg.org/spec/UML/2.5.1/About-UML (besucht am 28.02.2023).

Paal, Boris P. und Pauly, Daniel A. (Hrsg.) (2021): *Kommentar DS-GVO/BDSG*. München: C.H.Beck.

Roßnagel, Alexander (2018): Datenschutzgrundsätze unverbindliches Programm oder verbindliches Recht? Bedeutung der Grundsätze für die datenschutzrechtliche Praxis. *Zeitschrift für Datenschutz (ZD)*, 9(8), S. 339-344.

Roßnagel, Alexander (2019): Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht – Zur Dogmatik der Datenverarbeitung als Grundrechtseingriff. *Neue Juristische Wochenschrift (NJW)*, 72(1-2), S 1-5.

Roßnagel, Alexander und Geminn, Christian (2020): *Datenschutz-Grundverordnung verbessern – Änderungsvorschläge aus Verbrauchersicht*. Baden-Baden: Nomos.

Schwartmann, Rolf; Jaspers, Andreas; Thüsing, Gregor und Kugelmann, Dieter (Hrsg.) (2020): *Kommentar DS-GVO/BDSG*. Heidelberg: C.F. Müller.

Sharon, Tamar (2017): Self-Tracking for Health and the Quantified Self: Re-Articulating Autonomy, Solidarity, and Authenticity in an Age of Personalized Healthcare. *Philosophy & Technology,* 30(1), S. 93-121. https://doi.org/10.1007/s13347-016-0215-5.

Simitis, Spiros; Hornung, Gerrit und Spiecker genannt Döhmann, Indra (Hrsg.) (2019): *Kommentar Datenschutzrecht*. Baden-Baden: Nomos.

Šmahel, David; Macháčková, Hana; Šmahelová, Martina; Čevelíček, Michal; Almenara, Carlos A. und Holubčíková, Jana (2018): *Digital Technology, Eating Behaviors, and Eating Disorders*. Cham: Springer.

Stiglbauer, Barbara; Weber, Silvana und Batinic, Bernad (2019): Does your health really benefit from using a self-tracking device? Evidence from a longitudinal randomized control trial. *Computers in Human Behaviour*, 94, S. 131-139. https://doi.org/10.1016/j.chb.2019.01.018.

Streinz, Rudolf und Michl, Walther (2011): Die Drittwirkung des europäischen Datenschutzgrundrechts (Art. 8 GRCh) im deutschen Privatrecht. *Europäische Zeitschrift für Wirtschaftsrecht (EuZW)*, 22(10), S. 384-388.

Swan, Melanie (2012): Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensor and Actuator Networks*, 1(3), S. 217-253.

Sydow, Gernot und Marsch, Nikolaus (Hrsg.) (2022): *DS-GVO BDSG Datenschutz-Grundverordnung Bundesdatenschutzgesetz Handkommentar*. Baden-Baden: Nomos.

Taeger, Jürgen und Gabel, Dettlev (2022): *Kommentar DSGVO - BDSG - TTDSG*. Frankfurt (Main): Recht und Wirtschaft.

Van Hoof, Chris; Baert, Kris und Witvrouw, Ann (2004): The Best Materials for Tiny, Clever Sensors. *Science*, 306 (5698), S. 986-987. doi/10.1126/science.1100080.

Vitak, Jessica; Liao, Yuting; Kumar, Priya; Zimmer, Michael und Kritikos, Katherine (2018): Privacy Attitudes and Data Valuation Among Fitness Tracker Users. *Transforming Digital Worlds*. S. 229-239. Cham: Springer. https://doi.org/10.1007/978-3-319-78105-1_27.

Voigt, Marlene (2020): *Die datenschutzrechtliche Einwilligung Zum Spannungsfeld von informationeller Selbstbestimmung und ökonomischer Verwertung personenbezogener Daten*. Baden-Baden: Nomos.

Wieczorek, Michal; O'Brolchain, Fiachra; Saghai, Yashar und Gordijn, Bert (2023): The ethics of self-tracking. A comprehensive review of the literature. *Ethics & Behavior*, 33(4), S. 239-271. https://doi.org/10.1080/10508422.2022.2082969.

Wolff, Heinrich Amadeus und Brink, Stefan (Hrsg.) (2023): *Beck'scher Online-Kommentar Datenschutzrecht*. München: C.H.Beck.

Social Media und das algorithmische Streben nach „Vertrauenswürdigkeit“

Florian Müller

Zusammenfassung

Social-Media-Plattformen zählen zu den meistgenutzten digitalen Diensten überhaupt. Dabei verbinden diese Plattformen jedoch nicht nur Nutzerzahlen im Milliardenbereich sowie eine außerordentlich hohe gesellschaftliche Bedeutung. Wie dieser Beitrag argumentiert, kennzeichnet diese Plattformen auch ein gewisses Spannungsgefüge, das sich zwischen traditionell mit Privatheit assoziierten Werten einerseits und normativen Erwartungen, die mit Vertrauenswürdigkeit in eine Beziehung gesetzt werden andererseits aufspannt. Dieses Spannungsgefüge ist sowohl Ausdruck von Wandlungsprozessen, welche die gesellschaftliche Wahrnehmung sowie die institutionelle Regulierung von Social-Media-Plattformen betreffen, als auch charakteristisch dafür, wie diese Plattform-Unternehmen sich und ihre algorithmischen Koordinations- und Regelungssysteme in Verbindung mit diesen Wandlungsprozessen nun präsentieren und positionieren.

1. Einführung

> *„Our mission is to give everyone a voice and show them the world. We believe that everyone deserves to have a voice, and that the world is a better place when we listen, share and build community through our stories”* (YouTube 2023a)

Social-Media-Plattformen, wie bspw. Facebook, YouTube, Instagram, Twitter oder TikTok, zählen schon seit geraumer Zeit zu den meistgenutzten digitalen Diensten überhaupt. Milliarden von Menschen nutzen diese Plattformen alltäglich, um sich mit anderen auszutauschen, um sog. Gemeinschaften zu gründen und zu pflegen, um sich unterhalten zu lassen, Nachrichten zu konsumieren, ökonomisches Kapital zu akkumulieren und vieles mehr.

Dabei verbindet diese Dienste, bzw. die Unternehmen, die sich hinter diesen Diensten verbergen, jedoch nicht nur Nutzerzahlen im Milliardenbereich[1] und damit einhergehend eine außerordentlich hohe gesellschaftliche Bedeutsamkeit. Wie im Folgenden nun vor allem mit Blick auf YouTube diskutiert werden soll, charakterisiert diese Plattformen auch ein gewisses Spannungsgefüge, welches sich zwischen traditionell mit Privatheit assoziierten Werten einerseits sowie mit Vertrauenswürdigkeit in eine Beziehung gesetzte normative Erwartungen andererseits aufspannt. Dieses wertbehaftete und normativ aufgeladene Spannungsgefüge ist dabei, wie argumentiert wird, sowohl Ausdruck von Wandlungsprozessen, welche die gesellschaftliche Wahrnehmung sowie die institutionelle Regulierung von Social Media Plattform-Unternehmen betreffen als auch charakteristisch dafür, wie diese Plattform-Unternehmen sich und ihre algorithmischen Koordinations- und Regelungssysteme, in Anbindung an diese Wandlungsprozesse, nun präsentieren und positionieren.

2. Zum traditionellen Branding von Social-Media-Plattformen

Seit ihrer Geburtsstunde bewerben und assoziieren große Social Media Plattform-Unternehmen – durchaus auch in strategischer und bewusster Abgrenzung zu den traditionellen Massenmedien – ihre Dienste mit einem Beteiligungsversprechen, mit gesteigerten Partizipationsmöglichkeiten („User Empowerment") (Schmidt 2018, S.97) sowie mit Werten wie Authentizität und Selbstverwirklichung. Ein jeder solle eine Stimme bekommen und ganz nach dem lange Zeit offiziellen Motto von YouTube – „Broadcast Yourself" - die Möglichkeit dazu erhalten, sich und sein authentisches Selbst in diesen „neuen" Handlungs- und Erfahrungsräumen zu präsentieren und zu verwirklichen.

Im Fokus des traditionellen Branding von Social-Media-Plattformen steht adäquat hierzu das Individuum, welches nun dazu ermächtigt wird „*to share and make the world more open and connected*" (Facebook 2011), „*[to] create and share ideas and information instantly, without barriers*" (Twitter 2013) sowie „*to become the broadcasters of tomorrow*" (YouTube 2006). Die Plattform-Unternehmen setzen ihre Dienste damit wesentlich mit Werten in eine

1 Bis auf Twitter (0,56 Mrd.) haben die anderen genannten Plattformen (Facebook, 2,96 Mrd.; Instagram, 2,00 Mrd.; TikTok, 1,05 Mrd.; YouTube, 2,51 Mrd.) alle mehr als eine Milliarde sog. monatlich aktive NutzerInnen (Statista 2023).

Beziehung, die vor allem in einem modernen Verständnis mit Privatheit assoziiert werden[2].

Passend zu diesem Bild des selbstbestimmten und verantwortlichen Individuums bzw. Nutzers, inszenieren sich die Plattform-Unternehmen selbst lange Zeit erfolgreich als neutrale Intermediäre, die mit ihren wertfreien Infrastrukturen Möglichkeiten generieren, ohne selbst eine (allzu) aktive Rolle zu bekleiden. Anstatt selbst in Diskurse einzugreifen seien diese Plattformen - wie sich bspw. auch in verschiedenen Reden von Mark Zuckerberg[3] widerspiegelt - vielmehr „facilitators" von „free speech" bzw. „free expression", was wiederum vor allem auch in einer Charakterisierung von algorithmischen Systemen über deren technische Objektivität und Neutralität Ausdruck findet.[4]

Wie Gillespie vor allem mit Blick auf den Plattform-Begriff argumentiert, rahmen und positionieren diese Unternehmen ihre Dienste damit in einer Weise, die gleich in mehreren Hinsichten für das Unternehmen und dessen Geschäftsmodell strategisch günstig ist:

„They do so strategically, to position themselves both to pursue current and future profits, to strike a regulatory sweet spot between legislative protections that benefit them and obligations that do not, and to lay out a cultural imaginary within which their service makes sense (...)." (Gillespie 2010, S. 348)

Bis heute bilden dabei Authentizität, User-Empowerment, Selbstbestimmung und Selbstverwirklichung zentrale Bausteine des Branding und der diskursiven Arbeit von Social-Media-Plattformen. Auffallend ist dabei jedoch auch, dass im Zuge dieser Erfolgs- und Wachstumsgeschichten großer

2 Im Zuge ihres historischen Strukturwandels wurde "Privatheit" bereits mit verschiedenen Werten in eine Beziehung gesetzt. Vor allem in sog. "modernen Gesellschaften" wird das Private dabei wesentlich als eine Sphäre charakterisiert, welche der Individualität, der Selbstverwirklichung, der Autonomie und der Authentizität dient (vgl. Hans 2017). In den Sozialwissenschaften werden Social-Media-Plattformen folglich auch gerne als Beschleuniger einer ohnehin schon diagnostizierten "Intimisierung oder Privatisierung des Öffentlichen" interpretiert. Somit stellt sich, vor allem auch mit Blick auf Social-Media-Plattformen, die Frage, inwiefern auch die Werte, die mit Privatheit assoziiert werden, im Zuge dieser Intimisierung bzw. Privatisierung, eine Transformation und einen Bedeutungswandel erfahren.

3 Siehe hierzu bspw. folgende Veröffentlichung von Meta, bzw. folgende Rede von Mark Zuckerberg: "Mark Zuckerberg Stands for Voice and Free Expression" (Meta 2019).

4 Der aktuelle CEO von Twitter - Elon Musk - bezeichnete sich selbst sogar als „free speech absolutist" (Pearce 2022). Wie sich anhand zahlreicher Zeitungsartikel zeigt, ist ihm dieser Titel nach seiner Übernahme von Twitter und verschiedenen fragwürdigen Regulierungsentscheidungen dann durchaus zum Verhängnis geworden (siehe bspw. Krause 2022/ Suciu 2023).

Social-Media-Plattformen deren Image und Positionierung als neutraler und wertfreier Vermittler, welcher frei von Verantwortlichkeiten ist, zunehmend Risse bekommen hat.

3. Zur neuen Verantwortlichkeit von Social Media Plattform-Unternehmen

In den aktuellen Positionierungsbestrebungen der Plattform-Unternehmen findet dieser Wandel insofern einen Ausdruck, als dass nun verstärkt auch von der eigenen Verantwortung, von Vertrauen und Vertrauenswürdigkeit die Rede ist.

So präsentiert sich bspw. YouTube zwar immer noch als *„eine offene Videoplattform, auf der jeder Videos hochladen und mit der Welt teilen kann"*, betont jedoch gleichzeitig auch, dass diese Offenheit *„einige Herausforderungen mit sich"* bringt und dass sie als Plattform-Unternehmen ständig darum bemüht sind, *„ein Gleichgewicht zwischen kreativem Ausdruck und unserer Verantwortung für den Schutz der Community vor schädlichen Inhalten herzustellen"* (YouTube 2023b).[5]

Auch mit Blick auf die aktuellen sog. „Missionen' von Social-Media-Plattformen wie Facebook oder Twitter fällt auf, dass es nicht mehr nur um freie Meinungsäußerung und Selbstbestimmung geht. Vielmehr geht es nun vor allem auch darum, ein gewisses Gleichgewicht herzustellen und Verantwortung zu übernehmen, die in der Stärkung und dem Schutz der Community sowie dem Aufbau von Vertrauen eine wesentliche Zielsetzung und Begründung findet.

An die Stelle des wertfreien und neutralen Intermediärs rücken, im Fall von YouTube, vier Prinzipien[6], die Ausdruck der (neuen) Verantwortung und Agenda des Plattform-Unternehmens sind:

---

5 Seit neuestem gibt es auf YouTube sogar eine eigene Website, auf welcher „YouTube's Responsibility Efforts" thematisiert und gesammelt werden. Dort heißt es ausdrücklich: *„At YouTube, we're committed to building a responsible platform our users, creators, and artists can rely on, and over the years, we've made huge progress making our community safer"* (YouTube 2023d).

6 Hierbei ist anzumerken, dass es auf Social-Media-Plattformen sicherlich schon immer Richtlinien und Prinzipien gab, die dem Geschehen auf der Plattform zugrunde liegen. Der qualitative Unterschied, über welchen sich das "neue Verantwortungsbewusstsein" von Social Media Plattform-Unternehmen ausdrückt, besteht nun aber darin, dass diese zunehmend selbst Verantwortung für die Umsetzung dieser Richtlinien übernehmen. Zuvor haben Social Media Plattform-Unternehmen, passend zu den in Szene gesetzten Images des "selbstbestimmten Plattform-Nutzers" und des "wertfreien und

„Wir entfernen richtlinienwidrige Inhalte schnellstmöglich, schränken die Verbreitung schädlicher Fehlinformationen und grenzwertiger Inhalte ein, stufen Inhalte aus verlässlichen Quellen hoch, wenn Nutzer nach Nachrichten und Informationen suchen, und belohnen vertrauenswürdige und berechtigte Creator und Künstler." (YouTube 2023b)

Dabei ist hervorzuheben, dass dieses „neue Verantwortungsbewusstsein" von Plattform-Unternehmen wohl nicht ganz freiwillig auf der Bildfläche erscheint, sondern vielmehr im Kontext einer sich im Laufe der Zeit gewandelten gesellschaftlichen, medialen, wissenschaftlichen und staatlichen Wahrnehmung und Rezeption der Plattform-Unternehmen steht und zu betrachten ist[7]. Vor allem ab Mitte der 2010er-Jahre wurden so, bspw. mit Blick auf die Geschäftsmodelle von Social Media Plattform-Unternehmen sowie im Anschluss an diverse Datenskandale, zunehmend deren datenverarbeitende und privatheitsverletztende Praktiken thematisiert und kritisiert. Es wurde, u.a. in Bezug auf den Vorwurf der Manipulation von Nutzenden und „Biases" von Algorithmen, auf die durchaus problematische Macht und den Einfluss dieser Unternehmen aufmerksam gemacht, und mit Begriffen bzw. Phänomenen wie „Fake News", „Hate Speech", „Echo Chambers" oder „Filter Bubbles" wurden problematische gesellschaftliche Effekte dieser Plattformen in den Fokus gerückt.[8]

Das lange Zeit implizite und stillschweigende Vertrauen in diese Plattform-Unternehmen wird durch diese Ereignisse und Diskurse problematisiert und in der Form von „Vertrauensproblemen", mit welchen Social Media Plattform-Unternehmen folglich konfrontiert werden, zu einem expliziten Phänomen.

Diese neue Form der Rechenschaft und Verantwortlichkeit von Plattform-Unternehmen spiegelt sich auch in verschiedenen institutionellen Regulierungsbestrebungen wider. Eine beachtliche Zeit lang wurden Social Media Plattform-Unternehmen, im Zuge ihres Versprechens der Selbstregulation, von staatlicher Seite nur schwach bzw. informell reguliert und haben hierdurch geschickt die Möglichkeit genutzt sich der eigenen Verant-

neutralen Intermediärs", die Verantwortung für die Umsetzung ihrer Richtlinien wesentlich an die NutzerInnen der Plattform delegiert.

7 Dies wird vor allem auch anhand der expliziten Thematisierung von Vertrauen deutlich, da Vertrauen vor allem dann explizit zum Thema gemacht wird, wenn es verletzt oder problematisiert wurde.

8 Siehe für eine umfassende Sammlung wissenschaftlicher Studien, welche die genannten Aspekte thematisieren, u.a.: Haidt & Twenge (ongoing) sowie Haidt & Bail (ongoing).

wortung zu entziehen, bzw. diese nach eigenem Ermessen auszulegen und umzusetzen. Dagegen verdeutlichen Verordnungen und Gesetze, wie bspw. das „Netzwerkdurchsetzungsgesetz" (Bundesministerium der Justiz 2017), der „Medienstaatsvertrag" (die Medienanstalten 2020) oder der ab Februar 2024 gültige „Digital Services Act" (Europäische Kommission 2023), dass diese Plattform-Unternehmen nun auch formell zunehmend in die Pflicht und Verantwortung genommen werden.

Die Thematisierung der eigenen Verantwortlichkeit durch die Social Media Plattform-Unternehmen sowie die Stilisierung von Vertrauenswürdigkeit oder mit Vertrauen assoziierten Werten und Normen zu einem Referenzrahmen und Gradmesser der plattform-eigenen Koordination und Regulierung zeigt sich vor diesem Hintergrund folglich als eine Form der Antwort auf die Explikation verschiedener Vertrauensprobleme sowie auf die hiermit in Beziehung stehenden neuen Anforderungen, mit welchen Plattform-Unternehmen nun umzugehen haben.

4. Zum algorithmischen Streben nach „Vertrauenswürdigkeit'

In Anbetracht der Frage, wie diese Plattform-Unternehmen nun mit diesen neuen Anforderungen und Verantwortlichkeiten umgehen, bzw. wie, mit Blick auf YouTube, die vier sog. Rs (Remove, Raise, Reduce, Reward) umgesetzt werden sollen, rückt vor allem ein Koordinations- und Regelungsmodus in den Mittelpunkt, der selbst vielfach kritisiert wurde und eine prominente Quelle von Vertrauensproblemen darstellt: die Rede ist von algorithmischen Verfahren bzw. algorithmischen Systemen.

Mit Blick auf die riesigen Datenmengen, die mittlerweile auf großen Social-Media-Plattformen verarbeitet werden, wird deutlich, dass die Vertrauensprobleme und die neue Verantwortung der Plattform-Unternehmen nicht nur auf einer qualitativen Ebene neue Herausforderungen mit sich bringen, sondern vor allem auch auf einer quantitativen Ebene: Auf YouTube werden mittlerweile pro Minute mehr als 500 Stunden Videomaterial hochgeladen (Jens 2021), Facebook User posten jede Minute 136.000 Fotos (Schultz 2019) und auf Twitter werden jede Minute etwa 456.000 Tweets gesendet (Schumacher 2021). So erscheinen automatisierte algorithmische Verfahren nun, der Argumentation der Plattform-Unternehmen folgend, als einzig mögliche und, wie die sog. „Transparenzberichte" der

Plattform-Unternehmen belegen sollen, als äußerst erfolgreiche Lösungen[9]. Bezeichnend hierfür ist auch, dass „Algorithmic Trust" im „Gartner Hype Cycle" aus dem Jahr 2020 zu einem von fünf bedeutenden technologischen Trends ernannt wurde (Panetta 2021). Algorithmische Koordinations- und Regelungssysteme, wie sie auf YouTube oder anderen Plattformen zum Einsatz kommen, um Inhalte zu filtern, zu empfehlen, auf ihre Monetarisierung zu prüfen, zu bewerben u.a., werden vor diesem Hintergrund, indem Vertrauen zu einem Referenzrahmen und Gradmesser ihrer Operationsweise erklärt wird, als Generatoren von Vertrauen in Szene gesetzt. Damit entscheiden diese Systeme aber nicht nur auf automatisierte Weise, was im jeweiligen Fall als „vertrauenswürdig" gilt und was nicht, sondern konditionieren über Anreiz- und Sanktionsmechanismen im gleichen Zuge auch Plattform-Nutzende, mit welchen sie in rekursiven Loops verklammert sind, zu einem in diesem Sinne „vertrauenswürdigen" Verhalten. Wer will, dass seine Inhalte auf YouTube monetarisiert und empfohlen werden, der muss vom System als ein vertrauenswürdiger und verlässlicher „Creator" eingeschätzt werden. Im Umkehrschluss kann Verhalten, welches gewisse Erwartungen verletzt oder nicht erfüllt und damit als nicht vertrauenswürdig gilt, verschiedene Sanktionen nach sich ziehen, die von der eigenen Unsichtbarkeit bis zur lebenslangen Sperrung reichen können.

Kontrastierend zur zuvor proklamierten Wertfreiheit und Neutralität dieser Systeme tritt das Algorithmische nun als eine Art Botschafter und Generator des Vertrauens und der Vertrauenswürdigkeit in Erscheinung. Auch wenn in YouTubes Community Guidelines betont wird *„Die YouTube-Community basiert auf Vertrauen*" (YouTube 2023c), zeigt sich nun mit Blick auf die Herstellung von „Vertrauenswürdigkeit" ein etwas anderes Bild: Vor dem Hintergrund der eigenen Rechenschaft und Verantwortung kontrollieren Social Media Plattform-Unternehmen wie YouTube, mit Hilfe algorithmischer Systeme und unter dem Banner der Vertrauenswürdigkeit, das Handeln und Verhalten ihrer NutzerInnen und richten dieses (zielorientiert) zu. Zum Zweck der Adressierung und Bearbeitung von Vertrauensproblemen wird das Vertrauen in Nutzende in diesem Sinne durch effizientere funktionale Äquivalente substituiert. Werte wie Authentizität, Selbstverwirklichung und Selbstbestimmung, die traditionell sowie nach wie vor einen wesentlichen Bestandteil des Branding von Social-Media-

9 Mit Evgeny Morozov (2013) kann man diese Stilisierung von algorithmischen Systemen als Lösungen verschiedener durchaus komplexer Probleme auch als „technological solutionism" interpretieren.

Plattformen bilden, werden damit überformt und gerahmt von normativen Erwartungen, welche wiederum Formen von Vertrauenswürdigkeit begründen. Kultur und Subjektivität auf Social-Media-Plattformen werden in diesem Sinne auf einen Erfahrungs- und Handlungsspielraum begrenzt, der wesentlich durch algorithmische Systeme und deren Streben nach Vertrauenswürdigkeit strukturiert und mitgestaltet wird. Im Zuge der Delegation von Verantwortlichkeit an die Plattform-Unternehmen und deren abermalige Delegation von Verantwortlichkeit an algorithmische Koordinations- und Regelungssysteme erscheint die Stilisierung von Vertrauenswürdigkeit als Gradmesser algorithmischer Aktivität vor diesem Hintergrund somit auch als eine wirksame Legitimationsstrategie für die außerordentliche Macht und Handlungsträgerschaft dieser Systeme.

Die Fragen, die an dieser Stelle jedoch gestellt werden müssen, sind: Wer entscheidet, wer oder was als vertrauenswürdig gilt und was nicht, was passiert mit Formen von Vertrauenswürdigkeit im Zuge ihrer technischen Übersetzung und Automatisierung und welchen Zielen und Motiven dienen diese Formgebungen und das damit verbundene „Streben nach Vertrauenswürdigkeit" tatsächlich[10]?

Insofern die Bestimmung von Vertrauenswürdigkeit auf die Hinterbühne und in die „Black Box' verlegt wird, gesellschaftlichen Aushandlungsprozessen entzogen wird und in Gestalt automatisierter Verfahren versucht wird zu fixieren, bleibt Plattform-Nutzenden letztlich nichts anderes als

10 Auch wenn Social Media Plattform-Unternehmen ihr "Streben nach Vertrauenswürdigkeit" vor allem durch den Schutz der Community und mit Bezug auf geteilte Moralvorstellungen begründen, so wurde im Zuge verschiedener Untersuchungen zu meiner Dissertation deutlich, dass es sich hierbei auch wesentlich um Formen der Koordination und Regelung handelt, durch welche verschiedene Markt- und Machtpositionen formiert und gestärkt werden, die letztlich dem Geschäftsmodell des Plattform-Unternehmens dienen. So verdeutlicht bspw. die Verteilung von Zugriffs- und Nutzungsrechten an YouTubes sog. „Content ID" – einem System zur automatischen Identifizierung von Inhalten -, dass große Rechteinhaber bei Copyright-Fragen, im Vergleich zu "gewöhnlichen Plattform-Nutzenden", einen Vertrauensvorschuss und eine privilegierte Stellung genießen. Ähnliches zeigt sich auch mit Blick auf andere (algorithmische) Koordinationssysteme, wie bspw. dem Empfehlungssystem oder dem Monetarisierungssystem, deren Operationsweise wesentlich mit Richtlinien von Werbetreibenden („advertiser friendly guidelines") verschränkt ist und folglich auch Formen von "Vertrauenswürdigkeit" generiert und vermittelt, die an Maßstäben wie "Werbefreundlichkeit" und "Werbepassung" ausgerichtet sind. Zwischen der diskursiven Rahmung des "Strebens nach Vertrauenswürdigkeit" und dessen praktischer Umsetzung besteht in diesem Sinne eine gewisse Diskrepanz, die auf verschiedene Weise zwar zum Ausdruck kommt, aufgrund weitgehend intransparenter algorithmischer Operationsweisen jedoch weitgehend auch im Verborgenen gründet.

diesen Verfahren und Systemen selbst zu vertrauen oder an sie zu glauben. Aber wie vertrauenswürdig sind diese automatisierten Problemlöser und Vertrauensgeneratoren tatsächlich (selbst) und für wen?

Literatur

Facebook (2011): About Facebook. URL: https://web.archive.org/web/20110401002753mp_/http://www.facebook.com/facebook?sk=info (besucht am 16.02.2023).

Gillespie, Tarleton (2010): The Politics of 'Platforms'. *New Media & Society*, 12(3), S. 347-364. doi: 10.1177/1461444809342738.

Haidt, Jonathan und Bail, Chris (ongoing): Social media and political dysfunction: A collaborative review. Unpublished manuscript, New York University. URL: https://tinyurl.com/PoliticalDysfunctionReview (besucht am 16.02.2023).

Haidt, Jonathan und Twenge, Jean (ongoing). Social media and mental health: A collaborative review. Unpublished manuscript, New York University. URL: tinyurl.com/SocialMediaMentalHealthReview (besucht am 16.02.2023).

Hans, Barbara (2017): *Inszenierung von Politik. Zur Funktion von Privatheit, Authentizität, Personalisierung und Vertrauen*. Wiesbaden: Springer Fachmedien.

Jens (29. Dez. 2021): YouTube: Nutzer laden 500 Stunden Videomaterial pro Minute hoch & Google entwickelt neuen Encoding-Chip. GoogleWatchBlog. URL: https://www.googlewatchblog.de/2021/12/youtube-nutzer-stunden-videomaterial-2-chip/ (besucht am 16.02.2023).

Krause, Daniel (20. Dez. 2022): „Der Vogel ist frei“: Was Elon Musk unter Meinungsfreiheit versteht. *Tagesspiegel*. URL: https://www.tagesspiegel.de/wirtschaft/der-vogel-ist-frei-was-elon-musk-unter-meinungsfreiheit-versteht-9067603.html (besucht am 17.02.2023).

Meta (17. Okt. 2019): Mark Zuckerberg Stands for Voice and Free Expression. Meta Newsroom. URL: https://about.fb.com/news/2019/10/mark-zuckerberg-stands-for-voice-and-free-expression/ (besucht am 17.02.2023).

Meta (2023): About Us. URL: https://about.meta.com/company-info (besucht am 16.02.2023).

Morozov, Evgeny (2013): *To Save Everything Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs.

Panetta, Kasey (2021): 5 Trends Drive the Gartner Hype Cycle for Emerging Technologies, 2020. *Gartner*. URL: https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020 [besucht am 16.02.2023].

Pearce, Jonathan M.S.(16. Dez. 2022): “I’m a free speech absolutist!”*. *OnlySky*. URL: https://onlysky.media/jpearce/im-a-free-speech-absolutist/ (besucht 16.02.2023).

Schmidt, Jan-Hinrik (2018): *Social Media*. Wiesbaden: Springer VS.

Schultz, Jeff (8. Juni 2019): How Much Data is Created on the Internet Each Day? *Micro Focus Blog*. URL: https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/ (besucht am 16.02.2023).

Schumacher, Jan (2021): Faszinierende Statistiken und Fakten über unsere Lieblingsplattform Twitter. *Webhoster*. URL: https://webhoster.de/statistiken-twitter-2020/#:~:text=Auch%20wenn%20es%20%C3%BCberm%C3%A4%C3%9Fig%20viele,das%20heute%20656%20Millionen%20Tweets (besucht am 16.02.2023).

Statista (2023): Most popular social networks worldwide as of January 2023, ranked by number of monthly active users. URL: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (besucht am 16.02.2023).

Suciu, Peter (26. Jan. 2023): Free Speech Absolutist Elon Musk Removed BBC Documentary Critical Of India's Leader. *Forbes*. URL: https://www.forbes.com/sites/petersuciu/2023/01/26/free-speech-absolutist-elon-musk-removed-bbc-documentary-critical-of-india/?sh=24e0cd01ceaa (besucht am 17.02.2023).

Twitter (2013): About Twitter. URL: https://web.archive.org/web/20131129015047/https://about.twitter.com/ (besucht am 16.02.2023).

Twitter (2023): About Us. URL: https://about.twitter.com/en (besucht am 16.02.2023).

YouTube (2006): About YouTube. URL: https://web.archive.org/web/20060701050517/http://youtube.com/t/about (besucht am 16.02.2023).

YouTube (2023a): About YouTube. URL: https://about.youtube/ (besucht am 16.02.2023).

YouTube (2023b): Wie geht YouTube mit schädlichen Inhalten um? URL: https://www.youtube.com/intl/ALL_de/howyoutubeworks/our-commitments/managing-harmful-content/#remove (besucht am 16.02.2023).

YouTube (2023c): Community-Richtlinien von YouTube. URL: https://support.google.com/youtube/answer/9288567 (besucht am 16.02.2023).

YouTube (2023d): Building a more responsible platform over the years. URL: https://www.youtube.com/howyoutubeworks/progress-impact/timeline/ (besucht am 16.02.2023).

Faire globale Daten-Governance im Sicherheitsbereich? Risiken bei der internationalen Zusammenarbeit von Sicherheitsbehörden und eine mögliche Rolle der Europäischen Union[1]

Hartmut Aden, Sabrina Schönrock, Steven Kleemann und Milan Tahraoui

Zusammenfassung

Dieser Beitrag identifiziert bestehende Schutzlücken bei der internationalen Zusammenarbeit von Sicherheitsbehörden (Polizeibehörden und Nachrichtendienste) und Risiken für die Menschenrechte, die durch Überwachungstechnologien und durch KI-basierte Technologien für die Auswertung von *Big Data* entstehen. Er zeigt, dass Prinzipien wie Fairness, Transparenz oder Erklärbarkeit von Entscheidungen, die auf Anwendungen Künstlicher Intelligenz basieren, bislang innerhalb der Europäischen Union nur unzulängliche und jenseits der EU noch deutlich weniger praktische Wirkungen erzeugen. Dies wird u.a. am Beispiel des sogenannten *EncroChat*-Falls gezeigt. Der Verwirklichung rechtsstaatlicher Grundsätze steht dabei auch die ausgeprägte Geheimhaltungskultur entgegen, die für die internationale Zusammenarbeit von Sicherheitsbehörden prägend ist.

1. Einleitung

Spätestens seit den Enthüllungen durch Edward Snowden im Jahr 2013 ist weithin bekannt, dass Sicherheitsbehörden global nicht nur im großen Stil personenbezogene Daten sammeln und auswerten, sondern diese auch intensiv austauschen. Für die Betroffenen ist diese Praxis weitgehend intransparent, auch mit der Folge, dass sie sich kaum dagegen gerichtlich zur Wehr setzen können. Auch Staaten wie die Bundesrepublik Deutschland, die sich

1 Teile dieses Beitrags basieren auf Erkenntnissen aus den Forschungsprojekten *FAKE-ID: Videoanalyse mit Hilfe künstlicher Intelligenz zur Detektion von falschen und manipulierten Identitäten* und *VIKING: Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen,* beide gefördert vom Bundesministerium für Bildung und Forschung (BMBF), FKZ: 13N15737 (FAKE-ID) bzw. 13N16241 (VIKING).

als ausgeprägte Rechtsstaaten verstehen, beteiligen sich hieran intensiv, aber oftmals in rechtlichen Grauzonen, wie u. a. das Verfahren vor dem Bundesverfassungsgericht zur Überwachung internationaler Telekommunikation durch den Bundesnachrichtendienst (BND) gezeigt hat.[2] Obwohl bereits seit einiger Zeit sichtbar ist, dass hierfür im Interesse des Menschenrechtsschutzes völkerrechtliche Regelungen erforderlich sind, haben diese bislang kaum Fortschritte gemacht. Durch die zunehmende Bedeutung von Methoden Künstlicher Intelligenz (KI) hat sich das Risiko weiter erhöht, dass die massive Datensammlung und der globale Datenaustausch im Sicherheitsbereich zu intensiveren Grundrechtsbeeinträchtigungen führen.

Risiken entstehen im internationalen Kontext u. a. dann, wenn unklar ist, woher die verwendeten Daten stammen und wie zuverlässig sie sind. Das ist auch innerhalb der Europäischen Union (EU) problematisch. Im Rahmen des Prinzips gegenseitiger Anerkennung, das die EU-Innen- und Justizpolitik seit den 1990er Jahren prägt,[3] wird davon ausgegangen, dass es sich um eine rechtmäßige Erhebung handelt, allein weil diese Daten in einem Mitgliedstaat der EU nach den dortigen Regeln erhoben wurden. Auf der Basis dieses Prinzips würden die Daten also ungeprüft übernommen, da eine rechtmäßige Erhebung grundsätzlich unterstellt würde. Auch der Rückgriff des Staates auf private Akteure mit dem Ziel der Datengewinnung kann zu Risiken für die Grundrechte von Betroffenen führen.[4] Hier besteht insbesondere die Gefahr der Umgehung von Anforderungen, an welche staatliche Behörden gebunden sind, da die privaten Unternehmen die Daten möglicherweise auf Wegen erlangt haben, die Sicherheitsbehörden verwehrt sind.

Das EU-Recht stellt zwar in seinem Zuständigkeitsbereich, zu dem der polizeiliche, nicht aber der nachrichtendienstliche Informationsaustausch gehört (Art. 4 Abs. 2 S. 3 AEUV), zunehmend Anforderung an eine Herkunftsdokumentation von übermittelten Daten sowie relativ hohe Anforderungen an die Datenübermittlung in Nicht-EU Länder;[5] Ausnahmeregelungen im Hinblick auf nationale Sicherheitsinteressen gehen dabei allerdings

2 BVerfGE 154, 152.

3 *Aden*, in Lisken/Denninger (Hrsg.), Polizeirecht, 2021, 7. Aufl., Rn. M 73; *Lavenex*, Journal of European Public Policy 2007.

4 Hierzu z. B. *Lowe*, Rutgers Computer & Technology Law Journal 2021, 1 (38-39).

5 Vgl. etwa ECLI:EU:C:2015:650, Schrems-I; im Sekundärrecht z. B. Art. 23 Abs. 8 Europol-VO (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol), zuletzt geändert durch VO (EU) 2022/991.

zulasten des Grundrechtsschutzes. Die *Schrems-I*- und die *Schrems-II*-Entscheidung des Europäischen Gerichtshofs (EuGH)[6] enthalten wichtige Hinweise auf die Rolle des Privatsektors bei der Generierung von *Big Data*.

Die sogenannte *EncroChat*-Affäre zeigt die weitreichenden Auswirkungen, die unklare Datenverantwortlichkeit auf gerichtliche Verfahren haben kann.[7] In dieser Affäre erhielten deutsche Behörden durch den Datenaustausch mit französischen Behörden Zugriff auf Kommunikationsdaten deutscher Staatsangehöriger in Deutschland, wobei fraglich ist, ob diese nach deutschem Recht hätten erhoben werden können und ob diese in einem Strafverfahren verwertet werden dürfen. Hierzu gibt es bisher keine einheitliche Rechtsprechung: So hält das Landgericht Berlin die Nutzung für unzulässig[8] - im Gegensatz z. B. zum Oberlandesgericht Hamburg,[9] das kein Beweisverwertungsgebot angenommen hat. Der Bundesgerichtshof (BGH) hat bereits dem Grunde nach entschieden, dass die Daten aus dem *EncroChat* Messenger auch in deutschen Strafverfahren genutzt werden können.[10] Das Bundesverfassungsgericht (BVerfG) wird hierüber im Rahmen eines anhängigen Verfassungsbeschwerdeverfahrens zu entscheiden haben.[11] Voraussichtlich werden auch der EuGH und der Europäische Gerichtshof für Menschenrechte (EGMR) mit diesem Fall befasst werden.[12] Angesichts ihrer bisherigen Rechtsprechung könnten sie durchaus zu einer anderen Einschätzung als der BGH kommen.[13]

Dieser Beitrag identifiziert bestehende Schutzlücken bei der internationalen Zusammenarbeit von Sicherheitsbehörden und Risiken für die Menschenrechte, die durch KI-basierte Technologien für die Auswertung von *Big Data* entstehen. Rechtsprechung (EuGH, EGMR, nationale Verfassungsgerichte) und Dokumente mit regulatorischen Intentionen werden hinsichtlich ihres Potenzials untersucht, bestehende Lücken bei der rechtsstaatlichen Einhegung der Daten-Governance im Sicherheitsbereich

6 ECLI:EU:C:2020:559, Schrems-II.
7 Siehe dazu z.B. *European Union Agency for Criminal Justice Cooperation*, Pressemitteilung vom 2.7.2020.
8 LG Berlin, Beschluss vom 1.7.2021 (525 KLs) 254 Js 592/20 (10/21).
9 OLG Hamburg, Beschluss vom 29.01.2021 - 1 Ws 2/21.
10 Ausführlich in BGH, Beschluss des 5. Strafsenats vom 2.3.2022 - 5 StR 457/21.
11 Anhängig unter dem Aktenzeichen: 2 BvR 558/22.
12 *Europäisches Parlament*, EncroChat's path to Europe's highest courts, 2022.
13 Siehe beispielsweise ECLI:EU:C:2022:703 zur Vorratsdatenspeicherung oder CE:ECHR:2021:0525JUD005817013 (Big Brother Watch ua/Vereinigtes Königreich) zur Datenerfassung, -verarbeitung und -übermittlung.

zu schließen. Hierzu zählen internationale Anforderungen, welche sich beispielsweise aus dem *Report on the Democratic oversight of Signals Intelligence Agencies*[14] der Venedig-Kommission oder Ausführungen des UN-Menschenrechtsrats[15] ergeben. Der Verwirklichung rechtstaatlicher Grundsätze steht allerdings eine ausgeprägte Geheimhaltungskultur entgegen, die für die internationale Zusammenarbeit von Sicherheitsbehörden prägend ist.[16]

In diesem Kontext ist auch die globale Rolle der EU von Interesse. EU-Regulierungsansätze können weitreichende faktische Auswirkungen weit über die EU hinaus haben, was etwa für Elemente der Datenschutz-Grundverordnung (DSGVO) vielfach gezeigt worden ist.[17] Auch der Entwurf einer EU-Verordnung zur Künstlichen Intelligenz, den die Europäische Kommission im April 2021 vorgelegt hat, lässt Ambitionen für regulatorischen Einfluss über die EU hinaus erkennen.[18] Als im globalen Maßstab wirtschaftlich starker Akteur hat die EU die Möglichkeit, über Zugangsregeln für den EU-Markt weitreichenden Einfluss auf die Regulierungsstrategien anderer Länder und das Verhalten globaler Konzerne zu nehmen. Der Beitrag fragt, inwieweit dieser Effekt auch für die internationale Daten-Governance im Sicherheitsbereich relevant werden kann. Strukturelle Grenzen sind dem allerdings durch die begrenzten Zuständigkeiten der EU im Sicherheitsbereich (insbesondere bzgl. der Nachrichtendienste) und durch gegenläufige Interessen anderer global mächtiger ökonomischer Akteure (USA, China) gesetzt.

2. Risiken für personenbezogene Daten bei der internationalen Zusammenarbeit der Sicherheitsbehörden

Die internationale Informationszusammenarbeit der Sicherheitsbehörden führt zu mehreren Dimensionen von Risiken für personenbezogene Daten und damit für die Privatsphäre der Betroffenen: im Hinblick auf defizitäre Rechtsstaatlichkeit in beteiligten Staaten, international unterschiedliche Grundrechtsstandards bei der Datenverarbeitung und spezielle Risiken bei

14 CDL-AD(2015)011 vom 15.12.2015.
15 A/HRC/48/31 vom 15.09.2021.
16 Näher hierzu *Aden*, WEP 2018, 981.
17 Auch „Brussels Effect" genannt. Siehe dazu *Bradford*, The Brussels Effect, 2020.
18 *Europäische Kommission*, COM(2021) 206 final, 2021/0106(COD), s. dort insbesondere Erwägungsgrund 5.

der Analyse großer Datenmengen (*Big Data*) mithilfe von Anwendungen Künstlicher Intelligenz.

2.1 Risiken aufgrund defizitärer Rechtsstaatlichkeit in beteiligten Staaten

Die Zusammenarbeit mit Sicherheitsbehörden anderer, insbesondere außereuropäischer Staaten, welche geringere Anforderungen an rechtsstaatliches Handeln, vor allem an den Daten- und Grundrechtsschutz sowie an verfahrenssichernde Maßnahmen als das europäische Recht stellen, kann zu weitreichenden Problemen führen. Als Maßstab gelten hier sowohl verfahrensrechtliche Prinzipien im Sinne des *Fair Trial* aus Art. 6 EMRK als auch grundrechtliche Ausprägungen zur Sicherung des Rechts auf Datenschutz und Privatsphäre. Die Datenübermittlung kann dabei ebenso problematisch sein wie die Verwendung und Weitergabe KI-basierter Systeme und Technologien, welche durch Sicherheitsbehörden eingesetzt werden. Die Risiken sind dabei vielfältig und umfassen beispielsweise die Nutzung von Daten, die im Land der Erhebung für die Personen keinerlei Auswirkungen haben, aber durch Weitergabe an Länder mit geringeren Schutzstandards erhebliche negative Folgen haben können, bis hin zu Verfahren, die zur Todesstrafe führen.

Innerhalb der EU ist der Datenaustausch für Strafverfolgungszwecke inzwischen weitreichend durch EU-Recht geregelt, das auf den Prinzipien der Verfügbarkeit und der gegenseitigen Anerkennung basiert: Die EU-Staaten sollen im Interesse effektiver Strafverfolgung bei ihnen verfügbare Daten möglichst miteinander teilen und dabei auf der Basis gegenseitiger Anerkennung handeln.[19] Dem liegt allerdings die nicht ganz unproblematische Hypothese zugrunde, die rechtsstaatlichen Standards seien in allen EU-Staaten gleichermaßen hoch. Zahlreiche EuGH-Entscheidungen, u. a. zur Überstellung aufgrund eines Europäischen Haftbefehls, deuten indes darauf hin, dass hier weiterhin eine differenzierende Bewertung geboten ist.[20] Zum Datenaustausch mit Drittstaaten hat der EuGH ebenfalls Maßstäbe definiert. Demnach muss in einem Drittstaat nicht zwingend ein identisches Schutzniveau wie in der EU bestehen, jedoch muss entweder aufgrund innerstaatlicher Regelungen oder internationaler Verpflichtungen

19 Näher hierzu *Aden,* in Lisken/Denninger (Hrsg.), Polizeirecht, 2021, 7. Aufl., Rn. M 230 ff.; *Lavenex*, Journal of European Public Policy 2007.

20 *Aden,* in Lisken/Denninger (Hrsg.), Polizeirecht, 2021, 7. Aufl., Rn. M ., Rn. 71 ff. m.w.N.

ein tatsächlicher menschenrechtlicher Schutzstandard bestehen, der dem des EU-Rechts und insbesondere der DSGVO gleichwertig ist.[21] Dies wurde in der *Schrems-II*-Entscheidung für die USA erneut verneint.[22] Grund dafür ist beispielsweise die fehlende Unabhängigkeit des nach US-Recht organisierten Ombudsmann-Mechanismus von der Exekutive.[23] Weiterhin sind insbesondere die weitreichenden Überwachungsbefugnisse der US-Behörden und deren rechtliche Grundlagen[24] nicht mit dem europäischen Grundsatz der Verhältnismäßigkeit vereinbar, wie ihn der EuGH versteht.

Bezüglich der Rechtsstaatlichkeit des Auslandsdatentransfers ist es allerdings auch nicht ratsam, den Blick einseitig auf die USA zu lenken und ausschließlich die dortige Überwachungspraxis zu kritisieren. Der aktuelle Angemessenheitsbeschluss zur Datenübermittlung in das Vereinigte Königreich, welches ebenfalls seit Jahrzehnten ein rigoroses Überwachungsregime etablierte und Mitglied der Geheimdienstallianz *Five Eyes* ist und dennoch ein angemessenes Datenschutzniveau besitzen soll, zeigt die etwas inkonsistente Haltung der EU-Kommission in diesem Zusammenhang.[25]

2.2 Risiken aufgrund unterschiedlicher grundrechtlicher Datenverarbeitungs-Standards

Aufgrund unterschiedlicher grundrechtlicher Datenverarbeitungs-Standards besteht das Risiko, dass unrechtmäßig erhobene Daten im internationalen Bereich weiterverarbeitet und sodann sogar zu Beweiszwecken in der Strafverfolgung eingesetzt werden. Am aktuellen Beispiel der sog. *EncroChat*-Verfahren wird dies in besonderer Weise deutlich. Hier gelang es den französischen Ermittlungsbehörden in einer europäisch koordinierten Aktion in Zusammenarbeit mit Behörden aus den Niederlanden, Europol und Eurojust den Kommunikationsdienst *EncroChat* zu infiltrieren.[26] Die französischen Ermittler:innen vermuteten, dieser werde in erheblichem Umfang von Täter:innen aus der organisierten Kriminalität genutzt. Zunächst wurde Schadsoftware (Trojaner) auf die in Frankreich befindlichen Server des Unternehmens eingespielt. Von dort wurden die Endgeräte

21 ECLI:EU:C:2020:559, „Schrems-II", Rn. 94.
22 Ebd., Rn. 168.
23 Ebd., Rn. 190-198.
24 Insbesondere Section 702 des Foreign Intelligence Surveillance Acts (FISA) und Executive Order 12333.
25 *Kipker*, ZD 2021, 397 (398).
26 BGH, Beschluss des 5. Strafsenats vom 2.3.2022 - 5 StR 457/21, Rn. 8.

sämtlicher Nutzer:innen weltweit „infiziert", was das Auslesen der auf den Telefonen gespeicherten Daten und der darüber geführten Kommunikation ermöglichte. Die erlangten Daten wurden sodann den nationalen Strafverfolgungsbehörden über Europol zur weiteren Verwendung zur Kenntnis gegeben. Inwieweit dabei bereits KI-basierte Auswertungsmethoden verwendet wurden, ist nicht bekannt.

Angesichts des Umfangs und der Eingriffstiefe der heimlichen Überwachungsmaßnahme stellt sich nicht nur die Frage nach der Verwertbarkeit der erlangten Beweismittel in einem deutschen Strafverfahren, gemessen an den Voraussetzungen und Begrenzungen des deutschen Strafverfahrensrechts,[27] sondern auch nach dem internationalen Aspekt der (ggfs. rechtswidrigen) Erhebung der Daten durch die französischen Behörden und der Übermittlung an die deutschen Strafverfolgungsbehörden im Rahmen der Rechtshilfe.[28]

Überprüfbarkeit der Datenverarbeitung und Recht auf faires Verfahren

Die Art und Weise, wie die *EncroChat*-Daten erlangt wurden, beschränkt ihre Nachprüfbarkeit. Der Verfassungsgerichthof Frankreichs (*Conseil Constitutionnel*) bestätigte in einer Entscheidung vom 8. April 2022 zwar, dass die Geheimhaltung der technischen Vorgänge um die Erlangung der *EncroChat*-Daten in Frankreich als ein nationales Militärgeheimnis (*secret défense*) verfassungsgemäß sei und die Verfahrensrechte Beschuldigter – insbesondere das Recht auf ein faires Verfahren gemäß Art. 6 EMRK – nicht beeinträchtigt seien. Jedoch verwies er zugleich auf die erforderliche strafprozessuale Transparenz hinsichtlich der staatlichen „Hacking-Operation".[29] Das französische Verfassungsgericht äußerte sich dahingehend, dass Techniken und Verfahren nachrichtendienstlicher Informationsgewinnung zu schützen seien. In diesem Zusammenhang betonten die Richter:innen, wie wichtig der vertrauliche Charakter solcher Verfahren sei.[30] Auffällig hierbei ist, dass sich das Gericht dabei auf die nachrichtendienstlichen Anforderungen und Techniken beruft, obwohl es im Fall *EncroChat* um die Rechtmäßigkeit des Handelns der beteiligten Strafverfolgungsbehörden ging. Dass die Maßnahme der französischen Behörden konzeptionell auf

27 Hierzu ausführlich *Derin/Singelnstein*, NStZ 2021, 449; *Ruppert*, NZWiSt 2022, 221 (224f.).
28 Zu den Grundlagen der Rechtshilfe: *Pauli*, NStZ 2021, 146 (147f.).
29 Conseil Constitutionnel, Décision n° 2022-987 QPC vom 8.4.2022, 6, Rn. 8.
30 Ebd., S. 7, Rn. 15.

die Erfassung einer großen Anzahl Nichtverdächtiger angelegt war und die eingriffsintensive Maßnahme nicht auf einem individualisierten Tatverdacht beruhte, ist nicht nur nach dem deutschen Recht rechtswidrig,[31] sondern auch nach internationalen rechtsstaatlichen Maßstäben mehr als problematisch. Bemerkenswerterweise entschied das französische Verfassungsgericht, dass die Vorschriften der französischen Strafprozessordnung (Artikel 230-1 bis 230-5 und 706-102-1 *Code de procédure pénale*), deren Verfassungsmäßigkeit in diesem Fall strittig war, tatsächlich ein angemessenes Gleichgewicht (im Original „*une conciliation équilibrée*") zwischen mehreren, aus der französischen Verfassung abgeleiteten Anforderungen herstellen.

Dabei stützte sich die Entscheidung auf drei Kernargumente:[32] Erstens habe das Ziel des französischen Gesetzgebers bei der Verabschiedung der angefochtenen strafprozessualen Maßnahmen darin bestanden, den Ermittlungsbehörden effiziente Mittel zur Sammlung und Entschlüsselung von Daten zur Verfügung zu stellen, ohne den vertraulichen Charakter der von den Nachrichtendiensten zu diesem Zweck eingesetzten Techniken zu schwächen. Diese gesetzgeberischen Maßnahmen trügen daher, so der Gerichtshof, zu den „Zielen des Verfassungswertes" der Suche nach den Urhebern von Straftaten bei und dienten den verfassungsrechtlichen Anforderungen in Bezug auf „die grundlegenden Interessen der Nation".[33] Zweitens stellten die französischen Verfassungsrichter:innen in ihrer Argumentation darauf ab, dass die Durchführung besonderer Ermittlungsmaßnahmen von Richter:innen genehmigt und durch die Notwendigkeit einer Untersuchung im Zusammenhang mit besonders komplexen und schweren Straftaten gerechtfertigt werden muss. Dieses Verfahrenserfordernis stelle daher für das französische Verfassungsgericht implizit eine Garantie für den Schutz der Interessen der Rechtstaatlichkeit und der Grundrechte dar.[34] Drittens nahmen die französischen Verfassungsrichter:innen zur Kenntnis, dass die angefochtenen gesetzgeberischen Maßnahmen es den Ermittlungsbehörden zwar ermöglichen, einige technische Informationen aufgrund des Militärgeheimnisses als streng geheime Verschlusssache zu schützen und so aus dem Geltungsbereich des strafprozessualen Grundsatzes der „Waffengleichheit"

31 BVerfG, Urteil vom 16.2.2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 32, 134; *Arzt*, in: Lisken/Denninger (Hrsg), Handbuch des Polizeirechts, 2021, 7. Aufl., Rn. G 1184 ff.
32 Conseil Constitutionnel, Décision n° 2022-987 QPC vom 8.4.2022, S. 8, Rn. 19.
33 Ebd., S. 7, Rn. 15.
34 Ebd., S. 7, Rn. 16.

herauszunehmen. Sie vertraten jedoch die Auffassung, diese gesetzlichen Regelungen seien in Ordnung, da andere Informationen nach wie vor der Dokumentationspflicht durch die genehmigenden Richter:innen unterlägen. Im Falle der Nichteinhaltung könnten die Maßnahmen darüber hinaus für nichtig erklärt werden. Außerdem verweist das Gericht auf die gesetzliche Vorschrift, dass alle Informationen, die durch besondere Ermittlungsmaßnahmen zum Aufbrechen verschlüsselter Kommunikation gewonnen und an die Ermittlungsbehörden übermittelt werden, zwingend mit der Vorlage einer Bescheinigung einhergehen müssen. Mit dieser Bescheinigung gewährleistet die Organisation, die diese Techniken einsetzt, die „Aufrichtigkeit" der Ergebnisse der besonderen Ermittlungsmaßnahmen.[35]

Die geforderte „Aufrichtigkeitsbescheinigung" von „technischen Organisationen", d. h. möglicherweise auch von Privatfirmen, die auf sicherheitstechnische Produkte spezialisiert sind, wurde in der französischen Rechtsdiskussion als reine Formalität angesehen,[36] bei der eine mögliche Nichteinhaltung von den Strafverfolgungsbehörden einfach korrigiert werden kann. Dies zeigt, dass das französische Recht bei der Regulierung spezieller Ermittlungstechniken, die von Strafverfolgungsbehörden eingesetzt werden, besonders permissiv ist, insbesondere im Vergleich zum deutschen sowie internationalen und europäischen Recht. Angesichts dieser Unterschiede erscheint die Entscheidung des Bundesgerichtshofs, nach der *EncroChat*-Daten keinem Verwertungsverbot unterliegen sollen,[37] kritikwürdig.

Auswirkungen in Großbritannien

In einem *EncroChat*-Verfahren am Londoner *Central Criminal Court* kamen IT-Forensiker vor dem Hintergrund einer Analyse des in Frankreich verwendeten „Staatstrojaners" zu dem Ergebnis, dass dessen Zuverlässigkeit durchaus zweifelhaft sei.[38] Ohne Rückverfolgbarkeit der Daten im Verarbeitungsprozess könne nicht eindeutig gesagt werden, ob die verwendeten Daten authentisch seien – es sei denn, weitere unabhängige Beweise bestätigten den Inhalt der Daten. Zudem sei diese Methode der Datenerhebung

35 Ebd., S. 7, Rn. 17.
36 *Pidoux*, Dalloz actualité v. 14. November 2022.
37 BGH, Beschluss des 5. Strafsenats vom 2.3.2022 - 5 StR 457/21, Rn. 32 ff.
38 *Campbell*, The Guardian v. 14. März 2022.

nicht mit den in Großbritannien geltenden Regeln und Prinzipien zum forensischen Umgang mit digitalen Beweisen vereinbar.[39]

Das Recht auf ein faires Verfahren (Art. 6 EMRK) stellt Anforderungen auch an die Digitalforensik.[40] Mit den Techniken digitaler Beweiserhebung geht geradezu zwangsläufig die Gefahr einer Verletzung von Art. 6 Abs. 1 EMRK einher.[41] *Big-Data*-Analyse und KI-Anwendungen greifen dabei tief in die herkömmliche Art individueller strafrechtlicher Verantwortung ein und haben massive Auswirkungen auf das individuelle Recht auf ein faires Verfahren und auf „Waffengleichheit". Einerseits besteht eine starke Wissens-Asymmetrie zwischen Angeklagten oder Betroffenen und der Anklage,[42] andererseits werden Transparenz und Erklärbarkeit oftmals unzureichend gewährleistet. Hier könnte, jedenfalls im Rahmen eines Gerichtsprozesses, beispielsweise durch die Offenlegung des Softwarequellcodes „Waffengleichheit" geschaffen werden. Letztlich kann damit jedoch auch noch nicht ausreichend nachvollzogen werden, wie die digitalen Beweise zustande gekommen sind und wie zuverlässig sie sind. Hier geht es um das Zusammenspiel und die Abhängigkeiten zwischen Fairness, Transparenz und Erklärbarkeit von KI-Systemen und der Massendatenverarbeitung (näher hierzu unten, 3.1).

Transparenz der Datenerhebung und -verarbeitung im deutschen Strafverfahrensrecht

Die Frage der notwendigen Überprüfbarkeit der *EncroChat*-Daten, ihrer Authentizität und Integrität wird auch anlässlich der aktuellen Verfahren in Deutschland aufgeworfen. Sind Daten im Ausland nicht nach nationalem Recht rechtmäßig erhoben worden oder kann die Frage der rechtmäßigen Erhebung im nationalen Strafverfahren nicht festgestellt werden, steht die Einhaltung rechtsstaatlicher Verfahrensprinzipien, insbesondere die Gewährleistung von Transparenz und Nachvollziehbarkeit der durch

39 *Goodwin,* Computer Weekly v. 11. März 2022.

40 Siehe zu digitalforensischen Standards beispielsweise: *NIST*, Digital and Multimedia Evidence v. 22. November 2022; *European Network of Forensic Science Institutes*, Best Practice Manual for Digital Image Authentication; *Kävrestad*, Fundamentals of Digital Forensics, 2020.

41 *Ewald*, in: Strafverteidigervereinigungen, Organisationsbüro (Hrsg.), 2018, 268 (270).

42 *Wexler*, UCLA Law Review 2021, 212 (242ff.); *Stoykova*, Computer Law & Security Review, 2021, 1; *Ewald*, in: Strafverteidigervereinigungen, Organisationsbüro (Hrsg.), 2018, S. 268.

polizeiliche Ermittlungstätigkeit erzeugten Beweise, auf dem Spiel. Diese würde ersetzt durch die Akzeptanz eines „Blackbox-Prinzips", in dem die Strafgerichte digitale Beweise als Verurteilungsgrundlage akzeptieren, ohne dass die Möglichkeit ihrer Überprüfung besteht. Das Landgericht Berlin[43] bejahte entgegen den Ansichten der Oberlandesgerichte Bremen, Hamburg, Schleswig und Brandenburg sowie des BGH[44] einen Verstoß gegen EU-rechtliche Vorschriften für die Zusammenarbeit in Strafsachen, da keine Unterrichtung der deutschen Behörden über die Kommunikationsüberwachung einer Person in Deutschland stattgefunden habe und diese auch nicht entbehrlich gewesen sei. Zudem sei die Überwachung durch französische Behörden ein nicht gerechtfertigter Eingriff in das Telekommunikationsgrundrecht gemäß Art. 10 GG und das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG; die Bereitstellung der Daten für die Verwendung durch deutsche Behörden sei ein weiterer eigenständiger und nicht gerechtfertigter Eingriff.

Die 25. Große Strafkammer des Landgerichts Berlin setzte die Hauptverhandlung in einem *EncroChat*-Verfahren aus und legte dem EuGH Fragen zur Zulässigkeit der Datenerhebung und Verwertung von *EncroChat*-Daten zur Vorabentscheidung vor.[45] In dem Vorlagebeschluss stellt das Landgericht 14 Fragen zur Auslegung der Richtlinie (EU) 2014/41 zur Europäischen Ermittlungsanordnung (EEA); dabei geht es unter anderem um die Frage, ob ein deutsches Gericht die EEA für Eingriffsmaßnahmen gegen deutsche Staatsbürger:innen hätte anordnen müssen, wie es sich rechtlich auswirkt, wenn sich eine EEA auf sämtliche auf dem Hoheitsgebiet befindlichen Anschlüsse eines Dienstes erstreckt, obwohl keine konkreten Anhaltspunkte für das Begehen schwerer Straftaten durch individu-

43 LG Berlin,Beschluss vom 1.7.2021 (525 KLs) 254 Js 592/20 (10/21); aufgehoben durch Beschluss des KG Berlin vom 30.8.2021 - 2 Ws 79/21 und zur Eröffnung eines Hauptverfahrens an eine andere Strafkammer verwiesen. Das Gericht stellte fest, die Daten seien nach französischem Recht rechtmäßig erhoben worden und dürften deshalb in Deutschland verwendet und verwertet werden. Dadurch, dass die Erkenntnisse spontan übermittelt wurden und dem § 100b StPO entsprachen, liege kein Verstoß gegen Art. 31 Abs. 1 lit. b) RL-EEA vor. Deutschland habe die Daten zudem verwendet und somit konkludent die Übermittlung genehmigt; so dann auch BGH, Beschluss des 5. Strafsenats vom 2.3.2022 - 5 StR 457/21, Rn. 21 ff.

44 OLG Bremen, Beschluss vom 18.12.2020 - 1 Ws 166/20, Rn. 23, 27, 29; OLG Schleswig, Beschluss vom 29.4.2021 - 2 Ws 47/21, Rn. 22; OLG Brandenburg, Beschluss vom 9.8.2021 - 2 Ws 113/21, Rn. 14; BGH Beschluss vom 2.3.2022 – 5 StR 457/21.

45 LG Berlin, Beschluss vom 19.10.2022 - (525 KLs) 279 Js 30/22 (8/22).

elle Nutzer:innen bestehen, ob Daten von Frankreich nach Deutschland übermittelt werden dürfen, auch wenn die Datenerhebung in Deutschland unzulässig wäre oder ob sich durch eine unionsrechtswidrige Ermittlungsanordnung ein Beweisverwertungsverbot ergibt. Die Entscheidung des EuGHs zu den aufgeworfenen rechtlichen Unklarheiten steht noch aus.

Perpetuierter Rechtsverstoß bei grenzüberschreitendem Datentransfer

Im Zusammenhang mit dem hier untersuchten *EncroChat*-Fall geht es im Kern nicht um die Rechtmäßigkeit der Maßnahme nach französischem Recht, sondern um die Frage, ob und unter welchen Voraussetzungen die im Ausland erhobenen Daten in einem deutschen Strafverfahren verwendet werden können. Der Grundrechtseingriff ist als gravierender einzustufen, wenn die Daten nicht nur nach deutschem Recht nicht hätten erhoben werden dürfen (sog. hypothetischer Ersatzeingriff), sondern (nach diesem Maßstab hypothetisch) rechtswidrig erhobene Daten gleichsam „wider besseren Wissens" zu einem abweichenden Maßstab bei der Verwendung im Strafverfahren durch die deutschen Behörden führt. Die in Frankreich und zum Teil von den französischen Behörden auch in Deutschland erhobenen Daten wurden von den Endgeräten erhoben, gespeichert, zusammengeführt, versandt und aufbereitet – also mehrfach verarbeitet. Die Integrität mehrfach verarbeiteter Daten ist gefährdet, wenn die Erhebung und Verarbeitung nicht durch die Einhaltung einheitlicher (europa-)rechtlicher Vorgaben sowie technisch-organisatorischer Maßnahmen sichergestellt wird.[46] Sollen die „abgeschöpften" Daten im deutschen Strafprozess zum Beweis geeignet sein, ist Voraussetzung für eine nachvollziehbare Datenauthentizität und -integrität eine rechtlich wie auch technisch transparente Erhebung der Daten im Ausland. Die Vearbeitung muss in einer „Legitimationskette" (englisch: „chain of custody") bis zur Einbringung in das Gerichtsverfahren nachvollziehbar sein.

2.3 Risiken der KI-basierenden Big Data-Analyse

Die beschriebenen Problematiken des *EncroChat*-Falls stehen exemplarisch für die Schwierigkeiten der *Big-Data*-Nutzung durch Sicherheitsbehörden. Basiert die internationale Zusammenarbeit der Sicherheitsbehörden auf

46 So auch: *Kipker/Bruns*, MMR 2022, 363 (365f.).

KI-Anwendungen, was im *EncroChat*-Fall nicht öffentlich bekannt ist, so vergrößern sich die Risiken für die Grundrechte der Betroffenen erheblich.

Die Risiken einer KI-basierten Datenanalyse durch polizeilich genutzte Technologien sind vielfältig. Dazu zählen die oftmals fehlende oder unklare Rechtsgrundlage für den Verarbeitungszweck, Diskriminierungs- und Biasrisiken ebenso wie weitreichende Eingriffe in das Recht auf informationelle Selbstbestimmung, das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (beide geschützt durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und das Telekommunikationsgrundrecht (Art. 10 GG). Ähnliche Risiken für diese Rechtsgüter bestehen auch auf internationaler Ebene.[47] Mit Blick auf den technischen Fortschritt sowie auf das Tempo der KI-Entwicklung und *Big-Data*-Analysen muss davon ausgegangen werden, dass sich die Risiken erhöhen werden.

Diskriminierungsrisiken bestehen hier beispielsweise aufgrund von Geschlecht, ethnischer Herkunft, Behinderungen, Religion und Glaube, Alter oder sexueller Orientierung. Durch *Big-Data*-Analysen können bereits bestehende Diskriminierungsdynamiken und -gefahren um ein Vielfaches erhöht und automatisiert reproduziert und verfestigt werden. Generell entstehen mit Blick auf KI-basierte Systeme *Bias*-Risiken bereits und zuvörderst im Zusammenhang mit den Trainingsdatensätzen. Sind diese Risiken bereits in den Trainingsdaten angelegt, werden diese durch das Trainieren des KI-basierten Systems fortgeführt und möglicherweise noch verstärkt. Demzufolge müssen im Zusammenhang mit polizeilichen Grundrechtseingriffen hier besonders hohe Anforderungen gestellt und erfüllt werden.

Mit der Überarbeitung der Europol-Verordnung, welche seit dem 28. Juni 2022 gilt,[48] haben sich einige Neuerungen für die internationale Datenverarbeitung ergeben. Auf europäischer Ebene ist die EU-Agentur für die Zusammenarbeit im Bereich Strafverfolgung (Europol) ein zentraler Akteur; insbesondere bezüglich Datenverarbeitung und Datenaustausch kommt Europol eine wesentliche Rolle zu. Die Verarbeitung und Analyse von Daten ist bereits primärrechtlich in Art. 88 Abs. 2 S. 2 lit. a AEUV als Aufgabe von Europol angelegt. Allerdings sah der Europäische Datenschutzbeauftragte (EDSB) unter der bisherigen Europol-Verordnung,[49] anders als die Europol-Agentur selbst, das tatsächliche Vorgehen von Europol

47 *OHCHR*, The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights, A/HRC/39/29 vom 3.8.2018.
48 VO (EU) 2022/991.
49 VO (EU) 2016/794.

teilweise als nicht vom geltenden Recht gedeckt an. Der EDSB rügte die Verarbeitung von *Big-Data* zu Analysezwecken als rechtswidrig und verpflichtete Europol im Januar 2022, die betroffenen Datensätze zu löschen.[50] Als direkte Reaktion darauf wurde in der Neufassung der Europol-Verordnung ein neuer Art. 18 Absatz 6a eingefügt. Damit soll klargestellt werden, dass die Agentur eingehende Daten vorab analysieren und feststellen kann, ob diese unter eine der zulässigen Kategorien des Art. 18 Europol-VO fallen. Die betreffenden Daten sollen dann auch mit bereits vorliegenden abgeglichen werden dürfen.[51] Dadurch kann Europol grenzüberschreitende Querverbindungen erfassen, welche die nationalen Behörden so nicht selbst hätten feststellen können. Problematisch ist hierbei, dass Europol nicht nur Daten über verurteilte Straftäter:innen und Tatverdächtige verarbeiten darf, sondern auch über „Personen, in deren Fall nach Maßgabe des nationalen Rechts des betreffenden Mitgliedstaats faktische Anhaltspunkte oder triftige Gründe dafür vorliegen, dass sie Straftaten begehen werden, für die Europol zuständig ist."[52] Eine solch weitgehende und unbestimmte Formulierung erfasst potenziell auch Verhaltensweisen, welche weit im Vorfeld eventueller Straftaten liegen und genügt damit nur schwerlich den Anforderungen an die Bestimmtheit einer Eingriffsnorm.[53]

Ebenfalls in diesem Zusammenhang kann auf den neuen Art. 18a Europol-VO verwiesen werden, wonach nationale Strafverfolgungsbehörden nunmehr Europol mit der Auswertung von Daten beauftragen können, sofern diese auch unter dem entsprechenden nationalen Rechtsrahmen in Ermittlungsverfahren ausgewertet und erhoben werden dürfen.[54] Damit wurde auf Bedenken des EDSB eingegangen und der Versuch unternommen, rechtlich klarzustellen, dass die Datenverarbeitung und Datenübermittlung möglich sind, solange sie den rechtlichen Anforderungen im jeweiligen Mitgliedsstaat genügen.

Auch die Neuregelungen der Europol-VO zum Informationsaustausch mit Drittstaaten (Art. 25 Europol-VO) und der Abschnitt zur Zusammenarbeit mit Privaten (Art. 26 ff. Europol-VO) sind im Hinblick auf eine faire Daten-Governance problematisch. Der neue Art. 25 Abs. 4a Europol-VO er-

50 EDSB, Entscheidung vom 17.9.2020 – C 2019-0370, S. 7 f.; EDSB, Entscheidung vom 21.12.2021 – C 2021-0699.
51 *Rüß/Lutz*, GSZ 2022, 221 (223).
52 Europol-VO Anhang II, Abschnitt A, Abs. 1 lit. b.
53 *Aden*, in Lisken/Denninger (Hrsg.), Polizeirecht, 2021, 7. Aufl., Rn. M 214.
54 *Rüß/Lutz*, GSZ 2022, 221 (223).

weitert Europols Möglichkeiten zum strukturellen Datenaustausch, ähnlich jenen von Eurojust, und ermöglicht damit Ausnahmen oder gar die Umgehung eines Angemessenheitsbeschlusses der EU-Kommission oder des Erfordernisses eines bestehenden Abkommens nach Art. 218 AEUV. Damit kann Europol künftig auch personenbezogene Daten übermitteln, wenn geeignete Datenschutzgarantien in einem rechtsverbindlichen Instrument vorgesehen sind oder die Agentur selbst alle Umstände der Datenübermittlung prüft und der Auffassung ist, dass geeignete Garantien für den Schutz von Daten existieren.[55] Eine solche selbstständige Beurteilung ermöglicht zwar eine gewisse Flexibilität bezüglich der besonderen Bedeutung des Informationsaustausches für die innere Sicherheit, beinhaltet aber insbesondere auch mit Blick auf die Rüge des EDSB erhebliche Gefahren für den Grundrechtsschutz.

Auch die Neuregelungen zur Zusammenarbeit von Strafverfolgungsbehörden und Privaten sollten einer kritischen Prüfung unterzogen werden. Der neue Art. 26 Abs. 2 und 4 präzisiert das Verfahren zur Feststellung und Information betroffener Stellen, wenn die Agentur personenbezogene Daten direkt von Privaten entgegennimmt. Europol darf alle betroffenen Stellen ermitteln und die Daten zu diesem Zweck nach Art. 18 Europol-VO verarbeiten und muss diese Daten sowie die relevanten Ergebnisse aus deren Verarbeitung, die für die Feststellung der Zuständigkeit erforderlich sind, unverzüglich an die betreffenden nationalen Stellen weiterleiten. Demgegenüber soll die Weiterleitung an Drittstaaten und internationale Organisationen nun in einer Art pflichtgemäßem Ermessen von Europol liegen.[56] Sofern die private Partei in einem Drittstaat niedergelassen ist, mit dem keine Möglichkeit zum strukturellen Informationsaustausch nach Art. 25 Abs. 1 und 4a Europol-VO besteht, räumt Art. 26 Abs. 4 UAbs. 2 der Agentur schließlich die Möglichkeit ein, diesem das Ergebnis der Verarbeitung unter den Voraussetzungen von Art. 25 Abs. 5 und 6 weiterzuleiten. Der neue Art. 26 Abs. 5 Europol-VO behält zwar das Grundprinzip bei, dass die Agentur keine personenbezogenen Daten an private Akteure übermitteln darf, der Katalog der Ausnahmen wurde jedoch erweitert.

Die Neuerungen erweitern somit die Datenverarbeitungsmöglichkeiten und bereiten den Weg für die Agentur zur Verarbeitung großer und komplexer Datensätze.[57] Europol erhält damit ein weitergehendes Mandat als

55 Ebd, 224.
56 Ebd.
57 *Quintel*, EDPL 2022, 90 (92).

bisher, mit privaten Stellen und Drittländern zusammenzuarbeiten. Im Hinblick auf eine wirksame Datenschutzaufsicht für die internationale Daten-Governance der Sicherheitsbehörden erscheint es äußerst problematisch, dass Europol rechtswidrig verarbeitete Daten aufgrund der Rüge des EDSB nicht etwa löschte, sondern die rechtswidrigen Praktiken im Nachhinein durch eine Verordnungsänderung „legalisiert" wurden.

3. Anforderungen an eine faire Daten Governance von Sicherheitsbehörden

In den folgenden Abschnitten werden Anforderungen an eine faire Daten-Governance durch Sicherheitsbehörden skizziert. Dabei ist vorab zu bemerken, dass diese Anforderungen bislang nur fragmentarisch sind und ein ganzheitlicher Blick auf die transnationale Polizeiarbeit und damit einhergehende Menschenrechtsrisiken fehlt. Die voranschreitende Technisierung der Polizeiarbeit erschwert zudem eine wirksame Kontrolle. Dies gilt umso mehr für KI-basierte Polizeiarbeit, bei der die praktische Umsetzung zentraler Prinzipien wie Fairness, Transparenz und Erklärbarkeit von Entscheidungen, die mittels KI-basierter Systeme getroffen werden, sich als große Herausforderung erweist.[58]

3.1 Fairness als Prinzip der Datenverarbeitung

Im Zusammenhang mit der Datenverarbeitung durch Sicherheitsbehörden wird *Fairness* manchmal als erfüllt angesehen, wenn Transparenz gewährleistet ist. Diese Perspektive erscheint jedoch unterkomplex. Transparenz als Anforderung von Datenverarbeitung stellt zwar einen wichtigen Teilaspekt dar, jedoch geht *Fairness* als übergreifendes Konzept darüber hinaus und muss im Zusammenhang mit Erklärbarkeit und Transparenz gesehen werden. Erst durch die Gewährleistung all dieser Prinzipien kann auch ein höheres Maß an Verfahrensgerechtigkeit entstehen. Der internationale Datenaustausch kann die Umsetzung dieser Prinzipien erschweren. Auch die bereits beschriebenen *EncroChat*-Daten und deren Nutzung müssen sich an diesen Prinzipien messen lassen, und insbesondere das Recht auf ein faires Verfahren darf hier nicht umgangen werden.

58 *Aden u.a.*, zfmr 2022, 50 (68f.).

Bezüglich künftiger Regelungen kann auf die geplante EU-Verordnung zu Künstlicher Intelligenz geschaut werden. Es ist in diesem Zusammenhang bemerkenswert, dass der Begriff *Fairness* so konkret gar nicht im Verordnungsentwurf vorkommt. Der Fairness-Grundsatz wird jedoch in mehreren europäischen und internationalen Empfehlungen und Regelungen zu KI-Systemen erwähnt.[59] In diesem Kontext steht Fairness in engem Zusammenhang mit dem ethischen und normativen Grundsatz der Nichtdiskriminierung. Darüber hinaus umfasst er auch den rechtlich weniger normierten Aspekt, dass KI-basierte Entscheidungen so ausgestaltet sein sollen, dass Betroffene das Ergebnis als fair und akzeptabel wahrnehmen können – ein Aspekt, der auch in *Procedural Justice*-Theorien zur Akzeptanz von Behördenhandeln eine zentrale Rolle spielt.[60] Damit ist Fairness sowohl als rechtliche als auch ethische Kategorie anzusehen und kann zusätzlich aus unterschiedlichen, auch technischen, Blickwinkeln betrachtet werden. Algorithmische Fairness meint beispielsweise solche Methoden, die Verzerrungen in datenverarbeitenden Systemen verringern oder ausschließen, wenn diese zu sozialen Stigmatisierungen oder Diskriminierungen führen können. In der Informatik wird dabei auch zwischen individueller und gruppenbezogener Fairness unterschieden.[61] Bei Gruppenfairness sollen die Ergebnisse beispielsweise eines KI-Systems so angeglichen werden, dass für unterschiedliche vordefinierte Gruppen diese gleich oder zumindest ähnlich sind; individuelle Fairness soll sicherstellen, dass die Ergebnisse für vergleichbare Individuen auch gleich sind.[62] Für den Kontext der Sicherheitsbehörden und deren Datenverarbeitung und -austausch folgt daraus, dass die effektive Gewährleistung von Fairness, aber auch von Transparenz und Erklärbarkeit, eine besondere Herausforderung darstellt. Um dieser zu begegnen und damit insbesondere auch Verfahrensgerechtigkeit herzustellen, wären adressat:innenspezifische Lösungen ein geeignetes Mittel. Das bedeutet, dass die unterschiedlichen Bedürfnisse an eine faire globale Daten-Governance, an Datenverarbeitung, Datenaustausch und

59 UNESCO Recommendation on the ethics of artificial intelligence, SHS/BIO/REC-AIETHICS/2021; OECD, Empfehlung des Rats zu künstlicher Intelligenz, OECD/LEGAL/0449, 22.5.2019; Europarat, CAHAI, Feasibility Study, CAHAI(2020)23, 17.12.2020; United Nations System CEB/2022/2/Add.1, Chief Executives Board for Coordination Distr.: General 27.10.2022.

60 Näher hierzu *Sunshine/Tyler*, Law and Society Review 2003, 513; *O'Brien/Tyler*, Behavioral Science & Policy 2019, 35.

61 *Mehrabi et al.*, ACM Computing Surveys 2021, 1 (11ff.)

62 Ebd.

eine faire Ausgestaltung KI-basierter Technologien im Rahmen der Arbeit von Sicherheitsbehörden, akteursspezifischen Anforderungen unterliegen. Interessant ist, dass der Verordnungsentwurf auch die Tatsache berücksichtigt, dass die Verarbeitung nicht personenbezogener Daten ebenfalls zu grundrechtlichen Risiken führen kann, weswegen eine solche Datenverarbeitung auch verfahrensrechtlich einzuhegen sei.[63]

Bezüglich dieser Anforderungen kann hier erneut der *EncroChat*-Fall beispielhaft herangezogen werden. Es kann auch in diesem Fall davon ausgegangen werden, dass Ermittler:innen, Gerichtssachverständige, Anwäl:innen, Richter:innen, KI-Fachleute, Beschuldigte, sonst Betroffene und die breite, auch internationale Öffentlichkeit unterschiedliche Bedürfnisse und Interessen bezüglich Fairness, Transparenz und Erklärbarkeit haben. Um dies zu verdeutlichen, könnte nun anhand einer Art „Zwiebelmodell" eine gruppenspezifische Gewährleistung und Offenlegung verschiedener Informationen möglich gemacht werden. Praktisch bedeutet dies, dass im Falle von KI-Anwendungen Fachleuten, denen der Betrieb der KI-Anwendung obliegt, ebenso wie den Ermittelnden und Gerichtssachverständigen, in einer inneren Schicht umfangreiche technische und inhaltliche Informationen zur Verfügung gestellt werden, um KI-basierte Entscheidungen fundiert und kritisch bewerten zu können. Betroffene von KI-basierten Entscheidungen erhalten nach diesem Modell die für sie relevanten Informationen, um eine effektive Grundrechtsausübung gewährleisten zu können, ohne dass diese eine vertiefte technische Expertise benötigen. Die äußere Schicht hält alle für die allgemeine Öffentlichkeit notwendigen Informationen bereit. Um dies zu gewährleisten, müssen differenzierte Anforderungen bereits bei der KI-Entwicklung mitbedacht und von Beginn an in ein holistisches Konzept integriert werden. Wichtige Kriterien sind dabei auch die Partizipationsoffenheit und eine interdisziplinäre, integrierte Technikentwicklung.[64] Die Gesetzgebung wird die Verwirklichung eines solchen Modells durch die Etablierung entsprechender Pflichten für Sicherheitsbehörden gewährleisten müssen. Das Modell könnte den Anforderungen an Fairness im Zusammenhang mit Datenverarbeitung, insbesondere *Big-Data* und deren transnationale Dimension, erfüllen helfen. Im internationalen Kontext wären neben verbindlichem EU-Recht insbesondere

63 *Hornung*, AöR 2022, 147, 1 (66).
64 *Gressel/Orlowski*, TATuP 2019, 71.

völkerrechtliche Standards hierfür hilfreich – die allerdings bisher nicht konkret absehbar sind.[65]

Hieran anschließend stellt sich die Frage, inwieweit die Pflicht zur Wahrung nationaler Grundrechte bei der transnationalen Datenverarbeitung besteht, beziehungsweise inwiefern deutsche Sicherheitsbehörden überhaupt im Rahmen von internationaler Datenverarbeitung an das Grundgesetz gebunden sind. Dies wird nachfolgend erläutert.

3.2 Grundrechtsbindung der Sicherheitsbehörden bei transnationaler Datenverarbeitung

Inwiefern Sicherheitsbehörden im Rahmen von Datenverarbeitung auf trans- und internationaler Ebene an die deutsche Verfassung gebunden sind beziehungsweise wie weit die territoriale Geltung der Grundrechte reicht, war bereits Gegenstand etlicher, auch höchstrichterlicher Entscheidungen. Bereits 1999 hat das BVerfG Aussagen zur Vereinbarkeit strategischer Überwachung der Telekommunikationsbeziehung zwischen Deutschland und dem Ausland durch den BND nach § 3 G 10 a. F. (jetzt § 5 G 10) und zur Reichweite von Art. 10 GG getroffen, musste die Frage jedoch aufgrund fehlender Entscheidungserheblichkeit nicht beantworten.[66] Spätestens mit den Enthüllungen durch Edward Snowden 2013 rückten die Zusammenarbeit und der Datenaustausch zwischen Nachrichtendiensten, deren Kontrolle sowie die fehlende gesetzliche Befugnis des BND zur strategischen Überwachung von Ausland-Ausland-Telekommunikation erneut in den Mittelpunkt öffentlichen Interesses.[67] Als Konsequenz dieser Entwicklungen wurde 2016 das Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des BND[68] verabschiedet. Gegen dieses Gesetz richtete sich sodann eine erfolgreiche Verfassungsbeschwerde, durch die das BVerfG Maßstäbe bezüglich der internationalen Datenverarbeitung, aber insbesondere auch bezüglich der Auslandsgeltung deutscher Grundrechte gesetzt hat.[69] Das BVerfG stellte in dieser Entscheidung – angesichts der Ausgestaltung des Brief-, Post- und Fernmeldegeheimnisses (Art. 10 GG) als „Jedermann"-Grundrecht wenig

65 Hierzu auch *Aden,* in: Delpeuch/Ross (Hrsg.), Comparing the Democratic Governance of Police Intelligence, 2016, 322; *Aden*, WEP 2018, 981.
66 BVerfGE 100, 313, Rn. 173.
67 *Huber,* NVwZ-Beilage 2020, 3 (3).
68 Gesetz vom 23.12.2016 - BGBl. I 2016, Nr. 67, 30.12.2016, S. 3346.
69 BVerfGE 154, 152-312.

überraschend – eine dezidierte Bindung deutscher Staatsgewalt fest und klärte damit die bis dahin umstrittene Frage der territorialen grundrechtlichen Geltung dieses Grundrechts auch für Ausländer:innen im Ausland gegenüber technischer Überwachung ihrer Kommunikation durch deutsche Nachrichtendienste.[70]

Der strategischen Fernmeldeaufklärung wohnt die Besonderheit inne, weitere, eigenständige Grundrechtseingriffe nach sich zu ziehen. Das ist immer dann der Fall, wenn beispielsweise der BND die aus der Überwachung gewonnenen Erkenntnisse an in- und ausländische Behörden weiterleitet.[71] Hier sah das BVerfG die Notwendigkeit, zwingend rechtsstaatliche Garantien zu gewährleisten.[72] Insbesondere dürfen aufgrund der grenzüberschreitenden Kooperation und Übermittlung von Daten keine grundrechtlichen Garantien umgangen werden.[73] Bereits vor dem Urteil war anerkannt, dass die deutsche Staatsgewalt nicht an Menschenrechtsverletzungen im Ausland beteiligt sein darf, weswegen beispielsweise die Schutzpflicht aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG Abschiebungen verbietet, bei denen die Gefahr menschenunwürdiger Behandlung droht.[74] Es ist daher nur konsequent, dass die Verfassungsrichter:innen der Staatsgewalt vorschrieben, im Rahmen einer Rechtsstaatlichkeitsvergewisserung sicherzustellen, dass die aus der Überwachung erlangten Informationen im Empfängerstaat nicht zu Verletzungen des menschenrechtlichen Mindeststandards oder der elementaren Regeln des humanitären Völkerrechts führen.[75] Ähnliche Anforderungen folgen auch aus Rechtsprechung des EGMR zur extraterritorialen Informationsgewinnung durch den US-Auslandsnachrichtendienst *Central Intelligence Agency* (CIA). Der EGMR verurteile bereits 2012 Mazedonien (heute Republik Nordmazedonien) unter dem Gesichtspunkt einer Schutzpflichtverletzung aufgrund der Entführung und Überstellung von Khaled El Masri an die CIA im Rahmen des *extraordinary renditions*-Programms,

70 BVerfGE 154, 152, Rn. 87, 92, 104.
71 *Schmahl*, NJW 2020, 2221 (2224).
72 BVerfGE 154, 152, Rn. 211 ff.
73 BVerfGE 154, 152, Rn. 244.
74 BVerfGE 60, 348; BVerfGE 75, 1 (16f.); BVerfGE 113, 154 (162); BVerfGE 140, 317 (347); BVerfGE 141, 220 (342f.).
75 BVerfGE 154, 152, Rn. 233, 237.

bei dem mutmaßlich Terrorverdächtige zur Informationsgewinnung auf fremdes Staatsgebiet verbracht und gefoltert wurden.[76]

Der EGMR hat sich darüber hinaus bereits mehrfach mit Maßnahmen der Überwachung von Telekommunikation von Individuen und der Problematik von „Massenüberwachung" im Bereich der nachrichtendienstlichen Fernmeldeaufklärung befasst.[77] Hier sind insbesondere die Verfahren *Big Brother Watch v UK*[78] und *Rättvisa v Schweden*[79] zu nennen. In dem grundlegenden Urteil der Großen Kammer in der Rechtssache *Big Brother Watch* gegen das Vereinigte Königreich nahm der EGMR auf einige Schlüsselaspekte der BVerfG-Entscheidung zur Ausland-Ausland-Fernmeldeaufklärung des BND Bezug. Dabei nahmen die Straßburger Richter:innen insbesondere die Tatsache zur Kenntnis, dass nach deutschem Recht die internationale Zusammenarbeit mit ausländischen Nachrichtendiensten nicht dazu genutzt werden darf, geltende innerstaatliche Rechtsgarantien zu umgehen.[80] Der EGMR führte weiter aus, welches Recht anzuwenden sei, wenn ein Vertragsstaat Daten von ausländischen Nachrichtendiensten anfordert. Das Gericht formulierte explizit die Anforderung, es sei zu verhindern, dass die Vertragsstaaten ihre Verpflichtungen aus der EMRK umgehen, insbesondere, wenn nachrichtendienstliche Daten von einer Nichtvertragspartei angefordert werden.[81] Weiter muss es auch klare Regelungen bezüglich des Datenaustausches geben, welche die Bürger:innen in die Lage versetzen zu verstehen, wann und unter welchen Bedingungen ein solcher stattfindet; zudem bedarf es dafür einer expliziten gesetzlichen Grundlage im innerstaatlichen Recht.[82] Die Tatsache, dass die internationale nachrichtendienstliche Zusammenarbeit nicht dazu benutzt werden darf, die Verpflichtungen aus der Konvention zu umgehen, gilt nicht nur für die Datenübermittlung an Drittstaaten: Sie gilt auch unter den Vertragsparteien der EMRK selbst.

Diese Anforderungen wurden zwar im Zusammenhang mit Nachrichtendiensten aufgestellt, jedoch lassen sich hier auch für die Strafverfol-

76 Grundlegend dazu: EGMR NVwZ 2013, 631 Rn. 220 – El-Masri. Zur Folgejudikatur vgl. *Staffler*, EuGRZ 2016, 344 (346ff.); *Schmahl* in Dietrich/Sule (Hrsg.), Intelligence Law and Policies in Europe, 2019, 291 (317f.).
77 *Huber*, NVwZ-Beilage 2021, 3 (3f.).
78 CE:ECHR:2021:0525JUD005817013 (Big Brother Watch ua/Vereinigtes Königreich).
79 CE:ECHR:2021:0525JUD003525208.
80 CE:ECHR:2021:0525JUD005817013, Rn. 251.
81 Ebd., Rn. 251.
82 Ebd., Rn. 497.

gungsbehörden einzuhaltende Standards ableiten. Dies gilt umso mehr, weil Daten, welche Polizeien aus dem Ausland erhalten, originär auch von Nachrichtendiensten stammen können – auch vor dem Hintergrund, dass die Zuständigkeitsabgrenzung zwischen Polizeien und Nachrichtendiensten von Land zu Land variiert. Das Argument, es handele sich wahrscheinlich um Datensätze aus Rechtsstaaten und daher sei eine hiesige Verarbeitung gerechtfertigt, kann vor diesem Hintergrund nicht überzeugen. Dadurch würden die vom Bundesverfassungsgericht aufgestellten Kriterien unterlaufen und auch das informationelle Trennungsprinzip[83] umgangen.

Im Zusammenhang mit der internationalen Datenverarbeitung weist das US-amerikanische Rechtssystem indes noch weitaus größere Defizite auf als das europäische. Hier bestehen auch praktisch relevante Zusammenhänge, denn der Austausch von Daten zwischen europäischen Ländern und den USA hat erhebliche Ausmaße, sowohl im privatwirtschaftlichen Bereich als auch bei den Polizeien und Nachrichtendiensten.[84] In den USA sind die datenschutzrechtlichen Standards deutlich weniger ausgeprägt als in Europa. Hinzu kommt die allgemeine US-amerikanische Sichtweise, dass der Grundrechtsschutz in der Regel lediglich für eigene Staatsangehörige gilt.[85] Dies hat zur Folge, dass es schwer ist, den internationalen Datenaustausch zwischen den Ländern grundrechtsschonend zu regeln. Die Verfahren *Schrems-I* und *Schrems-II* verdeutlichen dies.[86] Der EuGH hat in *Schrems-II* zum Ausdruck gebracht, dass er Zweifel daran hegt, „ob das Recht der Vereinigten Staaten tatsächlich das nach Art. 45 der DSGVO im Licht der durch die Art. 7, 8 und 47 der Charta verbürgten Grundrechte erforderliche Schutzniveau gewährleistet."[87] Der Europäische Datenschutzausschuss (EDSA) hat als Reaktion auf *Schrems-II* für Drittstaatentransfers ein sechsstufiges Prüfprogramm vorgeschlagen,[88] damit die Verantwortlichen prüfen können, „ob nebst den Garantien nach Art. 46

83 Vgl. BVerfGE 133, 277, Rn. 123; BVerfGE 156, 11, Rn. 101, 105.

84 Siehe dazu z.B. *Glouftsios/Leese,* Review of International Studies 2023, 125 (129-131); *Bellanova/de Goede*, Regulation & Governance 2022, 102; *Raposo,* Information & Communications Technology Law 2023, 45; *Bäuerle,* CR 2023, 64; *Iliadis/Acker,* The Information Society 2022, 334; PE 694.678, July 2021; ECLI:EU:C:2020:559, „Schrems-II"; *Bignami*, Boston Legal Law Review 2007, 609(655ff.); *Huber*, NVwZ-Beilage 2021, 3 (6ff.).

85 Europäisches Parlament (2021): *Bignami*, GWU Law School Public Law Research Paper 2015, 9; UN Doc A/69/397, 16, Abs. 42; CCPR/C/USA/CO/4, 9f., Abs. 22.

86 *Dehmel u.a.*, MMR 2023, 17 (17).

87 ECLI:EU:C:2020:559, „Schrems-II", Rn 168.

88 EDSA Empfehlungen 01/2020; sowie EDSA Empfehlungen 02/2020.

DS-GVO – insbesondere nebst Standarddatenschutzklauseln nach Art. 46 Abs. 2 lit. c DS-GVO – zusätzliche Maßnahmen vereinbart werden müssen bzw. ob der Transfer trotz möglicher zusätzlicher Maßnahmen zu unterlassen ist."[89] Mittlerweile ist die EU bemüht, ein neues Datenschutzabkommen mit den USA zu schließen. US-Präsident Joe Biden unterzeichnete dazu im Oktober 2022 eine Verfügung (*Executive Order*), die als Grundlage eines neuen Rechtsrahmens für den Datentransfer zwischen den USA und der EU dienen soll.[90] Daran anschließend hat die EU-Kommission ein Verfahren gem. Art. 45 DSGVO zur Annahme eines Angemessenheitsbeschlusses für einen sicheren Datenverkehr mit den USA eingeleitet.[91] Inwiefern dieser Beschluss gefasst wird, ist aktuell noch unklar. Das Europäische Parlament und der EDSA haben noch Vorbehalte.[92]

3.3 Accountability-Anforderungen

Bezüglich der *Accountability*-Anforderungen stellen sich vielfältige Fragen, die ebenfalls durch den Einsatz KI-basierter Systeme und *Big Data*-Anwendungen verschärft werden. Die höhere Eingriffsintensität folgt aus den gestiegenen technischen Möglichkeiten, die zu einer komplexeren Auswertung, der Neugenerierung von Daten, aber auch Intransparenz von Abläufen für Betroffene solcher Maßnahmen führen.[93] In Demokratien wird die Kontrolle der Staatsgewalt durch Transparenz überhaupt erst ermöglicht. Der Sicherheitsbereich ist in diesem Zusammenhang durch ein gewisses Maß an „notwendiger" Intransparenz gekennzeichnet, um den sensiblen Charakter ihrer Ermittlungsfunktion zu wahren.[94] Aufgrund der „*Blackbox*"-Problematik KI-basierter Technologien und des hohen Maßes an Intransparenz solcher Systeme steigt die Gefahr für Demokratie und Menschenrechte durch den sicherheitsbehördlichen Einsatz solcher Systeme. Im Zusammenhang mit Aktivitäten im Rahmen der internationalen Zusammenarbeit von Sicherheitsbehörden tritt hinzu, dass diese häufig auf informellen Vereinbarungen und Praktiken beruhen, bei denen Staaten nur

89 *Dehmel u.a.*, MMR 2023, 17 (18).
90 *The White House*, Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities Executive Order 14086 vom 7.10.2022.
91 Europäische Kommission, Pressemitteilung vom 13.12.2022.
92 EDSA, Pressemitteilung vom 28.2.2023.
93 So die ständige Rspr. des Bundesverfassungsgerichts, vgl. BVerfGE 115, 320 (Rasterfahndung); BVerfGE 156, 11 (Antiterrordateigesetz).
94 *Aden* u.a., zfmr 2022, 50 (57 ff.).

ungern die für die Identifizierung und Bewertung möglicher Menschenrechtsverletzungen nötigen Informationen offenlegen.[95] Auch nach der Rechtsprechung des EGMR steht es Staaten frei, internationale Kooperationsstrukturen einzurichten, um beispielsweise Datensicherheitsoperationen durchzuführen.[96] Allerdings darf dies (gem. dem sog. *Bosporus-Prinzip*[97]) nur erfolgen, sofern und solange das nach der EMRK geltende Niveau des Menschenrechtsschutzes nicht unterlaufen wird.[98] Im Rahmen informeller internationaler Zusammenarbeit können *Accountability*-Mechanismen auch mit Konzepten wie gemeinsamer oder geteilter Verantwortung umrissen werden. Das bedeutet, dass die kooperierenden Staaten gemeinsam für mögliche Datenschutz- oder Menschenrechtsverstöße verantwortlich sind. Wenn Polizeibehörden und Nachrichtendienste international zusammenarbeiten, eröffnet ihnen dies Möglichkeiten, die weiterhin vorwiegend auf nationaler Ebene verankerten *Accountability*-Mechanismen zu umgehen[99] – der *EncroChat*-Fall zeigt dies eindrücklich. Gemeinsame Verpflichtungen, die zu einer gemeinsamen Verantwortung führen, haben sowohl in der Rechtwissenschaft als auch in den politischen Diskursen an Bedeutung gewonnen, sind aber in der Praxis noch nicht konkretisiert worden.[100]

Auch aus der *Big Brother Watch*-Entscheidung des EGMR lassen sich konkrete Anforderungen an eine faire und unabhängige Kontrolle der internationalen Datenverarbeitung ableiten. So betonte der Gerichtshof, es sei notwendig, dass in jedem Stadium der „Massenüberwachung" eine unabhängige Stelle dieses Vorgehen kontrolliert; zudem müsse die Kontrolle „robust" sein.[101] Dazu zählt auch die Verpflichtung der Nachrichtendienste, detaillierte Aufzeichnungen der „Massenüberwachung" zu Kontrollzwecken vorzuhalten. Weiterhin muss die Notwendigkeit und Verhältnismäßigkeit bezüglich der Anwendung von sog. personenbezogenen „starken Suchbegriffen" im Rahmen einer besonderen und objektiven Prüfung schriftlich begründet und behördenintern genehmigt werden.[102] Außerdem

95 *Ryngaert/van Eijk*, International Data Privacy Law 2019 61 (63).
96 Ebd.
97 ECLI:CE:ECHR:2005:0630JUD004503698, „Bosphorus v. Ireland"; Vgl. dazu: *Gonçalves*, JusGov Research Paper No. 2022-05; siehe auch zur Vergleichbarkeit mit Solange Rspr: *Haratsch,* ZaöRV 2006, 927; *Canor,* ZaöRV 2013, 249.
98 *Ryngaert/van Eijk*, International Data Privacy Law 2019, 61 (63).
99 Hierzu näher *Aden*, WEP 2018, 981 (995f).
100 *Ryngaert/van Eijk*, International Data Privacy Law 2019, 61 (64).
101 CE:ECHR:2021:0525JUD005817013, Rn. 356.
102 *Huber,* NvWZ-Beilage 2021, 3 (6).

muss es möglich sein, im Falle von „Massenüberwachung" durch einen EMRK-Konventionsstaat einen wirksamen Rechtsbehelf einzulegen. Das Gericht führte dazu aus, dass die Verpflichtung, eine betroffene Person im Nachhinein über die Massenüberwachung zu unterrichten, eine geeignete Maßnahme darstelle, um zu beurteilen, ob ein Rechtsbehelf wirksam sei.[103] Einer vorherigen Benachrichtigung bedarf es jedoch nicht, wenn auch ohne diese ein Rechtsschutzbegehren möglich ist und eine materiell-rechtliche Prüfung des Begehrens erfolgen kann.[104] Dies muss jedoch auch tatsächlich gegeben sein.

Im Zusammenhang mit der automatisierten Auswertung von Massendaten und den zunehmenden Möglichkeiten, welche die Nutzung KI-basierter Systeme eröffnet, ist es hier zwingend notwendig, die oben beschriebenen Anforderungen von Fairness, Erklärbarkeit und Transparenz in allen Stadien der Nutzung solcher Systeme zu gewährleisten, und zwar bedarfsgerecht und akteurspezifisch.

4. Schlussfolgerungen und Ausblick

Dieser Beitrag hat gezeigt, dass die internationale Zusammenarbeit der Sicherheitsbehörden im großen Umfang eine Informationszusammenarbeit ist und daher im Kern auf Datenaustausch basiert. Grundlegende Prinzipien wie *Fairness*, *Transparenz, KI-Erklärbarkeit* und *Accountability* werden dabei oft vernachlässigt. Die weitreichenden Möglichkeiten der Datenauswertung mithilfe sich stetig entwickelnder KI-Anwendungen verschärfen diese Problematik in der Tendenz. Selbst innerhalb der EU mit ihrem vergleichsweise ausgeprägten Rechtsrahmen für die Zusammenarbeit von Polizeibehörden, der durch verbindliches EU-Recht, die EMRK und die dazu ergehende Rechtsprechung geprägt ist, bleibt die Annahme identischer rechtsstaatlicher Standards bisher mehr Wunsch als Wirklichkeit. Der in diesem Beitrag näher betrachtete *EncroChat*-Fall hat vielmehr erneut gezeigt, dass die transnationale Informationszusammenarbeit den Sicherheitsbehörden „Hintertüren" zur Umgehung rechtsstaatlicher Schutzstandards öffnet.

Die Rolle der EU in diesem Zusammenhang ist durchaus ambivalent. Einerseits werden mit der aktuellen Digitalrechtsgesetzgebung umfangrei-

103 CE:ECHR:2021:0525JUD005817013, Rn. 357.
104 Ebd.

che Regelungen bezüglich der Datenverarbeitung allgemein, aber auch ganz speziell bezüglich der Regulierung von KI unter Einbeziehung von Polizei und Strafjustiz neu geschaffen bzw. konkretisiert. Diese zielen auch auf eine stärkere Informationszusammenarbeit im öffentlichen wie im privaten Bereich ab. Andererseits tragen die europäischen Gerichte wie der EuGH und der EGMR aktiv dazu bei, den bestehenden konventionsrechtlichen Menschenrechtsschutz auch auf diese neuen Entwicklungen anzuwenden. Die fortwährenden Bestrebungen nach immer neuen Überwachungstechniken und Datenverarbeitungsmethoden zu Lasten des Grundrechtsschutzes, können so in Europa jedenfalls ein Stück weit eingehegt werden.

Bei der Informationszusammenarbeit der Sicherheitsbehörden außerhalb der EU bzw. zwischen EU- und Drittstaaten sind Standards wie *Fairness, Transparenz, KI-Erklärbarkeit* und *Accountability* bislang noch deutlich weniger ausgeprägt als innerhalb der EU. Zwar mag die EU auch hier – wie bereits bei der DSGVO – Vorbildcharakter für den Rechtsrahmen außerhalb der EU haben. Höhere und effektive Schutzstandards dürften aber kaum ohne zusätzliche verbindliche völkerrechtliche Regelungen etabliert werden können.

Literatur

Aden, Hartmut (2016): The Role of Trust for the Exchange of Police Information in the European Multi-level System**.** In: Delpeuch, Thierry und Ross, Jacqueline (Hrsg.), *Comparing the Democratic Governance of Police Intelligence. New Models of Participation and Expertise in the United States and Europe*. Cheltenham, UK: Edward Elgar Publishing, S. 322-334.

Aden, Hartmut (2018): Information Sharing, Secrecy and Trust among Law Enforcement and Secret Service Institutions in the European Union. *West European Politics (WEP)* 41(4), S. 981-1002.

Aden, Hartmut (2021): Europäische Rechtsgrundlagen und Institutionen des Polizeihandelns (= Abschnitt M). In: Lisken, Hans und Denninger, Erhard (Hrsg.): *Handbuch des Polizeirechts,* 7. Aufl. München: C.H. Beck, S. 1809-1905.

Aden, Hartmut; Schönrock, Sabrina; John, Sonja; Tahraoui, Milan und Kleemann, Steven (2022): Accountability-Vorkehrungen für die Erfüllung von Menschenrechtspflichten der Polizei bei der Nutzung Künstlicher Intelligenz. *Zeitschrift für Menschenrechte (zfmr),* 16(2), S. 50-72.

Article-29-Datenschutzgruppe (2016): Opinion 01/2016 on the EU–U.S. Privacy Shield draft adequacy decision, 16/EN WP 238 vom 16. April 2016. Brussels. URL: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (besucht am 09. 05. 2023).

Arzt, Clemens (2021): Informationsverarbeitung im Polizei- und Strafverfahrensrecht (=Abschnitt G). In: Lisken, Hans und Denninger, Erhard (Hrsg.): *Handbuch des Polizeirechts,* 7. Aufl. München: C.H. Beck, Rn 1184-1189.

Bäuerle, Michael (2023): Elemente einer Europäischen Vision für die Regulierung von Big Data bei Polizei und Justiz. *Computer und Recht (CR)*, 49(1), S. 64-69.

Bellanova, Rocco; de Goede, Marieke (2022): The algorithmic regulation of security: An infrastructural perspective. *Regulation & Governance*, 16, S. 102-118.

Bignami, Francesca (2007): European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining. *Boston College Law Review 48,* S. 609-698.

Bignami, Francesca (2015): The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens. Study for the LIBE Committee, *GWU Law School Public Law Research Paper* No. 2015-54.

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

Campbell. Duncan (2022): Two convicted in first murder plot case involving EncroChat messaging system. *The Guardian* vom 14. März 2022. URL: https://www.theguardian.com/world/2022/mar/14/two-guilty-of-james-bond-gun-plot-in-encrochat-conviction (besucht am 09. 05. 2023).

Canor, Iris (2013): Solange horizontal – Der Schutz der EU-Grundrechte zwischen Mitgliedstaaten. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV),* 73, S. 249-294.

Dehmel, Susanne; Ossmann-Magiera, Lea Ludmilla und Weiss, Rebekka (2023): Drittstaatentransfers nach Schrems II. *Multimedia und Recht (MMR) Zeitschrift für IT-Recht und Recht der Digitalisierung*, S. 17-22.

Derin, Benjamin und Singelnstein, Tobias (2021): Verwendung und Verwertung von Daten aus massenhaften Eingriffen in informationstechnische Systeme aus dem Ausland (Encrochat). *Neue Zeitschrift für Strafrecht (NStZ)*, S. 449-454.

Europäische Kommission (2021): Entwurf einer Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final, 2021/0106(COD).

Europäische Kommission (2022): Pressemitteilung vom 13.12.2022. URL: https://ec.europa.eu/commission/presscorner/detail/de/ip_22_7631 (besucht am 09. 05. 2023).

Europäischer Datenschutzausschuss (EDSA) (2020) Empfehlungen 02/2020 zu den wesentlichen europäischen Garantien in Bezug auf Überwachungsmaßnahmen. URL: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_de.pdf (besucht am 09. 05. 2023).

Europäischer Datenschutzausschuss (EDSA) (2021): Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten. URL: https://edpb.europa.eu/system/files/2022-04/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_de.pdf (besucht am 09. 05. 2023).

Europäischer Datenschutzausschuss (EDSA) (2023): Pressemitteilung vom 28.2.2023. URL: https://edpb.europa.eu/news/news/2023/edpb-welcomes-improvements-under-eu-us-data-privacy-framework-concerns-remain_de (besucht am 09. 05. 2023).

Europäischer Datenschutzbeauftragter (EDSB) (2020): Entscheidung vom 17.9.2020 – C 2019-0370. URL: https://edps.europa.eu/sites/edp/files/publication/20-09-18_edps_decision_on_the_own_initiative_inquiry_on_europols_big_data_challenge_en.pdf (besucht am 09. 05. 2023).

Europäischer Datenschutzbeauftragter (EDSB) (2021): Entscheidung vom 21.12.2021 – C 2021-0699. URL: https://edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf (besucht am 09. 05. 2023).

Europäisches Parlament (2021): Exchanges of Personal Data after the Schrems II Judgment, PE 698.678. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf (besucht am 09. 05. 2023).

Europäisches Parlament (2022): EncroChat's path to Europe's highest courts. URL: https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/739268/EPRS_ATA(2022)739268_EN.pdf (besucht am 09. 05. 2023).

Europarat (2020): Ad Hoc Committee on Artificial Intelleigence (CAHAI), Feasibility Study, CAHAI(2020)23, 17.12.2020.

European Network of Forensic Science Institutes (2021): Best Practice Manual for Digital Image Authentication, ENFSI-BPM-DI-03, 1. URL: https://enfsi.eu/wp-content/uploads/2022/12/1.-BPM_Image-Authentication_ENFSI-BPM-DI-03-1.pdf (besucht am 09. 05. 2023).

European Union Agency for Criminal Justice Cooperation (2020): Eurojust Pressemitteilung vom 2.7.2020. URL: https://www.eurojust.europa.eu/news/dismantling-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe (besucht am 09. 05. 2023).

Ewald, Uwe (2018): Digitale Beweismittel und neue Wege der Strafverteidigung. In: Strafverteidigervereinigungen, Organisationsbüro (Hrsg.): *Räume der Unfreiheit, Texte und Ergebnisse des 42. Strafverteidigertages*, Münster, 2.-4.3.2018.

Generalversammlung der Vereinten Nationen (2014): Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc. A/69/397, 23.09.2014.

Gonçalves, Anabela Susana de Sousa (2022): The ECtHR's Bosphorus Presumption and the European Union's principle of mutual trust. JusGov Research Paper No. 2022-05.

Glouftsios, Georgios; Leese Matthias (2023): Epistemic Fusion: Passenger Information Units and the making of international security, *Review of International Studies*, 49(1), S. 125-142.

Goodwin, Bill (2022): Police EncroChat cryptophone hacking implant did not work properly and frequently failed, *Computer weekly* vom 11. März 2022. URL: https://www.computerweekly.com/news/252514476/Police-EncroChat-cryptophone-hacking-implant-did-not-work-properly-and-frequently-failed (besucht am 09. 05. 2023).

Gressel, Céline und Orlowski, Alexander (2019): Integrierte Technikentwicklung: Herausforderungen, Umsetzungsweisen und Zukunftsimpulse. *TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis*, 28(2), S. 71–72.

Haratsch, Andreas (2006): Die Solange-Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte – Das Kooperationsverhältnis zwischen EGMR und EuGH. *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht (ZaöRV),* 66, S. 927-947.

Hornung, Gerrit (2022): Künstliche Intelligenz zur Auswertung von Social Media Massendaten – Möglichkeiten und rechtliche Grenzen des Einsatzes KI-basierter Analysetools durch Sicherheitsbehörden. *Archiv des öffentlichen Rechts (AöR)*, 147(1), S. 1-69.

Huber, Bertold (2020): Das BVerfG und die Ausland-Ausland-Fernmeldeaufklärung des BND. *Neue Zeitschrift für Verwaltungsrecht (NVwZ-Beilage)*, S. 3-9.

Huber, Bertold (2021): „Massenüberwachung" vor dem EGMR. *Neue Zeitschrift für Verwaltungsrecht (NvWZ-Beilage)*, S. 3-10.

Iliadis, Andrew und Acker, Amelia (2022): The seer and the seen: Surveying Palantir's surveillance platform. *The Information Society*, 38(5), S. 334-363.

Kävrestad, Joakim (2020): *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications*, 2. Aufl., Heidelberg: Springer.

Kipker, Dennis-Kenji (2021): Der Elefant im Raum: Aktuelle Diskussion um den Drittlandtransfer personenbezogener Daten. *Zeitschrift für Datenschutz (ZD)*, S. 397-398.

Kipker, Dennis-Kenji und Bruns, Hauke (2022): EncroChat und die „Chain of Custody". *Multimedia und Recht (MMR) Zeitschrift für IT-Recht und Recht der Digitalisierung*, S. 363-368.

Lavenex, Sandra (2007): Mutual recognition and the monopoly of force: limits of the single market analogy, *Journal of European Public Policy*, 14(5), S. 762-779.

Lowe, Mattew R. (2021): All Eyes on U.S.: Regulating the Use & Development of Facial Recognition Technology, *Rutgers Computer & Technology Law Journal,* 48(1), S. 1-50.

Mehrabi, Ninareh; Morstatter, Fred; Saxena, Nripsuta Ani; Lerman, Kristina und Galstyan, Aram (2021): A Survey on Bias and Fairness in Machine Learning. *ACM Computing Surveys (CSUR)*, 54,(6), Article 115, S. 1-35.

Menschenrechtsrat der Vereinten Nationen (2014): Concluding observations on the fourth periodic report of the United States of America, CCPR/C/USA/CO/4, 23.04.2014.

Menschenrechtsrat der Vereinten Nationen (2018): The right to privacy in the digital age, Report of the United Nations High Commissioner for Human Rights, A/HRC/39/29, 3.8.2018.

Menschenrechtsrat der Vereinten Nationen (2021): The right to privacy in the digital age - Report of the United Nations High Commissioner for Human Rights, A/HRC/48/31, 13.9.2021.

National Institute of Standards and Technology (NIST) (22. Nov. 2022): Digital and Multimedia Evidence. URL : https://www.nist.gov/spo/forensic-science-program/digital-and-multimedia-evidence (besucht am 09. 05. 2023).

O'Brien, Thomas C. und Tyler, Tom R. (2019): Rebuilding trust between police & communities through procedural justice & reconciliation. *Behavioral Science & Policy*, 5(1), S. 35–50.

OECD (2019): Empfehlung des Rats zu künstlicher Intelligenz, OECD/LEGAL/0449, 22.5.2019.

Pauli, Gerhard (2021): Zur Verwertbarkeit der Erkenntnisse ausländischer Ermittlungsbehörden – EncroChat. *Neue Zeitschrift für Strafrecht (NStZ)*, S. 146-149.

Pidoux, Jérémy (2022): Premiers contrôles par la Cour de cassation de procédures ouvertes à la suite de l'opération dite « EncroChat », *Dalloz actualité* vom 14. Nov. 2022. URL: https://www.dalloz-actualite.fr/flash/premiers-controles-par-cour-de-cassation-de-procedures-ouvertes-suite-de-l-operation-dite-encr#.ZBRPDISZOUk (besucht am 09. 05. 2023).

Quintel, Teresa (2022): The EDPS on Europol's Big Data Challenge in Light of the Recast Europol Regulation: The Question of Legitimizing Unlawful Practices. *European Data Protection Law Review (EDPL)*, 8(1), S. 90-102.

Raposo, Vera L. (2023): (Do not) remember my face: uses of facial recognition technology in light of the general data protection regulation. *Information & Communications Technology Law*, 32(1), S. 45-63.

Ruppert, Felix (2022): Erheben ist Silber, Verwerten ist Gold? Verwendbarkeit und Verwertbarkeit von Daten ausländischer Ermittlungsbehörden im Lichte des Grundrechtsschutzes – EncroChat. *Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt)*, S. 221-227.

Rüß, Oliver und Lutz, Markus (2022): Die novellierte Europol-Verordnung: Eine europäische Antwort auf das FBI?. *Zeitschrift für das gesamte Sicherheitsrecht (GSZ),* S. 221-228.

Ryngaert, Cedric M.J. und van Eijk, Nico A.N.M. (2019): International Cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees. *International Data Privacy Law*, 9(1), S. 61-73.

Schmahl Stefanie (2019): Intelligence and Human Rights. In: Dietrich, Jan-Hendrick und Sule Satish (Hrsg.): *Intelligence Law and Policies in Europe*, München, Bloomsbury, S. 291-334.

Schmahl, Stefanie (2020): Grundrechtsbindung der deutschen Staatsgewalt im Ausland. *Neue Juristische Wochenschrift (NJW)*, S. 2221-2224.

Staffler, Lukas (2016): Geheimdienstliches Verschwindenlassen von Terrorverdächtigen (extraordinary renditions) im Lichte der EGMR-Judikatur: der Fall Nasr (alias Abu Omr) und Ghali gegen Italien. *Europäische Grundrechte-Zeitschrift (EuGRZ)*, S. 344-352.

Stoykova, Adi (2021): Digital Evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review*, 42, S. 1-20.

Sunshine, Jason und Tyler, Tom R. (2003): The Role of Procedural Justice and Legitimacy in Shaping Public Support for Policing. *Law and Society Review*, 37(3), S. 513-548.

The White House (07. Okt. 2022): Federal Register, Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities Executive Order 14086., URL: https://www.govinfo.gov/content/pkg/FR-2022-10-14/pdf/2022-22531.pdf (besucht am 09. 05. 2023).

UNESCO Recommendation on the ethics of artificial intelligence, SHS/BIO/REC-AI-ETHICS/2021, 2021.

United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism (2014): Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc A/69/397.

United Nations Chief Executive Board (2022): Principles for the ethical use of artificial intelligence in the United Nations system, CEB/2022/2/Add.1, Chief Executives Board for Coordination Distr.: General 27.10.2022.

Venice Commission (2015): Report on the Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session, Venedig 20.-21.3.2015, CDL-AD(2015)011.

Wexler, Rebecca (2021): Privacy Asymmetries: Access to Data in Criminal Defense Investigations. *UCLA Law Review*, 68(1), S. 212-287.

Teil IV: Desinformation

Wissenschaftliche Falschinformation: Erforschung von Faktoren der Verbreitung im Gesundheitsbereich

Juliane Stiller, Violeta Trkulja, Leyla Dewitz, Isabella Peters, Maria Henkel und Paulina Bressel

Zusammenfassung

Des- und Falschinformation ist ein globales Phänomen, welches gefährliche Auswirkungen für demokratische Strukturen und offene Gesellschaften haben kann. Wenn Informationsquellen, die Menschen nutzen und weitergeben, nicht verlässlich und korrekt sind, kann dies weitreichende Konsequenzen haben, vor allem im Gesundheitsbereich. Der Überfluss an falschen, aber auch evidenzbasierten Gesundheitsinformationen macht es immer schwieriger, valide Informationen zu identifizieren. Des- und Falschinformationskampagnen nutzen das Vertrauen der Menschen in wissenschaftliche Gesundheitsexpert:innen und Gesundheitsinformationen aus. Durch Nachahmung wissenschaftlicher Kriterien und Vortäuschung eines wissenschaftlichen Ursprungs kommt es zu einer weiteren Verbreitung von falscher Gesundheitsinformation. Daher müssen die Formen und Verbreitungswege wissenschaftlicher Falschinformation im Gesundheitsinformationsverhalten besser verstanden werden, um effektiv dagegen vorgehen zu können. Der Beitrag beschäftigt sich mit dem komplexen Begriffsfeld „Des- und Falschinformation" und diskutiert dies vor dem Hintergrund von Gesundheitsinformationsverhalten und wissenschaftlicher Falschinformation. Zudem werden Typen wissenschaftlicher Falschinformation erläutert sowie das vom BMBF geförderte Forschungsprojekt *DESIVE² – Desinformationsverhalten verstehen* vorgestellt. Dieses nutzt qualitative Forschungsmethoden, um Faktoren für die Verbreitung wissenschaftlicher Falschinformation zu bestimmen und sie in einem Modell des Falschinformationsverhaltens miteinander in Verbindung zu bringen. Die im Projekt durchzuführenden Studien sind multimethodisch angelegt und beinhalten qualitative Leitfadeninterviews, sowie Tagebuchstudien und Umfragen in der Bevölkerung mittels einer Smartphone-App.

1. Einleitung

Informationen, die von Menschen genutzt und weitergegeben werden, und die unverlässlich, falsch, missverständlich oder irreführend sind, können gefährliche Auswirkungen, u.a. auf demokratische Strukturen und offene Gesellschaften haben: Menschen sind nicht mehr in der Lage, fundierte Entscheidungen zu treffen oder treffen gegebenenfalls Entscheidungen, die ihnen selbst oder anderen Schaden zufügen.

Ein Beispiel hierfür sind Informationen im Kontext der COVID-19-Pandemie. Neben dem Anstieg der Anzahl von Nachrichten und Informationen zu COVID-19 und der Pandemie im Allgemeinen, kam es ebenfalls zu einem enormen Anstieg der Verbreitung wissenschaftlicher Gesundheitsinformationen (Islam u.a. 2020). Hier zeigte sich, dass die weite (oft absichtliche) Distribution falscher gesundheitsbezogener Informationen negative Auswirkungen auf Gesundheitsentscheidungen der Bevölkerung hatte, wie zum Beispiel die Entscheidung, sich nicht impfen zu lassen. Dadurch hemmen falsche Gesundheitsinformationen Maßnahmen zur Bekämpfung von Gesundheitskrisen (Baines/Elliott 2020).

Die gezielte Suche nach Gesundheitsinformationen gilt als eine wichtige Bewältigungsstrategie bei der psychosozialen Anpassung an Krankheiten und ist somit auch eine gesundheitsfördernde Aktivität. Menschen suchen über eine Vielzahl von verschiedenen Informationsquellen nach Informationen (Dewitz 2022). Die COVID-19-Pandemie wurde von einer großen Menge an falschen und irreführenden Informationen begleitet und entwickelte sich zu einer „Infodemie" – einer Überfülle an evidenzbasierter, aber auch falscher Informationen (World Health Organization 2020). Diese schnelle Verbreitung und die Vielzahl an Informationen führt dazu, dass die Informationsqualität nur schwer durch die Rezipierenden evaluiert werden kann (De Gani u.a. 2022). Hier gewinnt die Informationskompetenz eine immer größere Bedeutung, da sie Menschen befähigt, den Informationsgehalt von Quellen zu bewerten oder zu validieren. In diesem Zusammenhang stellt auch die Gesundheitskompetenz eine wichtige Voraussetzung für das Auffinden, Verstehen, Beurteilen und Anwenden von Gesundheitsempfehlungen dar (De Gani u.a. 2022).

Wie die COVID-19-Pandemie gezeigt hat, können informationelle Phänomene, wie *Information Overload* (Informationsüberlastung), *Information Anxiety* (Informationsangst) und *Information Avoidance* (Informationsvermeidungsverhalten) u.a. als Reaktionen auf eine fehlende Validierungsfähigkeit in Bezug auf Gesundheitsquellen entstehen, welche ebenfalls auf

eine limitierte Informationskompetenz zurückzuführen sind (Soroya u.a. 2021). Allerdings vertrauen Menschen Gesundheitsinformation, wenn sie von wissenschaftlichen Gesundheitsexpert:innen stammt (Baumann u.a. 2020). Das Vertrauen in diese Informationsquellen kann auch die Verbreitung derartiger Informationen legitimieren, und dies machen sich u.a. Des- und Falschinformationskampagnen zunutze. Information lediglich als wissenschaftlich erscheinen zu lassen oder einen wissenschaftlichen Ursprung vorzutäuschen, und damit in die Irre zu führen, kann zu einer weiteren und effektiveren Verbreitung von u.a. Gesundheitsinformation führen (Loomba u.a. 2021).

Um zukünftigen gesellschaftlichen Herausforderungen besser begegnen zu können, ist ein tiefergehendes Verständnis der Verbreitungsmechanismen von wissenschaftlich anmutender, aber falscher Information sowie deren Auswirkungen auf das Informationsverhalten von Menschen erforderlich. Wie auch in Greifeneder/Schlebbe (2023) beschrieben, wird allgemein unter Informationsverhalten der Umgang von Menschen mit Informationen verstanden und im Speziellen, wie diese Informationen suchen und nutzen (Bates 2017). Dies schließt auch die aktive und passive Informationssuche und Informationsnutzung ein (Wilson 2000). Die wahrgenommene Wissenschaftlichkeit als Motor für (digitale) Kampagnen mit Falsch- oder Desinformation ist hierbei noch wenig erforscht (Hahn u.a. 2020). Sie stellt Menschen vor neue Herausforderungen, da sie besondere Fähigkeiten und Expertise benötigen, um Gesundheitsinformation, die wissenschaftliche Merkmale aufweist (z.B. die Nennung von Quellen oder p-Werten), dennoch als Des- oder Falschinformation zu entlarven. Das individuelle und gesellschaftliche Vertrauen in (gesundheits-)wissenschaftliche Erkenntnisse und Fachexpertise wird durch Des- und Falschinformation, wie *Fake News* und Verschwörungsmythen, erschüttert (Schaeffer u.a. 2021).

Eine Möglichkeit, um dieser Herausforderung zu begegnen, ist die Identifizierung der verschiedenen Arten von irreführender wissenschaftlicher Gesundheitsinformation im Kontext des menschlichen Informationsverhaltens. Dabei kann es sich um Information handeln, die tatsächlich wissenschaftlichen Ursprungs, jedoch falsch ist oder im Nachhinein als falsch eingestuft wird, oder Falschinformation, deren Wissenschaftlichkeit vorgetäuscht wird. Weiterhin ist ein ganzheitliches Verständnis der relevanten Aspekte von Des- und Falschinformationsverhalten unerlässlich, z.B. die zugrundeliegenden Mechanismen der Verbreitung von derartiger Informa-

tion und damit die Wurzel von Des- und Falschinformationskampagnen. Eine Modellierung des Des- und Falschinformationsverhaltens trägt dazu bei, der Verbreitung von Desinformation entgegenzuwirken[1].

Ziel dieses Beitrages ist es, das Begriffsfeld um „Desinformation", „Falschinformation" und „Misinformation" aufzuspannen und für die Anwendungsbereiche Gesundheitsinformationsverhalten und wissenschaftliche Falschinformation zu diskutieren, sowie Definitionen für sie bereitzustellen. Dazu werden die Auswirkungen von Falschinformationen im Gesundheitsbereich erläutert und die verschiedenen Formen und Entstehungsweisen wissenschaftlicher Falschinformation eingehend betrachtet. In Abschnitt 3 werden die Ziele und der methodische Ansatz des Forschungsprojektes DESIVE² vorgestellt, für die beiden Anwendungsfelder kontextualisiert und die Notwendigkeit einer multimethodischen Herangehensweise zur Erforschung von Verbeitungsmechanismen von Des- und Falschinformation begründet. Der Beitrag schließt mit zusammenfassenden Bemerkungen und einem Ausblick.

2. Wissenschaftliche Falschinformation im Gesundheitsinformationsverhalten

Im Folgenden werden zunächst zentrale Begriffe aus dem Begriffsfeld „Desinformation" definiert und dann die Problematik um Falschinformation im Gesundheitsinformationsverhalten erläutert. Eine Beschreibung des Zusammenhangs zwischen Falschinformation und wissenschaftlicher Information sowie eine Chararakterisierung wissenschaftlicher Falschinformation folgt im Anschluss.

2.1 Das Begriffsfeld

Die drei Begriffe „Desinformation", „Falschinformation" und „Misinformation" werden im allgemeinen Sprachgebrauch häufig nicht unterschieden, erfahren im wissenschaftlichen Diskurs aber eine differenzierte Betrachtung. Unter *Desinformation* wird irreführende, missverständliche oder so-

1 Das im Herbst 2021 gestartete und vom Bundesministerium für Bildung und Forschung geförderte Verbundprojekt „DESIVE² – Desinformationsverhalten verstehen" möchte hierzu einen Beitrag leisten. Im Verbundprojekt arbeiten die ZBW – Leibniz-Informationszentrum Wirtschaft, die Humboldt-Universität zu Berlin und Grenzenlos Digital e.V. zusammen, Website: www.desive2.org. Abgerufen am 27.02.2023.

gar falsche Information verstanden, die vorsätzlich in Umlauf gebracht wird (Fallis 2015). Unter *Misinformation* hingegen wird eine Information verstanden, die zunächst als gültig angesehen, jedoch später zurückgezogen oder korrigiert wird (Lewandowsky u.a. 2012). Häufig wird hier auch die Unterscheidung von Wardle/Derakhshan (2017) herangezogen, bei der die Schadensabsicht das Hauptkriterium darstellt, um Misinformation von Desinformation zu unterscheiden.

Da es oftmals nicht möglich ist, zwischen vorsätzlicher Desinformation und unbeabsichtigter Misinformation zu unterscheiden (da man dazu die Intention der Erstellenden in Erfahrung bringen müsste, was vor allem, aber nicht nur, im Online-Kontext problematisch ist), wird im Folgenden die Bezeichnung *Falschinformation* als Oberbegriff verwendet, um die beiden anderen Begriffe einzuschließen. Es ist auch im Rahmen des Forschungsvorhabens (siehe Abschnitt 3) zielführender, keine Unterscheidung von (wissenschaftlicher) Misinformation und Desinformation vorzunehmen, die auf eine Absicht abstellt. Denn sobald eine Information nicht richtig ist, liegt ein Fall von wissenschaftlicher Falschinformation vor, unabhängig davon, ob dieser Vorgang unabsichtlich (wissenschaftliche Misinformation) oder absichtlich (wissenschaftliche Desinformation) geschieht.

2.2 Falschinformation im Gesundheitsbereich

Falschinformationen entfalten oftmals in der Interaktion mit und von Menschen ihren negativen Einfluss. Die menschliche Interaktion mit Information wird als „Informationsverhalten" (Wilson 2022, S. 12) bezeichnet. Dies schließt auch sämtliche aktiven, passiven (Kelly 2014) und vermeidenden menschlichen Interaktionen, sowie affektiven und zufälligen Verhaltensweisen beim Monitoring, Nutzen, Suchen, Teilen, Entdecken und Managen von (Gesundheits-)Informationen mit ein (Dewitz 2022). Ob eine Information in dem Zusammenhang wahr oder falsch ist, spielt für das Informationsverhalten eine untergeordnete Rolle und wird bisher lediglich in wenigen Modellen des Informationsverhaltens betrachtet (z.B. in Karlova/Fisher 2013 und Agarwal/Alsaeedi 2021).

Zahlreiche kontextuelle und individuelle Dimensionen beeinflussen oder prägen das Informationsverhalten von Menschen, so z.B. die Persönlichkeit, persönliche Erfahrungen, Wissen oder Vorkenntnisse über einen Sachverhalt sowie die sozialen Rahmenbedingungen und die kulturelle Eingebundenheit einer Person. Weiterhin ist der Informationsbedarf einer Person, das Werkzeug, welches zur Informationssuche genutzt wird, oder

die Art der Information, die gesucht (oder nicht gesucht), erhalten oder gar vermieden wird, mit diesen Dimensionen verbunden (Godbold 2006). Informationsverhalten ist somit individuell und kontextuell geprägt und spiegelt das komplexe Zusammenwirken dieser verschiedenen Facetten wider.

Wenn Menschen mit Gesundheitsinformationen interagieren, handelt es sich um das sogenannte „Gesundheitsinformationsverhalten" (*Health Information Behaviour*). Die am weitesten verbreitete Definition von „Gesundheit" stammt aus der Verfassung der Weltgesundheitsorganisation, die sie als "einen Zustand vollständigen körperlichen, seelischen und sozialen Wohlbefindens und nicht nur das Freisein von Krankheit und Gebrechen" (World Health Organization, 2020)[2] beschreibt. Demzufolge wird im Projekt DESIVE[2] jegliche Information im Kontext von Gesundheit als Gesundheitsinformation verstanden.

In Zusammenhang mit Health Information Behaviour steht die „Gesundheitskompetenz", die Menschen befähigt, Gesundheitsinformation zu finden und zu verstehen (De Gani u.a. 2022). Im digitalen Raum wird dies auch als digitale Gesundheitskompetenz bezeichnet. Darunter werden die "Fähigkeiten [verstanden], im Internet relevante Gesundheitsinformation zu suchen, zu finden, sie zu verstehen, deren Zuverlässigkeit zu beurteilen und sie umzusetzen" (Schaeffer u.a. 2021, S. 68). Nach der 2021 veröffentlichten Health-Literacy-Studie (HLS-GER 2) ist die digitale Gesundheitskompetenz bei der Mehrzahl (75,8%) der deutschen Bevölkerung eher gering (Schaeffer u.a. 2021). Dabei wird die Beurteilung von Gesundheitsinformationen am schwierigsten eingeschätzt und auffallend große Probleme bereitet vor allem die "Beurteilung der Vertrauenswürdigkeit digitaler und medialer Information" (Schaeffer u.a. 2021, S. 88).

Nicht einschätzbare oder beurteilbare Informationen können nicht nur zu Verunsicherung führen, sondern auch zu einer weiteren Verbreitung von Falschinformationen im Gesundheitsbereich. Schaefer/Bitzer (2021) nennen mehrere Konsequenzen, die falsche Informationen im Gesundheitsbereich haben können: Sie vermitteln ein verzerrtes Bild von Wirksamkeit und/oder Schäden von Gesundheitsmaßnahmen und können Menschen

2 In der Präambel der Verfassung der Weltgesundheitsorganisation (WHO) von 1946 definiert diese: "Health is a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity." Zitiert nach Basic documents: forty-ninth edition (including amendments adopted up to 31 May 2019). Geneva: World Health Organization; 2020. Online: https://apps.who.int/gb/bd/pdf_files/BD_49th-en.pdf. Abgerufen am 27.02.2023.

zu Handlungen motivieren, die ihnen selbst oder anderen Schaden zufügen können. Weiterhin können Falschinformationen das Vertrauen in die Institutionen und Maßnahmen untergraben, die diese einführen und durchführen sollen (Schaefer/Bitzer 2021). Welch schwerwiegende Folgen Falschinformationen im Gesundheitsbereich haben können, konnte auch in wissenschaftlichen Studien nachgewiesen werden. So hat eine Studie Menschen (n=6001) aus Großbritannien und den Vereinigten Staaten mit Falschinformationen zum Thema Impfung konfrontiert und festgestellt, dass sie im Anschluss weniger bereit waren, sich impfen zu lassen (Loomba u.a. 2021). Der Effekt auf die Senkung der Impfbereitschaft ist besonders stark bei der Art von Falschinformation, die wissenschaftlich erscheint oder wissenschaftlich anmutet, in welcher beispielsweise wissenschaftliche Bilder oder Links verwendet wurden (Loomba u.a. 2021).

Auch Islam u.a. (2020) zeigen, dass Falschinformationen und Gerüchte zur COVID-19-Pandemie in Sozialen Medien weit verbreitet sind und dass Menschen, die diesen Glauben schenken, schwerwiegende gesundheitliche Konsequenzen erfahren und manchmal sogar sterben können. Diese Beispiele verdeutlichen, wie wichtig es ist, das Auftreten von Falschinformation im Gesundheitskontext besser zu verstehen und Strategien gegen ihre Verbreitung zu entwickeln, sodass Menschen einfachen Zugang zu vertrauenswürdigen Gesundheitsinformationen erhalten.

Vertrauenswürdige Gesundheitsinformation sollte evidenzbasiert sein und somit aus wissenschaftlichen Quellen stammen. Dafür hat sich auch die evidenzbasierte Gesundheitsinformation etabliert, die neben weiteren Kriterien die Anforderung erfüllen muss, dass sie durch Methoden der evidenzbasierten Medizin entstanden ist (Büchter/Albrecht 2021). Da evidenzbasierte Gesundheitsinformation in der Fülle an Informationen zu bestimmten Gesundheitsthemen (wie COVID-19) nur eine von vielen und somit schwer zu identifizieren und von Falschinformation zu unterscheiden ist (World Health Organization, 2020), bedarf es einer weiteren tiefergehenden Analyse, wie Falschinformation zu Gesundheitsthemen weiter ausdifferenziert werden kann.

2.3 Wissenschaftliche Falschinformation

Falschinformation mit Bezug zur Wissenschaft präsentiert sich auf vielfältige Weise. Dieser Zusammenhang ist offensichtlich, wenn es um pseudowissenschaftliche oder anti-wissenschaftliche Aussagen geht, die bewusst fal-

sche Informationen enthalten. Hierbei handelt es sich um wissenschaftliche Falschinformation (*Science Disinformation* oder auch *Science Misinformation*). Die European Federation of Academies of Science and Humanities (ALLEA)[3] definiert wissenschaftliche Desinformation als faktisch falsche Information in Bezug auf Aussagen über wissenschaftliche Themen, die wissentlich fingiert und manipuliert wurden, mit dem Ziel, Menschen in die Irre zu führen (ALLEA 2021). In dieser Definition schließen sie auch die bewusste Verbreitung von Misinformation mit ein. Wissenschaftliche Misinformation ist "incorrect information regarding scientific matters that has been produced by mistake but without the intention to cause harm, caused for instance by scientific misconduct, lack of research integrity, or poor communication of scientific results" (ALLEA 2021, S. 3). Dies ist anders als bei den allgemeinen Definitionen, die eine Absicht der Erstellenden der Information zur Unterscheidung von Des- und Misinformation voraussetzen (siehe Abschnitt 2.1). Wir halten im Folgenden und für das Forschungsprojekt an der umfassenderen Bezeichnung „wissenschaftliche Falschinformation" fest, um alle Fälle betrachten zu können.

Um wissenschaftliche Falschinformation und deren Entstehung besser verstehen zu können, bedarf es auch eines Verständnisses darüber, wie wissenschaftliche Falschinformation im Allgemeinen zu erkennen und von evidenzbasierter wissenschaftlicher Information abzugrenzen ist. Southwell u.a. (2022) nennen hier zwei Merkmale: eine wissenschaftliche Behauptung kann falsch sein, wenn sie erstens vorhandenen empirischen Beweisen widerspricht, und zweitens, wenn es für eine wissenschaftliche Behauptung gar keine untermauernden empirischen Beweise gibt. Diese Kriterien ermöglichen es, bessere Analysen über das Ausmaß und die Verbreitung wissenschaftlicher Falschinformation durchzuführen.

Wie wissenschaftliche Falschinformation zustande kommt, ist bisher wenig systematisch untersucht worden. Eine häufig angebrachte Erklärung ist, dass die Ursache im Wissenschaftssystem selbst begründet liegt, in welchem schnelle Publikationen erwartet werden, von denen wiederum die Karrieren der Autor:innen abhängen. Dies führt dazu, dass Wissenschaftler:innen einen Anreiz haben, eher überraschende Ergebnisse zu publizieren, die potenziell mehr Aufmerksamkeit erhalten (West/Bergstrom 2021).

Es können drei Fälle von wissenschaftlicher Falschinformation unterschieden werden, die den Ursprung der Information (i.e., das Wissen-

3 https://allea.org/. Abgerufen am 27.02.2023.

schaftssystem) und die Art und Weise der Herstellung dieser Information (z.B. wissenschaftliche Kriterien) in Verbindung bringen:

1. Informationen, die Wissenschaftlichkeit vortäuschen und falsch sind. Dies wird als „Pseudoscience" kategorisiert (ALLEA 2021; Falyuna 2022) oder auch als „Fake-Science" (Hopf u.a. 2019) bezeichnet.
2. Informationen, die aus dem Wissenschaftssystem kommen und unter Einhaltung wissenschaftlicher Standards entstanden sind, und in der Folge als falsch betrachtet werden, da sie aus unterschiedlichen Gründen überholt und veraltet sind oder widerlegt wurden. Darüber hinaus können Informationen, die aus dem Wissenschaftssystem kommen und faktisch richtig sind, auch durch den Rezeptionsprozess verfälscht werden, z.B. durch Spins in der journalistischen Berichterstattung (Boutron u.a. 2019).
3. Informationen, die aus dem Wissenschaftssystem kommen und falsch sind, jedoch keine wissenschaftlichen Kriterien erfüllen, da sie beispielsweise durch wissenschaftliches Fehlverhalten entstanden sind. Dazu zählen u.a. das Fälschen von Daten oder fehlende wissenschaftliche Integrität, für die die Wissenschaft das Zurückziehen (*Retraction*) einer solchen Publikation vorsieht. Weiterhin kann Falschinformation auch von Wissenschaftler:innen unabhängig von Publikationen verbreitet werden, wenn diese außerhalb ihrer Fachdisziplin verzerrende Informationen, die mitunter auch komplett falsch sein können, weitergeben.

Abb. 1 zeigt eine grafische Interpretation dieser Fälle, angelehnt an die oft verwendete Darstellung zur Unterscheidung von Desinformation, Malinformation und Misinformation (Wardle/Derakhshan 2017). Drei der dort beschriebenen Phänomene, durch die wissenschaftliche Falschinformation ensteht oder in Umlauf gebracht wird, werden im Folgenden näher erläutert – wobei eine umfängliche Charakterisierung und Klassifikation von wissenschaftlicher Falschinformation noch ein Forschungsdesiderat ist und durch DESIVE² adressiert werden soll.

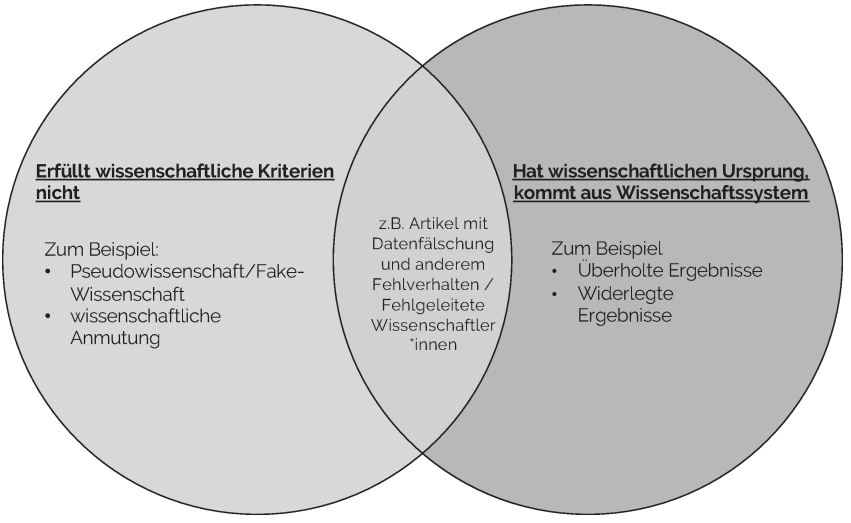

Abb. 1: Drei Fälle wissenschaftlicher Falschinformation, modifiziert nach (Wardle & Derakhshan, 2017)

Zurückgezogene Publikationen

Das Zurückziehen einer wissenschaftlichen Publikation wird gemeinhin als Mittel verstanden "by which the scientific record is corrected" (Wray/Andersen 2018). Die Gründe für den Rückzug einer Publikation sind sehr vielfältig. Der Blog "Retraction Watch"[4], der es sich zur Aufgabe gemacht hat, Rückzüge von Publikationen akribisch zu dokumentieren, listet neben wissenschaftlichem Fehlverhalten hunderte weitere Gründe auf, die zur Rücknahme von Fachartikeln aus wissenschaftlichen Zeitschriften geführt haben[5]. Ein Grund für die Revision oder den Rückzug von wissenschaftlichen Fachartikeln kann die beabsichtigte oder unbeabsichtigte „wissenschaftliche Verzerrung" (*scientific distortion* (Bar-Ilan/Halevi 2018, S. 1771)), oder auch „wissenschaftliches Fehlverhalten" (*scientific misconduct* (ebd. S. 1775)) von Forschungsartikeln sein. Dies beinhaltet u. a. die Manipulation von Daten, falsche Schlussfolgerungen, Nichtreplizierbarkeit, oder schlichtweg Datenfehler (Bar-Ilan/Halevi 2018).

4 https://retractionwatch.com/. Abgerufen am 27.02.2023.

5 Retraction Watch Database User Guide Appendix B: Reasons: https://retractionwatch.com/retraction-watch-database-user-guide/retraction-watch-database-user-guide-appendix-b-reasons/. Abgerufen am 27.02.2023.

Den meisten zurückgezogenen Publikationen liegen nicht wissenschaftliches Fehlverhalten zugrunde, sondern andere Fehler. Die Untersuchung von Wray/Andersen (2018) zeigt, dass für 51% der zurückgezogenen Artikel in der Fachzeitschrift "Science" unbeabsichtigte Fehler als Grund für die Rücknahme angeführt wurden. Wray und Andersen (2018) haben diese Kategorie gewählt, wenn die Information über die Retraction keinen Rückschluss auf Fehlverhalten zuließ. Für 35% der Artikel konnte wissenschaftliches Fehlverhalten als Grund für die Retraction identifiziert werden.

Die Berichtigung von wissenschaftlichen Ergebnissen (*scientific record*) bedeutet demnach nicht, dass etwas zwangsläufig faktisch falsch war und der Rückzug einer Publikation lässt nicht immer auf die schlechte Qualität der Publikation oder auf schlechte Absichten der Autor:innen schließen. Es bedeutet für die Wissenschaft jedoch immer, dass die besagte Publikation nicht mehr zitiert und nicht mehr weiterverbreitet werden sollte, zumindest nicht ohne den Kontext ihres Rückzugs zu nennen.

Rezeption durch Wissenschaftskommunikation

Im vorhergehenden Abschnitt bezog sich die Betrachtung von Falschinformation und das Zurückziehen auf wissenschaftliche Publikationen. Doch viele der sich in Umlauf befindenden Falschinformationen, die auf wissenschaftliche Publikationen zurückzuführen sind, in ihnen jedoch nicht notwendigerweise vorkommen müssen, entstehen in der Rezeption der Publikation. Deshalb ist es von Interesse, den Prozess, den wissenschaftliche Ergebnisse auf ihrem Rezeptionsweg durchlaufen, näher zu untersuchen und besser zu verstehen.

Southwell u.a. (2022) vertreten die Perspektive, dass wissenschaftliche Falschinformation eine Störung der „öffentlichen Wissenschaft" (*public science*), jedoch keine Störung der Wissenschaft selbst (*research science*) darstellt. Unter öffentlicher Wissenschaft verstehen sie den Ansatz, Forschung und ihre Ergebnisse für die Rezeption einer breiten Öffentlichkeit aufzubereiten. Dies geschieht durch vermittelte Kommunikation, z.B. durch Wissenschaftskommunikation oder Wissenschaftsjournalismus. Für die Autor:innen ist wissenschaftliche Misinformation ein "complex communication problem" (Southwell u.a. 2022, S. 103).

Wissenschaftliche Ergebnisse werden einem breiten, nicht-wissenschaftlichen Publikum oftmals durch Wissenschaftsjournalist:innen vermittelt. Die Aufbereitung wissenschaftlicher Ereignisse unterliegt anderen Mechanismen als die der wissenschaftlichen Publikation selbst (Leßmöllmann

2020). So kann es dabei zu Übertreibungen oder Verfälschungen der wissenschaftlichen Kernaussage kommen, wenn der Kontext geändert oder ein bestimmtes Framing eingesetzt wird (bspw. bei direkter Übernahme von Inhalten aus Pressemitteilungen, Leßmöllmann 2020). Sumner u.a. (2014) haben 462 Pressemitteilungen im Gesundheitsbereich, deren zugrundeliegenden wissenschaftlichen Publikationen sowie die darauf basierenden Nachrichtenartikel untersucht. 40% der Pressemitteilungen verstärkten die Empfehlungen aus den zugrundeliegenden Artikeln und die Wahrscheinlichkeit, dass die Übertreibungen auch in den journalistischen Beiträgen übernommen wurden, war 6,5-mal höher als bei Pressemitteilungen, die ohne Übertreibung auskamen.

Auch die journalistische Aufbereitung von wissenschaftlichen Artikeln kann durch sprachliche Elemente Verwirrungen erzeugen – z. B. durch sog. *Spins* (Boutron u.a. 2019), *Framing*, vermeintliche Kontextualisierungen oder Weglassungen. So kann sich durch die sukzessive Veränderung im Weitergabeprozess, eine Information ebenfalls zu einer Falschinformation entwickeln („Stille Post-Prinzip"). Abb. 2 verdeutlicht diesen Prozess, an dessen Anfang wissenschaftlicher Input in Form von Publikationen, Preprints und journalistische Aufarbeitungen stehen. Im Laufe des Rezeptionsprozesses kann diese Information dann zu wissenschaftlicher Falschinformation werden (Output).

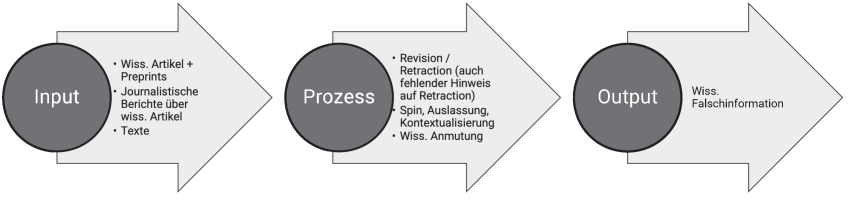

Abb. 2: Veränderung einer wissenschaftlichen Information im Weitergabeprozess und Entstehung von wissenschaftlicher Falschinformation

Pseudoscience und Fake-Wissenschaft

Falschinformation, die einen wissenschaftlichen Anschein hat, jedoch nicht wissenschaftlichen Standards entspricht (siehe Abb. 1, Fall 1), wird häufig als „Pseudowissenschaft" oder auch „Fake-Wissenschaft" (ALLEA 2021; Falyuna 2022; Hopf u.a. 2019) bezeichnet. Es wird ein wissenschaftliches Erscheinungsbild geschaffen, in dem wissenschaftliche Charakteristika nach-

gebildet oder nachgeahmt werden, um die Überzeugungskraft oder Glaubwürdigkeit der Falschinformation zu steigern. ALLEA hat dies in ihrem Diskussionspapier als "Plagiarising the Language of Science" (ALLEA 2021, S. 11) bezeichnet.

Viele Studien untersuchen den Zusammenhang von Wissenschaftlichkeit und Glaubwürdigkeit und zeigen, dass eine starke Korrelation zwischen den beiden Eigenschaften besteht: "Scientificness is mistaken for credibility" (Zaboski/Therriault 2020, S. 833). Genau diesen Zusammenhang macht sich die Pseudowissenschaft zunutze. Zaboski/Therriault (2020) schreiben dazu: "Disguised as genuine science that flaunts an attractive and intuitive appeal, pseudoscience encourages scientific illiteracy and can also provide an unwarranted level of confidence in misinformation" (Zaboski/Therriault 2020, S. 821).

Dass diese Nachahmung von Wissenschaftlichkeit, also Informationen mit wissenschaftlicher Anmutung, effektiv ist, konnte in weiteren Studien gezeigt werden. Tal/Wansink (2014) haben zum Beispiel festgestellt, dass Texte mit Elementen, die mit Wissenschaft in Verbindung gebracht werden, wie Tabellen und Formeln, Menschen von der Wirksamkeit eines Medikaments überzeugen können. Hahn u.a. (2020) konnten zeigen, dass Menschen glauben, dass ein Dokument wissenschaftlich sei, wenn dieses wissenschaftliche Formeln, Diagramme, Tabellen beinhaltet oder ein zweispaltiges Layout aufweist. Der tatsächliche Inhalt war dabei nebensächlich.

Hopf u.a. (2019) sehen *Fake Science* als eine große Bedrohung für die Glaubwürdigkeit der Wissenschaft, die sogar so weit führt, dass Wissenschaft per se als „Fake Science" bezeichnet wird, um Wissenschaft und faktische Daten zu diskreditieren. Hier liegt für Falyuna (2022) der grundlegende Unterschied zwischen Pseudoscience und anti-wissenschaftlichem Glauben. Während Pseudoscience an wissenschaftliche Kriterien glaubt und diese auch nutzt, stellen anti-wissenschaftliche Strömungen die Autorität der Wissenschaft infrage.

3. Projekt DESIVE²: Eine Qualitative Studie zum Gesundheits(falsch)informationsverhalten

Die zugrundeliegenden Mechanismen der Verteilung digitaler (wissenschaftlicher) Falschinformation im Gesundheitsbereich – und damit die Wurzel von Desinformations- bzw. nach unserer Definition Falschinformationskampagnen – sind bisher noch nicht ausreichend untersucht worden,

um ihnen effektiv entgegenwirken zu können. Technisch-basierte Ansätze zur Erkennung und Bekämpfung von Falschinformation stehen vor enormen Herausforderungen. So haben Sharma u.a. (2019) in ihrer Studie die Probleme der technischen Lösungen zusammengefasst und verweisen u.a. darauf, dass die fehlenden Erkenntnisse zu den Mechanismen der Distribution von Falschinformation in einem Mangel an hochwertigen Trainingsdaten begründet ist. Weiterhin ist die Analyse automatisch auswertbarer Datenspuren häufig an einzelne Informationsplattformen (z.B. Twitter) gebunden und dadurch nur siloartig und unvollständig. Gleiches gilt für Studien, die nur eine Verhaltensweise untersuchen (z.B. *retweet*-Verhalten). Aufgrund dessen eignen sich derartige Analysen nicht, um die Ausbreitung und Mechanismen von Falschinformationskampagnen in Gänze zu verstehen, da zahlreiche kontextuelle und individuelle Dimensionen das Informationsverhalten von Menschen beeinflussen oder prägen.

3.1 Zielsetzung

Es bedarf daher einer holistischen Betrachtung von Falschinformationsverhalten, das sich auch in komplexen Prozessen innerhalb digitaler und nicht-digitaler Umgebungen abspielt, um der Verbreitung von Falschinformation vorzubeugen. "Studying and characterizing the relationship between user actions and utilities at the microscopic level of the individual, and the macroscopic impact in different networked environments, will be essential for explaining the spread of fake news" (Sharma u.a. 2019, S. 35).

Dieser Forderung soll im Projekt DESIVE² durch eine qualitative Herangehensweise nachgekommen werden, die es ermöglicht, menschenzentriert den Verlauf von Information und deren Veränderungen in den Blick zu nehmen und somit auch Plattformübergänge zu berücksichtigen, wenn Information, die beispielsweise im nicht-digitalen Bereich aufgegriffen wurde, in der Folge verändert in Sozialen Medien verbreitet wird. Die Impulse, die Menschen dazu motivieren etwas zu teilen, sollen näher analysiert und beschrieben werden. Dazu werden sowohl induktiv individuelle Verhaltensmuster ermittelt, die Rückschlüsse auf Verhaltensweisen im Umgang mit Falschinformation zulassen, als auch deduktiv bekannte Phänomene überprüft, die das Verbreiten von Information beeinflussen.

Basierend auf den im Projekt erhobenen Daten und daraus gewonnen Erkenntnissen wird ein Modell des Falschinformationsverhaltens entwickelt, welches die Verbreitungsmechanismen von wissenschaftlicher Falschinformation beschreibt und verdeutlicht, welche kritischen Ereignis-

se bei der Verbreitung eine Rolle spielen. Es wird eine Charakterisierung wissenschaftlicher Falschinformation im Kontext des Gesundheitsinformationverhaltens angestrebt. Dabei steht im Fokus:

1. die wissenschaftliche Gesundheits(falsch)information, ihr Rezeptions- und Verbreitungsweg sowie die Situation des Empfängers bzw. der Empfängerin, die eine Falschinformation erhält oder weitergibt und
2. die Veränderung des Informationsinhalts einer wissenschaftlichen Gesundheitsinformation durch Framing, Spin oder ähnlicher Vorgänge.

Eine Theorie des Gesundheitsinformationsverhaltens unter Einbezug von Falschinformation ist grundlegend, um Entscheidungsträger:innen und Gesundheitsdienstleistende bei der Gestaltung optimaler Informationsinterventionen unterstützen zu können (Lambert/Loiselle 2007).

3.2 Methodischer Ansatz

Das Forschungsdesign von DESIVE² baut auf drei methodischen Bausteinen auf: Für das Gesamtdesign wird der *Grounded-Theory*-Ansatz verwendet, die Datensammlung greift auf die *Critical Incident Technique* (CIT) zurück und für die Entwicklung eines Modells des Falschinformationsverhaltens wird auf eine vergleichende Analyse existierender Modelle zurückgegriffen, deren Ergebnis mit Erkenntnissen aus dem Projekt abgeglichen wird. Ergänzt wird das so neu entstehende Modell des Falschinformationsverhaltens durch eine Klassifikation wissenschaftlicher Falschinformationen und einen Katalog an kritischen Ereignissen (*critical incidents*), die als Auslöser für die bewusste oder unbewusste Verbreitung von wissenschaftlicher Falschinformation im Gesundheitskontext maßgeblich sind.

Die Methode der kritischen Ereignisse (CIT) (Flanagan 1954) ist eine in verschiedenen Disziplinen eingesetzte qualitative Methode zur Exploration und Erklärung spezifischer Phänomene, die es ermöglicht, relevante Faktoren zu identifizieren, die eine Aktion auslösen (Bartsch/Specht 2009). In Bezug auf die Verbreitung von Gesundheits(falsch)informationen sollen kritische Ereignisse identifiziert werden, die sowohl subjektiv auf der Ebene des Individuums und seiner Handlungen als auch seiner Informationsumgebung auftreten. Von den subjektiven kritischen Ereignissen der untersuchten Personen ausgehend, soll in einem weiteren Schritt, auf die gesellschaftliche Relevanz der Ereignisse extrapoliert werden. In Anlehnung an die in Bartsch/Specht (2009) empfohlene Vorgehensweise, kritische Ereignisse mit konkreten Kriterien zu identifizieren, wird im Kontext des Pro-

jekts DESIVE² ein Ereignis als kritisch definiert, wenn alle der folgenden Gegebenheiten zutreffen:

- Eine Person nimmt Gesundheits(falsch)information bewusst wahr,
- aus der Perspektive dieser Person ist die Gesundheits(falsch)information in einem hohen Maße interessant (im positiven oder negativen Sinne),
- die Person teilt die Gesundheits(falsch)information mit anderen oder entscheidet sich bewusst, sie nicht zu teilen, und
- das Ereignis hat einen Bezug zu Wissenschaftlichkeit (entweder aus Perspektive der Person oder Perspektive der Quelle).

3.3 Datenerhebung

Die im Projekt geplanten Studien sind multimethodisch angelegt und beinhalten die Durchführung qualitativer Leitfadeninterviews, sowie Tagebuchstudien und Umfragen in der Bevölkerung mittels einer eigens dafür programmierten Smartphone-App. Die Erhebung der Daten erfolgt nach den Prinzipien der Grounded Theory, bei welcher durch eine simultane Datenerhebung und -analyse, Daten iterativ erhoben und analysiert werden.

In Abb. 3 wird der Forschungsprozess im Projekt visualisiert, der mit der Rekrutierung von Proband:innen für die Teilstudien (Interviews, Umfrage und Tagebucheinträge in einer Smartphone-App) beginnt. Dem Grounded-Theory-Ansatz folgend wird bei der Rekrutierung von Proband:innen eine theoretisch orientierte Samplingstrategie *(theoretical sampling)* genutzt. Die Größe des Samples ist vorher nicht festgelegt und endet mit der inhaltlichen Sättigung, d.h. wenn durch die Hinzunahme von Fällen keine neuen Erkenntnisse zum Untersuchungsgegenstand ergänzt werden können (Glaser/Strauss 1967). Die Rekrutierung von Proband:innen ist entscheidend für die spätere Zusammensetzung des Panels, was die Notwendigkeit regelmäßiger iterativer Reflexionsschleifen zur Folge hat. Eine strategische Vorgehensweise bei der Rekrutierung ist hier notwendig, um eine Diversifizierung des Samples in Bezug auf sozioökonomische Parameter zu erreichen.

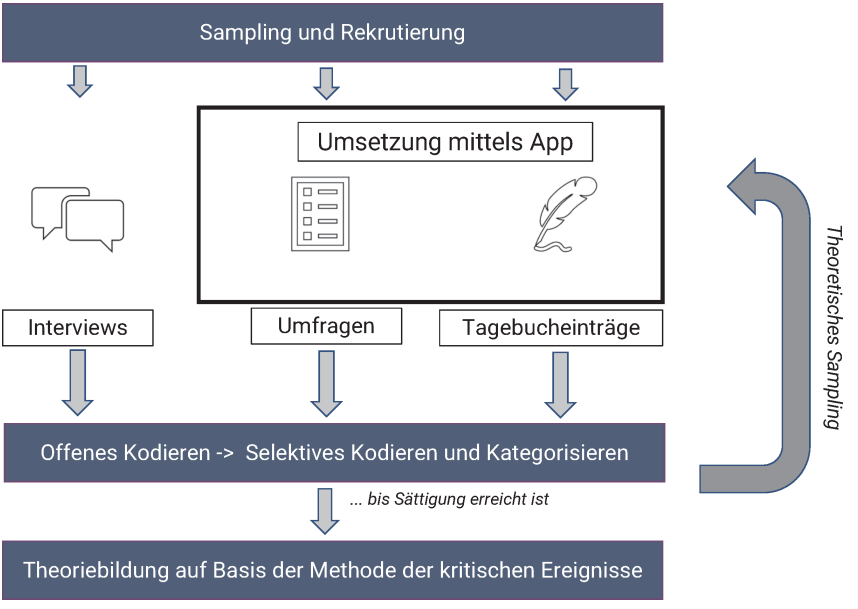

Abb. 3: Forschungsprozess im Projekt DESIVE²

Durch semi-strukturierte Interviews werden Erfahrungen von Proband:innen im Kontext ihrer Interaktionen mit Gesundheits(falsch)informationen erhoben. Dafür werden drei Themenkomplexe innerhalb des Interviewleitfadens einbezogen: 1) die persönliche Gesundheitsinformationsinfrastruktur, die sowohl Informationsquellen und Informationsbedarfe abdeckt, 2) das (Falsch)Informationsverhalten, das jegliche Interaktion mit Gesundheitsinformation, ob aktiv, passiv und/oder vermeidend umfasst; sowie 3) die Wahrnehmung von Wissenschaft als auch von Informationsquellen in Bezug auf ihre Wissenschaftlichkeit im Kontext von Gesundheitsthemen. Die Ergebnisse der Interviews sollen dann auch bei der Datenerhebung in der Smartphone-App berücksichtigt werden.

Die in DESIVE² entwickelte App ermöglicht Proband:innen die Übermittlung von Sprachnotizen, Screenshots und anderen Dateien, sowie die Teilnahme an Umfragen. Gesammelt werden Gesundheits(falsch)informationen oder Nachweise von Gesundheits(falsch)informationen, die 1) die Proband:innen an andere Personen weitergegeben haben oder 2) die Proband:innen selbst über das Smartphone erhalten haben, bzw. die ihnen auf anderem Wege mitgeteilt wurden. Abb. 4 verdeutlicht diese beiden Si-

tuationen, zu denen in der App anhand von Tagebucheinträgen Informationen überliefert werden können. Die dunkel dargestellte Figur symbolisiert eine:n Nutzer:in der App, der:die in Ereignis (1) Gesundheits(falsch)information weitergibt oder in Ereignis (2) diese erhält und mit dem Projekt teilt. Die Proband:innen haben die Möglichkeit, die Situationen in der App ausführlich zu beschreiben und strukturierte Fragen zu diesen zu beantworten. Ergänzt werden diese situativ gesammelten Informationen durch Umfragen, die die Proband:innen über eine zweimonatige Nutzungsphase hinweg in der Smartphone-App beantworten.

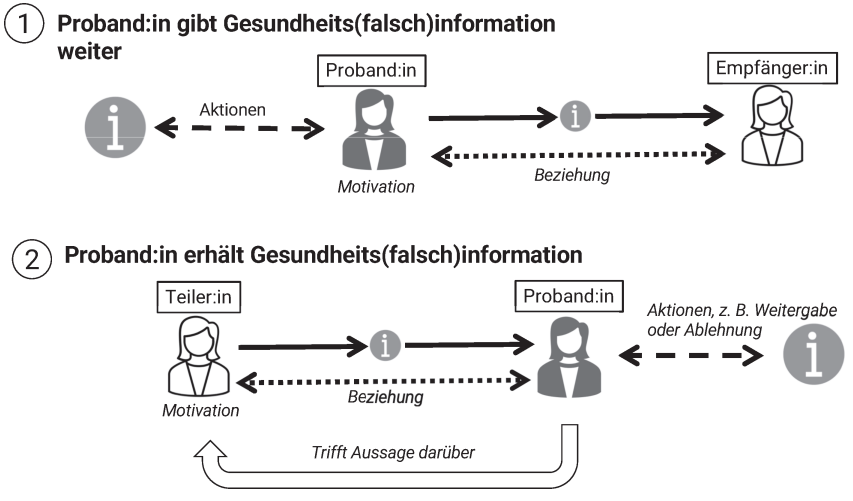

Abb. 4: Darstellung der situativ gesammelten Ereignisse, die Personen in der App hinterlassen können.

Die Datensammlung mittels Smartphone-App und Interviews erfolgt in zwei Runden und Erkenntnisse aus der Auswertung der ersten Datenerhebungsrunde fließen in die weitere Konzeption der Umfragen, Tagebucheinträge und weiterer Interviews ein. Ziel ist es, anhand der Ergebnisse aus den Interviews, Tagebucheinträgen und Umfragen kritische Ereignisse und daraus folgend Phänomene des Falschinformationsverhaltens zu identifizieren, die dann in ein Modell des Falschinformationsverhaltens überführt werden. Auch werden verschiedene Arten wissenschaftlicher Gesundheits(falsch)information im Kontext der Informationsverhaltensforschung näher beleuchtet und finden in dem zu entwickelnden Modell Berücksichtigung.

4. Zusammenfassung und Ausblick

Allgemeiner Sprachgebrauch und wissenschaftlicher Diskurs unterscheiden sich in der Verwendung von „Desinformation", „Misinformation" und „Falschinformation", sind sich aber darin einig, dass diese Informationstypen erhebliche Auswirkungen auf die Gesellschaft haben, ihr letztlich massiv schaden können. Dies ist insbesondere im Kontext von Gesundheitsinformation der Fall, wie sich aktuell in der COVID-19-Pandemie auch gezeigt hat (World Health Organization, 2020). Eine besondere Relevanz kommt dabei wissenschaftlicher Falschinformation zu, da sie besonders glaub- und vertrauenswürdig erscheint (Hahn u.a. 2020) und daher ein hohes Risiko für eine weite Verbreitung birgt. Forschung zur Typisierung von wissenschaftlicher Falschinformation sowie ihrer Entstehung und Veränderung im Laufe des Verbreitungsprozesses liegt in den Anfängen. Bislang konnten die folgenden unterschiedlichen Formen wissenschaftlicher Falschinformation identifiziert werden (siehe auch Abb. 1), wobei sie zukünftig einer eingehenderen Analyse bedürfen:

1) Information, die ursprünglich wissenschaftliche Kriterien erfüllt hat, aber als überholt gilt,
2) Information, die von Wissenschaftler:innen bewusst oder aufgrund von unbeabsichtigten Fehlern produziert wird,
3) Information, die wissenschaftlich anmutet, jedoch keine (allgemein anerkannte) wissenschaftliche Grundlage hat (Pseudoscience), und
4) Information, die zwar wissenschaftliche Kriterien erfüllt, jedoch auf ihrem Rezeptionsweg verzerrt oder verfälscht wiedergegeben wird.

Weiterhin ist unklar, welche Rolle wissenschaftliche Falschinformation in Des- und Falschinformationskampagnen spielt und inwiefern gerade die „Wissenschaftlichkeit" der Information zum Treiber ihrer Verbreitung wird. Das Projekt DESIVE² nimmt sich diesen Fragen an und führt eine umfassende Grounded-Theory-Studie zum Gesundheits(falsch)informationsverhalten von Bürger:innen durch. Verbunden wird dies mit einer Untersuchung kritischer Ereignisse, die zur Informationsverbreitung führen, um sowohl die Ebene des Individuums und seiner Handlungen als auch die Informationsumgebung plattformunabhängig zu betrachten. Der zentrale Untersuchungsgegenstand von DESIVE² ist das menschliche Verhalten in der Interaktion mit wissenschaftlicher Falschinformation im Gesundheitsbereich.

Es hat sich allerdings bereits gezeigt: Um Gesundheitsinformation als falsch zu entlarven, bedarf es großer Anstrengungen. Die Prüfung auf Korrektheit kann lediglich nach festgelegten Methoden und klaren Kriterien geschehen (Schaefer/Bitzer 2021), ein Unterfangen, welches die breite Öffentlichkeit kaum leisten kann. Ein Teil der Lösung können Investitionen in die Wissenschaftskompetenz der Bevölkerung sein.

Es ist wichtig, die Öffentlichkeit über die Funktionsweisen in der Wissenschaft zu unterrichten und klarzumachen, dass wissenschaftliche Ergebnisse stets mit Unsicherheit behaftet sind und sich ändern können (Schaefer/Bitzer 2021, S. 3). Denn das fehlende Verständnis großer Teile der Bevölkerung über wissenschaftliche Praktiken ist auch ein Grund dafür, warum wissenschaftliche Falschinformation sich überhaupt verbreiten kann. So wird der Einfluss der Wissenschaft oder auch der Ergebnisse einzelner Studien häufig zu hoch eingeschätzt (Howell/Brossard 2021) und es ist nicht klar, dass es für einen Konsensus in der Wissenschaft viele Jahre und Studien braucht. Das Wissen um diese Mechanismen, die zu wissenschaftlichen Erkenntnissen führen, wird als Wissenschaftskompetenz oder *Science Literacy* bezeichnet (Liu 2009). Wissenschaftskompetenz befähigt dazu, wissenschaftliche Arbeiten zu verstehen und sich mithilfe des wissenschaftlichen Diskurses eine Meinung über Themen bilden zu können, die einen Einfluss auf das Leben und die Gesellschaft haben – eine Fähigkeit, der in einer Demokratie besondere Bedeutung zukommt (National Research Council u.a. 2007).

Danksagung

Diese Publikation wird durch die Förderung des Bundesministeriums für Bildung und Forschung für das DESIVE²-Projekt unterstützt.

Literatur

Alle Online Quellen zuletzt abgerufen am 19.05.2023

Agarwal, N. K., und Alsaeedi, F. (2021): Creation, dissemination and mitigation: Toward a disinformation behavior framework and model. *Aslib Journal of Information Management*, *73*(5), S. 639–658. https://doi.org/10.1108/AJIM-01-2021-0034

ALLEA (2021): Fact or Fake? Tackling Science Disinformation. ALLEA Discussion Paper, 5. https://doi.org/10.26356/fact-or-fake

Bar-Ilan, J., & Halevi, G. (2018): Temporal characteristics of retracted articles. *Scientometrics*, 116(3), S. 1771-1783. https://doi.org/10.1007/s11192-018-2802-y

Bartsch, S., und Specht, N. (2009): Die Critical Incident Technique (CIT). In: *Theorien und Methoden der Betriebswirtschaft: Handbuch für Wissenschaftler und Studierende*. ORT: Vahlen, S. 377–400.

Bates, M. J. (2017): Information Behavior. In: J. D. McDonald und M. Levine-Clark (Hrsg.), Encyclopedia of Library and Information Science. 4. Aufl. ORT: CRC Press., S. 2074-2085.

Baumann, E., Czerwinski, F., Rosset, M., Seelig, M., und Suhr, R. (2020): Wie informieren sich die Menschen in Deutschland zum Thema Gesundheit? Erkenntnisse aus der ersten Welle von HINTS Germany. *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz*, *63*(9), S. 1151–1160. https://doi.org/10.1007/s00103-020-03192-x

Boutron, I., Haneef, R., Yavchitz, A., Baron, G., Novack, J., Oransky, I., Schwitzer, G., & Ravaud, P. (2019). Three randomized controlled trials evaluating the impact of "spin" in health news stories reporting studies of pharmacologic treatments on patients'/caregivers' interpretation of treatment benefit. *BMC Med*, *17, 105.* https://doi.org/10.1186/s12916-019-1330-9

Büchter, R. B., & Albrecht, M. (2021). Evidenzbasierte Gesundheitsinformationen in der Prävention und Gesundheitsförderung. In M. Tiemann & M. Mohokum (Hrsg.), *Prävention und Gesundheitsförderung* (S. 295–303). Springer. https://doi.org/10.1007/978-3-662-62426-5_17

Dahlstrom, M. F. (2021). The narrative truth about scientific misinformation. *Proceedings of the National Academy of Sciences*, *118*(15). https://doi.org/10.1073/pnas.1914085117

Baines, D., & Elliott, R. J R . (2020). *Defining misinformation, disinformation and malinformation: An urgent need for clarity during the COVID-19 infodemic* (Discussion Papers 20–06). Department of Economics, University of Birmingham. https://ideas.repec.org/p/bir/birmec/20-06.html

De Gani, S. M., Berger, F. M. P., Guggiari, E., & Jaks, R. (2022). Relation of corona-specific health literacy to use of and trust in information sources during the COVID-19 pandemic. *BMC Public Health*, *22*(1). https://doi.org/10.1186/s12889-021-12271-w

Dewitz, L. (2022). Positioning digital well-being in health information behaviour. In Proceedings of ISIC: the information behaviour conference, Berlin, Germany, 26-29 September, 2022. Information Research, 27(Special issue), isic2224. https://doi.org/10.47989/irisic2224

Fallis, D. (2015). What Is Disinformation? *Library Trends*, *63*(3), 401–426. https://doi.org/10.1353/lib.2015.0014

Falyuna, N. (2022). Science disinformation as a security threat and the role of science communication in the disinformation society. *Scientia et Securitas*, *3*(1), 69–78. https://doi.org/10.1556/112.2022.00086

Flanagan, J. C. (1954). The critical incident technique. *Psychological Bulletin*, *51*(4), 327–358. https://doi.org/10.1037/h0061470

Glaser, B. G., & Strauss, A. L. (1967). *The discovery of grounded theory: Strategies for qualitative research.* (2009. Aufl.). Aldine.

Godbold, N. (2006). Beyond information seeking: Towards a general model of information behaviour. *Information Research: An International Electronic Journal*, *11*(4).

Greifeneder, E. & Schlebbe, K. (2023). "D 1 Information Behaviour". Grundlagen der Informationswissenschaft, edited by Rainer Kuhlen, Dirk Lewandowski, Wolfgang Semar and Christa Womser-Hacker, Berlin, Boston: De Gruyter Saur, 497–510. https://doi.org/10.1515/9783110769043-043

Hahn, O., Lemke, S., Mazarakis, A., & Peters, I. (2020). Which visual elements make texts appear scientific? An empirical analysis. *Proceedings of the Conference on Mensch und Computer*, 61–65. https://doi.org/10.1145/3404983.3410014

Hopf, H., Krief, A., Mehta, G., & Matlin, S. A. (2019). Fake science and the knowledge crisis: Ignorance can be fatal. *Royal Society Open Science*, *6:190161*. https://doi.org/10.1098/rsos.190161

Howell, E. L., & Brossard, D. (2021). (Mis)informed about what? What it means to be a science-literate citizen in a digital world. *Proceedings of the National Academy of Sciences*, *118*(15). https://doi.org/10.1073/pnas.1912436117

Islam, M. S., Sarkar, T., Khan, S. H., Mostofa Kamal, A.-H., Hasan, S. M. M., Kabir, A., Yeasmin, D., Islam, M. A., Amin Chowdhury, K. I., Anwar, K. S., Chughtai, A. A., & Seale, H. (2020). COVID-19–Related Infodemic and Its Impact on Public Health: A Global Social Media Analysis. In *The American Journal of Tropical Medicine and Hygiene*. The American Society of Tropical Medicine and Hygiene, 103(4), 1621–1629. https://doi.org/10.4269/ajtmh.20-0812

Karlova, N. A., & Fisher, K. E. (2013). *A social diffusion model of misinformation and disinformation for understanding human information behaviour. Information Research*, 18(1) paper 573. http://informationr.net/ir/18-1/paper573.html

Kelly, S., Eldredge, S. A., Dalton, E. D., & Miller, L. E. (2014). Health-Information Behavior: An Initial Validity Portfolio for Active and Passive Measures. *Communication Research Reports*, *31*(2), 171–182. https://doi.org/10.1080/08824096.2014.907145

Lambert, S. D., & Loiselle, C. G. (2007). Health Information—Seeking Behavior. *Qualitative Health Research*, *17*(8), 1006–1019. https://doi.org/10.1177/1049732307305199

Leßmöllmann, A. (2020). Wissenschaft in den Nachrichten: Quadratur des Kreises? In *Fake News, Framing, Fact-Checking: Nachrichten im digitalen Zeitalter* (151–174). transcript Verlag. https://doi.org/10.1515/9783839450253-009

Lewandowsky, S., Ecker, U. K. H., Seifert, C. M., Schwarz, N., & Cook, J. (2012). Misinformation and Its Correction: Continued Influence and Successful Debiasing. *Psychological Science in the Public Interest*, *13*(3), 106–131. https://doi.org/10.1177/1529100612451018

Liu, X. (2009). Beyond science literacy: Science and the public. *International Journal of Environmental and Science Education*, *4*(3), 301–311.

Loomba, S., de Figueiredo, A., Piatek, S. J., de Graaf, K., & Larson, H. J. (2021). Measuring the impact of COVID-19 vaccine misinformation on vaccination intent in the UK and USA. *Nature Human Behaviour*, *5*(3), 337–348. https://doi.org/10.1038/s41562-021-01056-1

National Research Council, Division of Behavioral and Social Sciences and Education, Board on Science Education, Center for Education, Committee on Science Learning, Duschl, R. A., Schweingruber, H. A., & Shouse, A. W. (2007). *Taking Science to School*. National Academies Press. https://doi.org/10.17226/11625

Schaefer, C., & Bitzer, E.-M. (2021). *Umgang mit Fehl- und Desinformation in Medien*. Kompetenznetz Public Health COVID-19. https://www.public-health-covid19.de/images/2021/Ergebnisse/20210902_Hintergrund_Fehlinformation_update.pdf

Schaeffer, D., Berens, E.-M., Gille, S., Griese, L., Klinger, J., de Sombre, S., Vogt, D., & Hurrelmann, K. (2021). *Gesundheitskompetenz der Bevölkerung in Deutschland vor und während der Corona Pandemie: Ergebnisse des HLS-GER 2*. https://pub.uni-bielefeld.de/record/2950305

Sharma, K., Qian, F., Jiang, H., Ruchansky, N., Zhang, M., & Liu, Y. (2019). Combating fake news: A survey on identification and mitigation techniques. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *10*(3), 1–42. https://doi.org/10.1145/3305260

Soroya, S. H., Farooq, A., Mahmood, K., Isoaho, J., & Zara, S. (2021). From information seeking to information avoidance: Understanding the health information behavior during a global health crisis. *Information Processing & Management*, *58(2), 102440.* https://doi.org/10.1016/j.ipm.2020.102440

Southwell, B. G., Brennen, J. S. B., Paquin, R., Boudewyns, V., & Zeng, J. (2022). Defining and Measuring Scientific Misinformation. *The ANNALS of the American Academy of Political and Social Science*, *700*(1), 98–111. https://doi.org/10.1177/00027162221084709

Sumner, P., Vivian-Griffiths, S., Boivin, J., Williams, A., Venetis, C. A., Davies, A., Ogden, J., Whelan, L., Hughes, B., Dalton, B., Boy, F., & Chambers, C. D. (2014). The association between exaggeration in health-related science news and academic press releases: Retrospective observational study. *BMJ*, *349*, *g7015*. https://doi.org/10.1136/bmj.g7015

Tal, A., & Wansink, B. (2014). Blinded with science: Trivial graphs and formulas increase ad persuasiveness and belief in product efficacy. *Public Understanding of Science*, *25*(1), 117–125. https://doi.org/10.1177/0963662514549688

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking.* (Nr. 09). Council of Europe Strasbourg. https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

West, J. D., & Bergstrom, C. T. (2021). Misinformation in and about science. *Proceedings of the National Academy of Sciences*, *118*(15). https://doi.org/10.1073/pnas.1912444117

Wilson, T. D. (2000). Human information behavior. *Informing Science*, *32*, 49–56.

Wilson, T. D. (2022). *Exploring information behaviour: An introduction*. Published by the author. http://informationr.net/ir/Exploring%20information%20behaviour.pdf

World Health Organization (Hrsg.). (2020). *Novel Coronavirus(2019-nCoV) Situation Report—13*. WHO. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf

Wray, K. B., & Andersen, L. E. (2018). Retractions in Science. *Scientometrics*, *117*, 2009–2019. https://doi.org/10.1007/s11192-018-2922-4

Zaboski, B. A., & Therriault, D. J. (2020). Faking science: Scientificness, credibility, and belief in pseudoscience. *Educational Psychology*, *40*(7), 820–837. https://doi.org/10.1080/01443410.2019.1694646

Desinformationserkennung anhand von Netzwerkanalysen – ein Instrument zur Durchsetzung der Pflichten des DSA am Beispiel von Telegram

Tahireh Panahi, Gerrit Hornung, Karla Schäfer, Jeong-Eun Choi, Martin Steinebach und Inna Vogel

Zusammenfassung

Desinformationen werden verstärkt zu Krisenzeiten wie z. B. während der Covid-19 Pandemie oder dem Angriffskrieg auf die Ukraine erstellt und verbreitet. Propagandistische Akteure aus dem Ausland, aber auch z. B. extremistische Gruppen im Inland verwenden für ihre Desinformationskampagnen soziale Medien. Telegram stellt einen fast unmoderierten Kommunikationsdienst dar, der die Möglichkeit der nahezu ungestörten Verbreitung von Desinformationen ermöglicht. Unter anderem, um der Verbreitung von falschen und irreführenden Tatsachenbehauptungen entgegenzutreten, wurde von der EU der Digital Services Act (DSA) erlassen. Für die Erfüllung der darin angeordneten risikobezogenen Pflichten wird in diesem Beitrag das Instrument der Netzwerkanalyse vorgeschlagen und anhand des Hybrid-Mediums Telegram näher erklärt. Desinformationen können durch eine Netzwerkanalyse zwar auf inhaltlicher Ebene nicht direkt erkannt werden; in einem nutzerstarken Dienst wie Telegram ist es ist aber möglich, die Verbindungen zwischen Akteuren zu ermitteln und zu charakterisieren. Die Netzwerkanalyse kann daher als ein erstes Tool zur Desinformationserkennung im Rahmen der risikobezogenen Pflichten des DSA eingesetzt werden, verursacht aber auch rechtliche und technische Herausforderungen bei der Umsetzung.[1]

1 Dieser Beitrag ist im Rahmen des BMBF-Verbundprojekts „DYNAMO – Dynamiken der Desinformation erkennen und bekämpfen" (FKZ: 16KIS1498) entstanden.

1. Einleitung

Desinformation ist ein wachsendes Problem in der heutigen Online-Welt, das darin besteht, dass falsche oder irreführende Informationen gezielt verbreitet werden, um eine bestimmte, typischerweise illegitime Agenda zu unterstützen. Besonders der Dienst Telegram steht für die Duldung massenhafter Desinformation in der Kritik. Um Desinformation entgegenzutreten, hat die EU mit dem DSA[2] neue Vorschriften erlassen. Insbesondere die für sehr große Online-Plattformen geltenden risikobezogenen Pflichten können einen Beitrag zur langfristigen Erkennung und Bekämpfung von Desinformation leisten.

Eine offene Frage ist bislang jedoch, wie die in diesem Rahmen geforderten Risikobewertungen technisch umgesetzt werden können. Ein Instrument, das hierzu verwendet werden kann, ist die Netzwerkanalyse. Durch diese werden Interaktionen in Online-Plattformen analysiert, sodass Muster erkannt werden können, die auf eine Desinformationskampagne hindeuten. Die Netzwerkanalyse ermöglicht es damit, die Verbreitung von Desinformation besser zu verstehen und ihr entgegenzuwirken. In diesem Beitrag werden die risikobezogenen Pflichten des DSA der technischen Umsetzung durch die Netzwerkanalyse gegenübergestellt. Abschließend werden rechtliche und technische Probleme diskutiert. Zur Konkretisierung und Veranschaulichung wird das Beispiel des Dienstes Telegram herangezogen.

2. Telegram

Der Dienst Telegram ist in den letzten Jahren durch die Duldung massenhafter Desinformation negativ aufgefallen.[3] Die Betreiber verfolgen einen sehr weitgehenden „Free-Speech"-Ansatz[4], bei dem Sperrungen, Löschun-

2 Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG.

3 *Borscher/Woltert*, Monitor Medienpolitik – Ort der Meinungsfreiheit und Verschwörungsplattform, 2022; *Jünger/Gärtner*, Die Verbreitung und Vernetzung problembehafteter Inhalte auf Telegram, 2021; zum Aufstieg Telegrams: *Denga*, EuR 2021, 569 (574).

4 Die Redefreiheit ist hier im Sinne eines Free-Speech-Absolutism gemeint. Dieses Verständnis einer schrankenlosen Redefreiheit ist nicht gleichbedeutend mit der Meinungsfreiheit nach Art. 5 Abs. 1 GG bzw. Art. 11 GRCh.

gen und andere Moderationsmaßnahmen nur in seltenen Ausnahmefällen durchgeführt werden.[5] Verschiedene Länder, so auch die Bundesrepublik Deutschland, versuchten in jüngerer Zeit durchzusetzen, dass der Dienst aktiver gegen Desinformation vorgeht.[6] Dies hatte zumindest teilweise Erfolg; Telegram hat seine Bereitschaft zur Kooperation mit staatlichen Behörden in bestimmten Konstellationen angepasst.[7]

Bei Telegram handelt es sich um ein sog. Hybrid-Medium, da der Dienst neben rein interpersonaler Kommunikation auch Austausch in öffentlichen Gruppen und Kanälen anbietet.[8] Gruppen können dabei eine Größe von bis zu 200.000 Mitgliedern[9] annehmen; Kanäle sind unbegrenzt in ihrer Abonnentenzahl. Während in Gruppen jedes Mitglied Nachrichten veröffentlichen kann, ist dies in Kanälen grundsätzlich den Administratoren vorbehalten; Nutzer benötigen hierzu die Genehmigung des Administrators. Ein Kanal ist daher zur einseitigen Informationsverbreitung bzw. reinen Konsumierung von Informationen gedacht.

3. Der Digital Services Act

Mit dem DSA erfolgt eine vollständige Harmonisierung der Vorschriften für Vermittlungsdienste innerhalb des EU-Binnenmarkts (vgl. ErwG 9 S. 1). Als Vermittlungsdienste gelten gem. Art. 3 lit. g DSA Dienste zur reinen Durchleitung, Caching-Dienste und Hosting-Dienste. Als Verordnung i. S. d. Art. 288 Abs. 2 AEUV gilt der DSA unmittelbar in allen Mitgliedsstaaten der EU. Der Geltungsbeginn ist in Artt. 92 f. DSA innerhalb abgestufter Fristen vorgesehen.

Ziel der Verordnung ist ein sicheres, vertrauenswürdiges Online-Umfeld zu gewährleisten, das unter anderem den gesellschaftlichen Risiken durch Desinformation entgegenwirken soll (vgl. ErwG 9 DSA). Bemerkenswerterweise wird Desinformation weder im DSA, noch in sonstigen EU-Rechtsakten definiert. Stattdessen können lediglich rechtlich nicht bindende Stellungnahmen der EU herangezogen werden. Diese definieren Desinformati-

5 Vgl. *Telegram.org*, FAQ.
6 *Zeit.de*, Brasiliens oberstes Gericht nimmt Telegram-Sperrung zurück.
7 *Balser,* Telegram sperrt 64 Kanäle.
8 *Jünger/Gärtner*, Datenanalyse von Rechtsverstoßenden Inhalten in Gruppen und Kanälen von Messengerdiensten am Beispiel Telegram, 2020.
9 Vgl. *Telegram.org*, FAQ.

on als nachweislich falsche oder irreführende Informationen , die mit dem Ziel des wirtschaftlichen Gewinns oder der vorsätzlichen Täuschung der Öffentlichkeit konzipiert, vorgelegt und verbreitet werden und öffentlichen Schaden anrichten können.[10]

Vermittlungsdiensten wird in Kapitel 3 des DSA eine breite Palette unterschiedlicher Sorgfaltspflichten auferlegt, die zum Teil auch Desinformation adressieren. Gerade der risikobasierte Ansatz der Regelungen aus Kapitel 3 Abschnitt 5 DSA erfordert den Einsatz passender technischer Analyse-Instrumente, wie die in diesem Beitrag erläuterte Netzwerkanalyse.

3.1 Anwendungsbereich

Zunächst ist darzustellen, unter welchen Bedingungen Dienste wie Telegram in den Anwendungsbereich des DSA fallen. Dieser ist gem. Art. 2 Abs. 1, Art. 3 lit. g DSA für Vermittlungsdienste eröffnet (s.o.). Telegram und ähnliche Dienste sind i. d. R. jedenfalls als Hosting-Dienste zu qualifizieren, da sie gem. Art. 3 lit. g iii) DSA Informationen im Auftrag der Nutzer speichern.

Zu beachten ist, dass es sich bei Telegram um ein sog. Hybrid-Medium handelt, das interpersonale Kommunikation, Austausch in Gruppen und öffentliche Kanäle anbietet (s.o.). Die Teile von Telegram, die die gespeicherten Informationen gem. Art. 3 lit. k DSA öffentlich verbreiten, also für eine potenziell unbegrenzte Zahl von Dritten bereitstellen, können als Online-Plattformen i. S. d. Art. 3 lit. i DSA gelten (dies ist eine Untergruppe der Hosting-Dienste). Auch Gruppen, die durch einen öffentlich geposteten Einladungslink erweitert werden, stellen gem. ErwG 14 öffentliche Kommunikation dar, da die Nutzer, die auf die Informationen zugreifen möchten, automatisch registriert oder aufgenommen werden.[11] Funktionen, die „Instant-Messaging-Dienste" darstellen, können hingegen gem. ErwG

10 *Europäische Kommission*, Mitteilung zur Bekämpfung von Desinformation im Internet (COM(2018) 236 final); *Europäische Kommission*, Aktionsplan gegen Desinformation (JOIN(2018) 36 final).

11 An der Vorschrift des DSA kritisch zu betrachten ist jedoch, dass besonders mitgliederstarke geschlossene Gruppen mangels Verbreitung an eine potenziell unbegrenzte Zahl Dritter keine Online-Plattformen darstellen können (bei Telegram bis zu 200.000 Mitglieder möglich), vgl. *Setz*, in: Bernzen u.a. (Hrsg.), Immaterialgüter und Medien im Binnenmarkt Europäisierung des Rechts und ihre Grenzen, 2022, 175 (188 f.).

14 sogar ausdrücklich keine Online-Plattformen sein.[12] Eine solche funktionsbasierte Einordnung der Dienste in den Anwendungsbereich ist gem. ErwG 13-15 DSA vorgesehen.[13]

Wenn Online-Plattformen eine durchschnittliche aktive Nutzerzahl von monatlich mindestens 45 Millionen in der Union aufweisen, können sie gem. Art. 33 Abs. 1, 4 DSA von der EU-Kommission als „sehr große Online-Plattform"[14] benannt und damit den in diesem Beitrag relevanten Risikobewertungspflichten unterworfen werden.[15] Online-Plattformen (mit Ausnahme von Mikro- und Kleinunternehmen) waren und sind gem. Art. 24 Abs. 2 DSA dazu verpflichtet, bis zum 17. Februar 2023 – danach mindestens alle sechs Monate – Informationen über die durchschnittliche monatliche Zahl ihrer aktiven Nutzer in der Union zu veröffentlichen.[16] Nach eigenen Angaben erreichte Telegram den Schwellenwert von 45 Millionen aktiven Nutzern in der EU zum Stichtag am 17. Februar 2023 nicht, sondern schätzt seine durchschnittliche Nutzerzahl auf 38 Millionen.[17] Telegram macht zudem darauf aufmerksam, dass die Zahl tatsächlich noch niedriger sein könnte, da nur einige der Funktionen als Online-Plattformen i. S. d. DSA eingestuft werden könnten (s.o.).[18]

Der Koordinator für digitale Dienste[19] und die EU-Kommission können nun gem. Art. 24 Abs. 3 DSA zusätzliche Informationen über die in jenem

12 Dazu auch: *Gielen/Uphues*, EuZW 2021, 627 (634); *Kuhlmann/Trute*, GSZ 2022, 115 (115).

13 Anders als bei vergleichbaren deutschen Regelwerken, ist der Anwendungsbereich des DSA auch für hybride Dienste wie Telegram eröffnet. Während etwa bei NetzDG und MStV der Anwendungsbereich aufgrund starrer Legaldefinitionen von Dienste-Typen nicht ohne weiteres für diese doppelfunktionalen Dienste eröffnet ist, sieht der DSA in ErwG 12 ff. ausdrücklich eine funktionsbasierte Einordnung der Dienste in den Anwendungsbereich vor, vgl. *Setz*, in: Bernzen u.a. (Hrsg.), Immaterialgüter und Medien im Binnenmarkt. Europäisierung des Rechts und ihre Grenzen, 2022, 175 (189); so auch: *Gielen/Uphues*, EuZW 2021, 627 (635); *Eisenreich*, RDi 2021, 289 (289 f.); *Kalbhenn*, ZUM 2022, 266 (272); zur Einordnung von Gruppen: *Spindler*, GRUR 2021, 653 (654).

14 Gebräuchlich ist auch die Abkürzung des englischen Begriffs „VLOP" („Very large Online-Plattform"); s. dazu auch *Kuß/Lehmann*, DB 2021, 605 (607).

15 Die genaueren Modalitäten der Berechnung werden in ErwG 76 f. DSA beschrieben.

16 *Europäische Kommission*, Presseerklärung vom 17.02.23.

17 *Telegram.org*, FAQ.

18 *Telegram.org*, FAQ.

19 Gem. Art. 49 Abs. 3 DSA haben die Mitgliedstaaten bis zum 17.2.2024 jeweils eine Behörde als Koordinator für digitale Dienste zu benennen. Die Behörden müssen die Anforderungen des Art. 50 DSA erfüllen (unter anderem Unabhängigkeit, Unparteilichkeit, Transparenz).

Absatz genannte Berechnung sowie Erläuterungen und Begründungen in Bezug auf die verwendeten Daten verlangen. Zu prüfen wäre dabei, ob Telegram bei dieser Schätzung bereits die eher „großzügigen" Berechnungsvorgaben des ErwG 77 DSA angewendet hat. Danach gelten bereits alle diejenigen als aktive Nutzer, die den Dienst in dem bestimmten Zeitraum mindestens einmal in Anspruch nehmen, z. B. indem sie Informationen bereitstellen oder diesen auch nur ausgesetzt sind, wobei eine Registrierung beim Dienst nicht erforderlich ist und auch eine einmalige Nutzung ausreicht. Zu berücksichtigen sind nach ErwG 77 alle Online-Schnittstellen wie Websites oder Anwendungen. Nutzer müssen zwar nicht aktiv mit der Information interagieren. Eine nur gelegentliche indirekte Nutzung des Dienstes durch Nutzer anderer Anbieter von Vermittlungsdiensten reicht jedoch nicht aus.

Gem. Art. 24 Abs. 3 DSA dürfen bei der Übermittlung zusätzlicher Informationen an die genannten Behörden keine personenbezogenen Daten enthalten sein. Dies ist bei einem Hybrid-Medium (s.o.) wie Telegram problematisch, da der Anbieter berechnen muss, wie viele Nutzer die Funktionen, die als Online-Plattform gelten, nutzen, und welche nur die Messenger-Funktionen, die nicht unter den Anwendungsbereich des DSA fallen (s.o.).[20] Bei einer solch nutzer-spezifischen Unterscheidung fallen regelmäßig personenbezogene Daten an; z.B. kann eine Gruppen- oder Kanalzugehörigkeit Daten über weltanschauliche und politische Einstellungen enthalten. Inwiefern die Daten in anonymisierter oder pseudonymisierter Form übermittelt werden können, ohne die Aussagekraft der Berechnung zu gefährden, bleibt fraglich.

Schließlich ist festzuhalten, dass selbst wenn Telegram aktuell die Schwelle noch nicht erreicht, eine Neuberechnung alle sechs Monate zu erfolgen hat und zumindest damit gerechnet werden muss, dass die Zahlen mittelfristig ansteigen. Selbst wenn dies nicht der Fall sein sollte, könnte die im Folgenden erläuterte Netzwerkanalyse für den Anbieter sinnvoll und nützlich sein, z. B. für freiwillige desinformationsbezogene Untersuchungen oder zu Forschungszwecken.

20 *Jung*, DÖV 2023, 141 (147).

3.2 Risikobezogene Pflichten

Der DSA enthält unterschiedliche Pflichten, die sich zum Teil repressiv oder präventiv gegen die Verbreitung von Desinformation richten.[21] Zu nennen sind etwa Vorgaben zur Gestaltung und Durchführung von AGB (Art. 14 DSA), Transparenzpflichten (vgl. Artt. 15, 24, 38, 39, 42 DSA), Melde- und Abhilfeverfahren (Art. 16 ff. DSA) und die Deplatforming-Pflicht (Art. 21 Abs. 1 DSA).[22] Neu für das Recht der Vermittlungsdienste sind eine Reihe risikobezogener Pflichten aus Artt. 34 ff. DSA, die indes nur für „sehr große Online-Plattformen" (s.o.) gelten.[23] Die weiteren Ausführungen beschränken sich auf diese risikobezogenen Pflichten, da die in diesem Beitrag vorgestellte Netzwerkanalyse vor allem als Instrument zu ihrer technischen Umsetzung eingesetzt werden kann.

Risikobasierter Ansatz

Der zu Grunde liegende risikobasierte Ansatz wird in ErwG 75f. beschrieben.[24] Danach kommt sehr großen Online-Plattformen auf Grund ihrer Reichweite eine bedeutende Rolle z. B. für die öffentliche Debatte zu, was gesellschaftliche Risiken bewirken kann. Gem. ErwG 79 sind auch die Art und Weise, in der solche sehr großen Online-Plattformen genutzt werden können, unter anderem für die Online-Sicherheit, die öffentliche Meinungsbildung und den öffentlichen Diskurs von Bedeutung. Die Reichweite wird gerade bei der Verbreitung von Desinformation als kritischer Faktor betrachtet.[25]

21 Berberich und Seip sahen Desinformation im DSA-E nicht ausreichend berücksichtigt: *Berberich/Seip*, GRUR-Prax 2021, 4 (7). Die finale Verordnung enthält keine wesentlichen Änderungen im Bereich der Desinformation.

22 Zur Effektivität gegen Desinformation *Setz*, in: Bernzen u.a. (Hrsg.), Immaterialgüter und Medien im Binnenmarkt. Europäisierung des Rechts und ihre Grenzen, 2022, 175 (190 ff.).

23 Im nationalen Recht enthält § 2 NetzDG bislang Berichtspflichten, die sich zumindest teilweise mit den Risikobewertungspflichten des DSA überschneiden, jedoch auf rechtswidrige Inhalte beschränkt sind.

24 Zum risikobasierten Ansatz: *Achleitner*, MR-Int 2022, 114, (116); *Rau et al.*, Rechtsextreme Online-Kommunikation in Krisenzeiten, 2022, S. 8.

25 *Achleitner*, MR-Int 2022, 114 (116).

Risikobewertung, Art. 34 DSA

Nach Art. 34 Abs. 1 S. 1 DSA sind sehr große Online-Plattformen[26] dazu verpflichtet, bestimmte systemische Risiken in der Union, die sich aus der Konzeption, dem Betrieb und der Nutzung ihrer Dienste sowie eingesetzter algorithmischer Systeme ergeben, sorgfältig zu ermitteln, zu analysieren und zu bewerten.[27] ErwG 84 stellt klar, dass Anbieter dabei auch besonders darauf achten sollten, wie ihre Dienste zur Verbreitung oder Verstärkung von Desinformation genutzt werden. Die Risikobewertung erfolgt gem. Art. 34 Abs. 1 S. 2 DSA mindestens einmal jährlich, jedenfalls aber vor jeder Einführung risiko-relevanter Funktionen.

Die in Art. 34 Abs. 1 S. 3 lit. a – d DSA aufgezählten systemischen Risiken stehen zum Teil in unmittelbarem, zum Teil in mittelbarem Bezug zu Desinformation. In Art. 34 Abs. 1 S. 3 lit. a DSA werden Risiken genannt, die durch die Verbreitung rechtswidriger Inhalte entstehen. Manche mitgliedsstaatlichen Regelungen sind so ausgestaltet, dass bestimmte Formen von Desinformation als rechtswidrig gelten (z. B. in Deutschland der Tatbestand der Volksverhetzung nach § 130 StGB, jeweils in der Variante des „Verleumdens" oder „Leugnens"). Dabei ist allerdings darauf zu achten, dass nach dem DSA nur als systemisch einzustufende Risiken zu bewerten sind, also solche, die eine gewisse qualitative und/oder quantitative Erheblichkeitsschwelle erreichen.[28] Daneben bietet der DSA eine Reihe anderer Maßnahmen, die nicht systemische Risiken, sondern einzelne Inhalte und Akteure betreffen und im Rahmen dieses Beitrags nicht vertieft werden können (z.B. die Pflicht zur Vorhaltung eines Melde- und Abhilfeverfahrens nach Art. 16 DSA und die Aussetzungspflicht nach Art. 23 DSA).

In Art. 34 Abs. 1 S. 3 lit. c DSA werden alle nachteiligen Auswirkungen auf die gesellschaftliche Debatte und Wahlprozesse genannt. Diese können grundsätzlich durch Desinformation unmittelbar beeinträchtigt werden, indem der zu Grunde liegende freie Willensbildungsprozess verzerrt wird. Problematisch ist, dass es sich bei dem Begriff „gesellschaftliche Debatte" um eine sehr weite Formulierung handelt, die potenziell jegliche Themen und Debattenformen beinhalten kann. Um ausufernde und unbestimmte Pflichten für die Anbieter zu vermeiden, müssen einschränkende inhalt-

26 Diese Pflichten betreffen ebenso „sehr große Online-Suchmaschinen".
27 Zum Sinn und Zweck der risikobezogenen Pflichten auch: *Kalbhenn*, ZUM 2022, 266 (273).
28 *Janal*, ZEuP 2021, 227 (266).

liche und quantitative Kriterien für die Schwelle eines systemischen Risikos hinzugezogen werden.[29] ErwG 79 nennt beispielhaft die Anzahl der betroffenen Personen, die Unumkehrbarkeit und den Wiederherstellungsaufwand. Zu bewerten ist danach sowohl die Schwere als auch die Wahrscheinlichkeit dieser Risiken.

Auch die in Art. 34 Abs. 1 S. 3 lit. b DSA genannten Risiken für die Ausübung der Grundrechte können in Bezug auf Desinformation relevant sein. Hervorgehoben werden etwa Meinungs- und Informationsfreiheit, Medienfreiheit und -pluralismus aus Art. 11 Abs. 1 bzw. 2 GRCh. Durch Desinformation kann der Prozess der individuellen Meinungsbildung verzerrt werden. Umgekehrt können aber auch Maßnahmen die von Online-Plattformen gegen Desinformation eingesetzt werden, die Grundrechte der Nutzer beeinträchtigen und damit ein systemisches Risiko darstellen. Die Risikobewertung nach Art. 34 Abs. 1 S. 3 lit. b DSA wird also i. d. R. einen Abwägungsvorgang zwischen konkurrierenden Grundrechten beinhalten.

In 34 Abs. 1 S. 3 lit. d DSA werden schließlich Risiken für einige Schutzgüter aufgezählt, die jedenfalls mittelbar durch Desinformation beeinträchtigt werden können. Dies wird anhand der Desinformationskampagnen der letzten Jahre besonders deutlich: Während der Covid-19-Pandemie wurde auf Grund der massenhaften Verbreitung von Desinformation über die Existenz und den Ursprung des Corona-Virus und über Schutzmaßnahmen von einer „Infodemie" gesprochen.[30] Hiermit korrespondieren die in 34 Abs. 1 S. 3 lit. d DSA genannte Risiken für die öffentliche Gesundheit und das körperliche Wohlbefinden, die sich gem. ErwG 83 auch aus koordinierten Desinformationskampagnen ergeben können. Auch die in 34 Abs. 1 S. 3 lit. d DSA gelistete geschlechtsspezifische Gewalt ist in Fällen von Gewalt befördernder misogyner Desinformation öffentlichkeitsrelevant geworden.[31]

Bei der Risikobewertung müssen gem. Art. 34 Abs. 2 lit. a–e DSA die technischen Funktionen der Dienste berücksichtigt werden, wie z. B. Empfehlungs-, Moderations-, Werbeauswahl- und Anzeigesysteme sowie

29 Zur Flexibilität des Risikobegriffs: *Achleitner*, MR-Int 2022, 114 (117).

30 *UNRIC.org*, UN und Partner fordern Länder auf „Infodemie" zu bekämpfen.

31 Z. B. ergab eine Umfrage der Interparlamentarischen Union von 2018 unter 123 weiblichen Abgeordneten oder Mitarbeiterinnen in nationalen Parlamenten in der EU, dass fast 47 Prozent im Laufe ihrer Karriere schon einmal in sozialen Medien Vergewaltigung oder sonstige Gewalt angedroht wurden, vgl. *Klimpel*, Wie Politikerinnen im Netz diskreditiert werden; *Ipu.org*, Sexism, harassment and violence against women in parliaments in Europe.

andere relevante algorithmische Systeme[32] der Anbieter. In die Bewertung einzuschließen sind zudem voluntative Elemente, wie die AGB und die datenbezogene Praxis der Anbieter. Auch durch Nutzerverhalten bedingte Faktoren, wie die vorsätzliche Manipulation, unauthentische Nutzung und automatisierte Ausnutzung der Dienste sowie die ihren AGB widersprechende Verbreitung und Verstärkung von Inhalten sind zu analysieren (Art. 34 Abs. 2 S. 2 DSA). Als Beispiel nennt ErwG 84 Risiken, die sich aus automatisierten oder teilautomatisierten Verhaltensweisen ergeben, die zu Desinformationskampagnen beitragen.

Risikominderung

Art. 35 Abs. 1 S. 1 DSA verpflichtet Anbieter i. S. d. Art. 33 DSA dazu, verhältnismäßige und wirksame Risikominderungsmaßnahmen zu ergreifen, die auf die gemäß Art. 34 ermittelten Risiken zugeschnitten sind. Dabei müssen die Auswirkungen solcher Maßnahmen auf die Grundrechte besonders berücksichtigt werden. Art. 35 Abs. 1 S. 2 lit. a–k DSA nennt exemplarisch Risikominderungsmaßnahmen, die von der Anpassung technischer Funktionen über AGB bis zu Moderationsmaßnahmen reichen. Die Kennzeichnungsmaßnahme gegen Deepfakes in lit. k dient der Bekämpfung visueller Desinformation.[33] Abs. 2 enthält Berichtspflichten und in Abs. 3 wird der EU-Kommission und den Koordinatoren für digitale Dienste die Befugnis übertragen, unter bestimmten Voraussetzungen gemeinsame Leitlinien für die Risikominderung für besondere Risiken herauszugeben. Zurecht werden diese Maßnahmen als zu vage kritisiert.[34]

Krisenreaktionsmechanismus

Gem. Art. 36 Abs. 1 DSA kann die EU-Kommission in einem Krisenfall auf Empfehlung des europäischen Gremiums für digitale Dienste[35] einen Beschluss erlassen, durch den Anbieter sehr großer Online-Plattformen

32 Zur Funktionsweise von Algorithmen und Regulierungserfordernissen vgl. *Kühling*, JZ 2021, 529 (531).

33 Eine Kennzeichnungspflicht für Deep Fakes ist auch im Art. 52 Abs. 3 KI-VO-E geplant. Dieser richtet sich jedoch an Anbieter bestimmter KI-Systemen und ihrer Nutzer. Art. 35 DSA adressiert hingegen nur "sehr große Online-Plattformen".

34 *Flamme*, MMR 2021, 770 (774).

35 Das europäische Gremium für digitale Dienste (Art. 61 DSA) setzt sich zusammen aus den Koordinatoren für digitale Dienste; die Kommission hat den Vorsitz (Art. 62 DSA).

(s.o.) aufgefordert werden, eine oder mehrere Maßnahmen nach Art. 36 Abs. 1 lit. a–c DSA zu ergreifen. Als Krise gilt nach Abs. 2 das Auftreten außergewöhnlicher Umstände, die zu einer schwerwiegenden Bedrohung der öffentlichen Sicherheit oder öffentlichen Gesundheit in der Union oder in wesentlichen Teilen der Union führen. Zu den Maßnahmen gehören nach Art. 36 Abs. 1 DSA die Bewertung, ob und wie der Betrieb und die Nutzung des Dienstes erheblich zu einer schwerwiegenden Bedrohung beitragen oder beitragen werden (lit. a), das Ergreifen gezielter, wirksamer und verhältnismäßiger Maßnahmen (lit. b) und die Berichterstattung an die Kommission (lit. c).[36] Auch für die Erfüllung dieser Pflichten können analytische Instrumente wie die Netzwerkanalyse eingesetzt werden.

Zwischenfazit

Zusammenfassend ist festzustellen, dass durch die risikobezogenen Pflichten der Artt. 34 ff. DSA der Grundgedanke der Bekämpfung systemischer Risiken fortentwickelt wird, indem diese explizit benannt und die Plattformarchitektur und AGB der Plattformen ausdrücklich in die Bewertung miteinbezogen werden müssen. Angesichts koordinierter Desinformationskampagnen, die auf die Ausnutzung der Plattformfunktionen angelegt sind, ist dieses Vorgehen für eine effektive Desinformationsbekämpfung sinnvoll.

Im DSA selbst ist nicht vorgegeben, wie die erläuterten Pflichten technisch umzusetzen sind. Im Folgenden soll daher die Netzwerkanalyse als ein mögliches Instrument zur Erfüllung der risikobasierten Pflichten aus Artt. 34 ff. DSA dargestellt werden. Derartige Instrumente können nicht nur für die Plattformanbieter, sondern auch für zugelassene Forscher i. S. d. Art. 40 Abs. 4 DSA nützlich sein, denen ein Datenzugang zur Erforschung systemischer Risiken ermöglicht wird.[37]

4. Die Netzwerkanalyse

Durch die Analyse von Interaktionen auf großen Online-Plattformen können Muster identifiziert werden, die auf eine Desinformationskampagne hindeuten können. Dabei kann, wie im Folgenden beschrieben, zwischen der Analyse der über einzelne Akteure hinausgehenden Verbreitungswege und der Betrachtung einzelner Akteure durch selbstdefinierte Netzwerk-

36 Vgl. dazu *Kuhlmann/Trute*, GSZ 2022, 115 (122).
37 Vgl. *Löber*, ZD-Aktuell 2022, 014290.

strukturen unterschieden werden, wobei unter Akteuren in diesem Kontext neben Nutzern auch Gruppen und Kanäle verstanden werden.

4.1 Analyse der Verbreitungswege

Die Verbreitungswege von Nachrichten zwischen Akteuren werden im Folgenden zunächst anhand von Metadaten, anschließend anhand des Nachrichtentextes diskutiert.

Metadatenbasiert

Durch Metadaten können Verbreitungswege durch sogenannte Nachrichtenkaskaden, d. h. die direkte Darstellung der Nachrichtenverbreitung, ermittelt werden. Eine Nachrichtenkaskade bezeichnet einen Baum oder eine baumähnliche Struktur, welche die Verbreitung eines bestimmten Nachrichtenartikels in einem Online-Netzwerk erfasst. Der Wurzelknoten repräsentiert den Nutzer, der einen Nachrichtenartikel zuerst teilt. Die anderen Knoten in der Kaskade repräsentieren Nutzer, die den Artikel nach der Veröffentlichung durch ihre übergeordneten Knoten, mit denen sie über Kanten verbunden sind, weiterverbreiten. Eine Nachrichtenkaskade kann durch die Anzahl der Schritte (d. h. hop-based), welche die Nachricht durchlaufen hat, oder durch die Zeitpunkte, zu denen sie veröffentlicht wurde (d. h. time-based), dargestellt werden.[38] Der Inhalt der Nachricht wird dabei nicht betrachtet.

Telegramkanäle und -gruppen bestehen zum Teil aus weitergeleiteten Nachrichten. Die Abbildung der Verbreitungsstruktur dieser Nachrichten kann dabei helfen, die Quelle einer Desinformation zu identifizieren und zu verstehen, wie sie durch das Netzwerk verbreitet wurde. Die Verbreitungswege einer Nachricht können dabei mit Kanälen oder Gruppen als Knoten untersucht werden. Je nach Online-Plattform unterscheiden sich die Metadaten, die über weitergeleitete Nachrichten vorhanden sind. In Telegram ist von den weitergeleiteten Nachrichten nur der Ursprungskanal/-gruppe oder der originäre Nutzer bekannt. Durch die Angabe des Zeitpunkts der Veröffentlichung kann damit der Zeitverlauf der Weiterleitungen ermittelt werden, genannt time-based Nachrichtenkaskade. Die Zwischenkanäle/-gruppen, von denen die weitergeleitete Nachricht wiederum weitergeleitet wurde (hops), sind bei Telegram nicht bekannt. Verbin-

38 *Zhou/Zafarani,* ACM Comput. Surv. 2020, 21 (22f.).

dungen können daher immer nur zwischen einem Kanal/einer Gruppe und einem Ursprungskanal/einer Ursprungsgruppe hergestellt werden. Dies führt nicht zu den aus der Literatur bekannten Kaskaden[39] mit mehreren übergeordneten Knoten (siehe Abb.1a), sondern zu Kaskaden mit jeweils zwei Knoten (siehe Abb. 1b) oder zu einer langen Kaskade mit allen Knoten (unter der Annahme, dass die Gruppen/Kanäle nach dem Zeitpunkt der Veröffentlichung sortiert werden können).

Anders verhält es sich z. B. bei Twitter. Hier ist immer nur die Kennung des letzten Postings der Nachricht bekannt, so dass der Weg der Nachricht zurückverfolgt werden kann. Dies würde bei Twitter zu einer hop-based Nachrichtenkaskade führen (siehe Abb.1a).

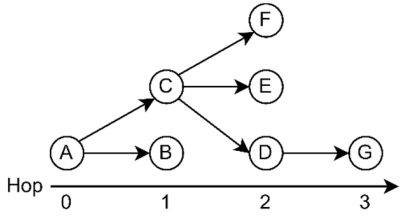

Abb. 1a: Nachrichtenkaskaden bei Twitter (hop-based), nach Zhou/Zafarani[40]

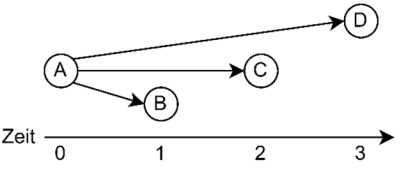

Abb. 1b: Nachrichtenkaskaden bei Telegram (time-based), eigene Darstellung

Durch die Nachverfolgung der Verbreitungswege können time-based Merkmale wie „Lifetime", „Real-time heat" und „Overall heat" ermittelt werden. Nach Zhou/Zafarani[41] geben diese drei Kennzahlen Hinweise darauf, ob es sich bei der vorliegenden Nachricht um Desinformation handeln könnte:

- *Lifetime* gibt die längste Kette an, in dem sich die Nachricht verbreitet hat (Abb. 1a, 4).
- *Real-time heat* (zum Zeitpunkt t) ist die Anzahl der Nutzer, die die Nachricht jeweils zum Zeitpunkt t gepostet/weitergeleitet haben und
- *Overall heat* die Gesamtzahl der Nutzer, die die Nachricht weitergeleitet/gepostet haben.

Ein weiteres Merkmal ist die Zeit, die Kaskaden von Desinformationen benötigen, um eine beliebige Tiefe und Größe zu erreichen. Die Tiefe gibt

39 *Zhou/Zafarani,* ACM Comput. Surv. 2020, 21 (22).
40 *Zhou/Zafarani,* ACM Comput. Surv. 2020, 22.
41 *Zhou/Zafarani,* ACM Comput. Surv. 2020, 22.

die maximale Anzahl an Schritten an, die die Nachricht innerhalb der Kaskade durchlaufen hat (Abb. 1a, Tiefe: 3). Die Größe wird durch die Gesamtzahl der Knoten bestimmt (Abb. 1a, Größe: 7). Die Zeit für das Erreichen einer beliebigen Größe und Tiefe ist laut Vosoughi u.a.[42] bei Desinformationen kürzer als bei Kaskaden mit echten Nachrichten. Die Tiefe einer Nachrichtenkaskade ist bei Telegram nicht bekannt, da mit den verfügbaren Informationen keine Verzweigungen identifiziert werden können, aber die Tiefe ist der Lifetime sehr ähnlich, die stattdessen als Merkmal verwendet werden könnte. Die Größe, also die Anzahl der Knoten innerhalb der Nachrichtenkaskade (Overall heat), ist auch bei Telegramdaten bekannt.

Für die Klassifizierung der Nachricht als Desinformation oder sonstige Information wird bei der Untersuchung der Verbreitungswege stellvertretend die Kaskade zur Klassifikation herangezogen. Dazu können Methoden des traditionellen maschinellen Lernens wie Support Vector Machine (SVM)[43], Entscheidungsbäume[44] oder Naive Bayes[45] verwendet werden. Auch (tiefe) neuronale Netze werden z. B. für Twitterdaten vorgeschlagen.[46] Dabei wird die Struktur der Nachrichtenkaskade in neuronalen Netzen nachgebildet, und es werden Werte für die Blattknoten ermittelt. Dies ist bei Telegram aufgrund der bereits erwähnten mangelnden Nachvollziehbarkeit der Verzweigungen nicht möglich. Auch Kontoeinstellungen wie die Anonymisierung des Nutzers in Telegram in den Privatsphäre-Einstellungen, die eine Nachverfolgung von geposteten Nachrichten unmöglich macht, erschweren diese Analyse. Aufgrund dieser Schwierigkeiten sollten

42 *Vosoughi* u.a., science 2018, 1147.

43 *Castillo* u.a., Information credibility on twitter in: Sadagopan u.a. (Hrsg.), Proceedings of the 20th international conference on World wide web, 2011, 680; *Kwon* u.a., Prominent Features of Rumor Propaganda in Online Social Media, in: 2013 IEEE 13th international conference on data mining 2013, 1108; *Wu* u.a., False rumors detection on Sina Weibo by propagation structures, in: 2015 IEEE 31st international conference on data engineering 2015, 653 (654).

44 *Castillo* u.a., Information credibility on twitter in: Sadagopan u.a. (Hrsg.), Proceedings of the 20th international conference on World wide web, 2011, 680; *Kwon* u.a., Prominent Features of Rumor Propaganda in Online Social Media, in: 2013 IEEE 13th international conference on data mining 2013, 1108.

45 *Castillo* u.a., Information credibility on twitter in: Sadagopan u.a. (Hrsg.), Proceedings of the 20th international conference on World wide web, 2011, 680.

46 *Zhou/Zafarani,* ACM Comput. Surv. 2020, 22 (23).

inhaltliche Analysen wie die „Semantic Similarity“[47] neben der Metadaten-Analyse in Betracht gezogen werden.

Semantische Analyse

Um die Verbreitungswege identischer und ähnlicher Inhalte zu analysieren, reicht es nicht aus, nur die Weiterleitungsfunktion von Inhalten in Telegram zu betrachten, da hier nur der Ursprungskanal oder die Ursprungsgruppe erkenntlich ist. Um gleiche Inhalte (Bilder, Videos und Texte) automatisiert erkennen zu können existieren unterschiedliche Ansätze. Auf der Textebene kann die semantische Ähnlichkeitsanalyse (engl. Semantic Similarity) in Betracht gezogen werden. Semantic Similarity ist eine Aufgabe im Bereich der Verarbeitung natürlicher Sprache („Natural Language Processing“, kurz NLP), bei der die Ähnlichkeit zwischen Texten oder Dokumenten anhand einer definierten Metrik bewertet wird. Die aktuell gängigste Methode besteht darin, ein maschinelles Lernmodell (z. B. einen Transformer) zu verwenden, welches Sätze zunächst in eine Vektordarstellung überführt.[48] In der Regel liegen dabei inhaltlich ähnliche Sätze im Vektorraum näher beieinander. Dann wird eine Ähnlichkeitsmetrik (z. B. Cosinus-Ähnlichkeit) verwendet, um zu berechnen, ob die Sätze sich inhaltlich ähnlich sind oder nicht. Es geht folglich darum, festzustellen, ob zwei oder mehr Textstücke die gleiche Bedeutung haben oder nicht.

Mithilfe der Ähnlichkeitsanalyse lässt sich nicht nur analysieren, wie dieselben Inhalte innerhalb Telegrams weitergeleitet werden, sondern auch wie identische oder ähnliche Inhalte generell plattformübergreifend verbreitet werden, d. h. über die Grenze einer Online-Plattform hinweg (Interoperabilität zwischen Online-Plattformen). Es können folglich unbekannte Verbreitungswege zwischen Kanälen/Gruppen innerhalb und außerhalb Telegrams identifiziert werden. Diese Kanäle/Gruppen teilen dieselben Inhalte, sind jedoch laut ihrer Metadaten nicht untereinander vernetzt.

Nachdem die identischen oder ähnlichen Nachrichten identifiziert wurden (durch Metadaten oder Semantic Similarity), können diese und die Akteure (Nutzer, Gruppe, Kanal) auf ihre Charakteristika (Medientyp, Thema etc.) untersucht werden).

47 *Chandrasekaran/Mago*, ACM Comput. Surv. 2021, 1.
48 *Chandrasekaran/Mago*, ACM Comput. Surv. 2021, 1.

4.2 Analyse einzelner Akteure

Einzelne Akteure (Nutzer, Gruppe, Kanal) können durch selbstdefinierte Netzwerkstrukturen abgebildet und analysiert werden.[49]

Anders als bei den Nachrichtenkaskaden können diese Netzwerke unterschiedliche (selbstdefinierte) Strukturen annehmen. Unterschieden wird zwischen homogenen, heterogenen oder hierarchischen Netzwerken.[50] Homogene Netzwerke (Bsp. siehe Abb. 2) bestehen aus einer Art, heterogene Netzwerke aus verschiedenen Arten an Knoten und Kanten. Hierarchische Netzwerke bilden verschiedene Arten von Knoten und Kanten in Mengen-Teilmengen-Beziehungen (d. h. Hierarchien) ab. In hierarchischen Netzwerken stellen beispielsweise die Kanten die Zugehörigkeit einer Nachricht (Knoten) zu einem übergeordneten Ereignis (Knoten) dar.

Beispielsweise können Ansichten der Nutzer zu einem Thema innerhalb eines Kanals/einer Gruppe durch homogene Netzwerke dargestellt werden. Dieses Netzwerk wird als Stance Net bezeichnet und bildet auf den Knoten die unterschiedlichen Ansichten der Nutzer zu einem Thema und auf den Kanten die Beziehung dieser (Unterstützend (+) oder Gegensätzlich (-)) ab (Abb. 2), wobei die Themen durch Methoden des NLP wie Topic Modeling identifiziert werden können. Topic Modeling, auch bekannt als Textkategorisierung, ist eine Technik der Textanalyse, mit der vorherrschende Themen eines Textkorpus identifiziert werden können.[51] Hierfür wird z. B. ein Algorithmus verwendet, der die Nachrichten auf Basis ihrer semantischen Ähnlichkeit zu Themen gruppiert, wobei jedes Thema mithilfe von Schlagwörtern extrahiert bzw. beschrieben werden kann.[52]

Desinformationen provozieren oft kontroverse Ansichten, wobei verneinende und hinterfragende Haltungen einen Hinweis darauf geben können, ob Nachrichten als falsch zu klassifizieren sind.[53] Informationen für die Bildung dieser Netzwerke können aus den Metadaten wie „gefällt mir"-Angaben oder dem Nachrichtentext mittels NLP, z. B. durch die Stimmungsanalyse (eng. Sentiment Analysis) oder der Analyse des Standpunktes einer

49 *Zhou/Zafarani,* ACM Comput. Surv. 2020, 24 (25f).
50 *Zhou/Zafarani,* ACM Comput. Surv. 2020, 24 (25f).
51 *Churchill/Singh,* ACM Comput. Surv. 2022, 1 (2f).
52 *Grootendorst*, arXiv preprint 2022, 1.
53 *Shu* u.a., Emerging research challenges and opportunities in computational social network analysis and mining 2019, 7; *Jin* u.a., News Verification by Exploiting Conflicting Social Viewpoints in Microblogs, in: Proceedings of the AAAI conference on artificial intelligence 2016, 2972 (2973f).

Nachricht (eng. Stance Detection) ermittelt werden. Hierbei kann ein „Profil" mit den Eigenschaften des jeweiligen Nutzers erstellt oder aber es können Standpunkte repräsentativ für eine Gruppe von Nutzern (einer/einem Telegram Gruppe/Kanal) gebildet werden. Werden Standpunkte auf Basis von Nutzerprofilen erstellt, kann auch hier die bereits erwähnte Anonymisierungsfunktion von Telegram den Autor einer Nachricht unkenntlich machen. Weiter zu beachten ist, dass hierfür in Telegram nur Daten aus Gruppen verwendet werden können und nicht aus Kanälen, da in diesen nur die Administratoren Nachrichten veröffentlichen können. In Telegram existieren keine Folgebeziehungen zwischen Nutzern („Follower"), wie dies bei Twitter der Fall ist. Analysen auf Basis von „Freundschaften" und den daraus resultierenden Einflüssen aufeinander sind daher, zumindest auf Nutzerebene, nicht möglich (z. B.: Spreader Net, nach Zhou/Zafrani[54]).

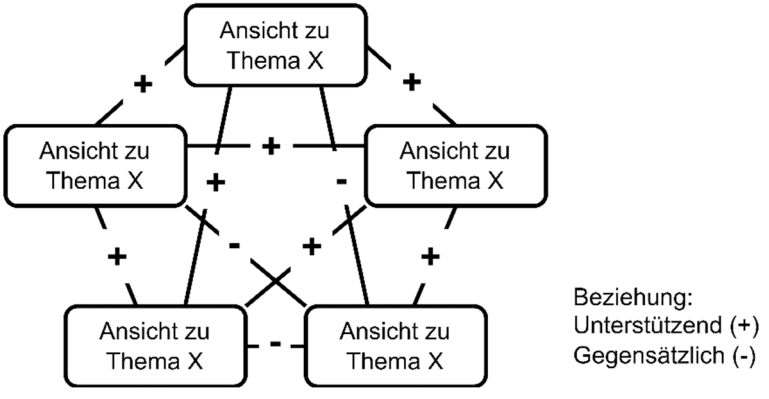

Abb. 2: Stance Net (Homogenes Netzwerk), eigene Darstellung nach Zhou/Zafarani[55] und Jin u.a.[56]

Mithilfe der Netzwerkanalyse können zwar keine Desinformationen als solche identifiziert werden. Allerdings können verdächtige Themen erkannt werden, die sich sehr schnell über die Kanäle/Gruppen hinweg oder auch plattformübergreifend verbreiten. Auf diese Weise ist es möglich die Relevanz eines Themas und entsprechende Kanäle/Gruppen mit einem hohen

54 *Zhou/Zafrani*, ACM SIGKDD explorations newsletter 2019, 48 (49f).
55 *Zhou/Zafarani,* ACM Comput. Surv. 2020, 25.
56 *Jin* u.a., News Verification by Exploiting Conflicting Social Viewpoints in Microblogs, in: Proceedings of the AAAI conference on artificial intelligence 2016, 2972 (2973f).

Einfluss zu erkennen, um zeitig darauf reagieren zu können (z. B. durch eine entsprechende Kennzeichnung durch Fact-Checking-Organisationen).

5. Diskussion

Die neuen risikobezogenen Pflichten aus Artt. 34 ff. DSA sind ein im Ausgangspunkt begrüßenswerter Versuch des europäischen Gesetzgebers, netzbasierte Desinformation, die oftmals keinen Straftatbestand erfüllt, regulatorisch einzuhegen. Allerdings zieht diese Regulierung auch rechtliche Bedenken nach sich. Allgemein ist problematisch, dass keinerlei Qualitätsvorgaben zur technischen Umsetzung gemacht werden. Zu befürchten ist, dass von den Plattformen Verfahren eingesetzt werden, die ein verzerrtes Bild wiedergeben. Hinzu kommen spezifische rechtliche und technische Herausforderungen konkreter Analyseinstrumente, die die Anbieter einsetzen könnten. Diese werden im Folgenden für das Beispiel der Netzwerkanalyse näher betrachtet werden.

5.1 Rechtliche Probleme

Aus rechtlicher Perspektive wird grundsätzlich kritisiert, dass die Vorschriften der Artt. 34 ff. DSA insgesamt sehr vage formuliert sind.[57] Dies führ zu einigen Folgeproblemen.

Überwachungspflichten der Anbieter

Zu befürchten ist zunächst, dass durch die neuen risikobezogenen Pflichten aus Artt. 34 ff. DSA de facto eine Überwachungspflicht für sehr große Online-Plattformen begründet wird. In Art. 8 DSA wird zwar statuiert, dass die Verordnung Vermittlungsdiensten gerade keine allgemeine Verpflichtung zur Überwachung auferlegt. ErwG 30 spezifiziert, dass eine solche Pflicht weder de jure noch de facto bestehen soll, wobei Ausnahmen gem. ErwG 30 lediglich für bestimmte Fälle gestattet sind. Zur Erfüllung der Risikobewertung nach Art. 34 DSA ist es jedoch faktisch erforderlich, dass die Dienste jegliche Inhalte auf ihre potenzielles Risikorelevanz prüfen und feststellen, ob die Schwelle zum „systemischen Risiko" überschritten

57 *Buri/Van Hoboken*, The Digital Services Act (DSA) proposal: a critical overview, 2021, S.33.

wurde. Wird die Pflicht nach ErwG 30 so ausgelegt, dass keine allgemeine Überwachungspflicht besteht, bleibt zweifelhaft, ob die Risikobewertung effektiv zur Pflichterfüllung erfolgen kann.

Eine ähnliche Widersprüchlichkeit ist hinsichtlich der Haftungsprivilegierung der Hosting-Dienste aus Art. 6 Abs. 1 DSA zu befürchten. Danach haften Anbieter von Hosting-Diensten nicht, sofern sie keine tatsächliche Kenntnis von rechtswidrigen Inhalten oder diese begründenden Umständen haben oder zügig tätig werden, um diese Inhalte zu sperren oder zu entfernen. Diese grundsätzlich geltende Privilegierung droht aber dadurch ausgehöhlt zu werden, dass sehr großen Online-Plattformen bei Verletzung der Risikobewertungspflichten, die eine aktive Ermittlung erfordern, Sanktionen nach Artt. 74 und 76 DSA drohen. Sollte die sog. „gute Samariter Privilegierung" aus Art. 7 DSA[58] so ausgelegt werden, dass Dienste bei freiwilligen Risikobewertungsmaßnahmen nicht sanktioniert werden, droht die Risikobewertungspflicht wiederum an Effektivität einzubüßen.[59]

Fehlende datenschutzrechtliche Verarbeitungsgrundlage

Zudem zeichnen sich durch die risikobezogenen Pflichten aus Artt. 34 ff. DSA datenschutzrechtliche Konfliktlagen ab. Problematisch ist in diesem Zusammenhang, dass die Ermittlung und Bewertung systemischer Risiken eine breite Datengrundlage erfordert, wobei aus funktionaler Sicht auch zahlreiche personenbezogene Daten i. S. d. Art. 4 Nr. 1 DSGVO verarbeitet werden müssten. Grundsätzlich lässt der DSA gem. Art. 2 Abs. 4 lit. g DSA Unionsvorschriften zum Schutz personenbezogener Daten, z. B. die DSGVO, unberührt. Daher ist etwa neben der Risikobewertung nach Artt. 34 ff. DSA bei der Einführung risikorelevanter neuen Funktionen ggf. auch eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen.

Besonders zweifelhaft ist, ob die Artt. 34 ff. DSA geeignete Rechtsgrundlagen i. S. d. Art. 6 Abs. 1 lit. c, Abs. 3 lit. a DSGVO darstellen, um die Analyse personenbezogener Daten im Rahmen des Risikomanagements zu legitimieren. Dafür müsste die Datenverarbeitung durch die gesetzliche

58 Dieser stellt klar, dass die Haftungsprivilegierung auch bei freiwilligen Untersuchungen der Dienste-Anbieter unter bestimmten Voraussetzungen gilt. So wird Vermittlungsdiensten einen Anreiz zum Ergreifen solcher Maßnahmen gesetzt.

59 So auch: *Holznagel*, CR 2021, 123 (132); Weitere grundrechtliche und medienrechtliche Probleme thematisieren *Berberich/Seip*, GRUR-Prax 2021, 4 (6).

Rechtsgrundlage festgelegt werden und zur Erfüllung einer rechtlichen Verpflichtung erforderlich sein.[60]

Bereits aus Art. 8 Abs. 2, Art. 52 Abs. 1 GRCh ergibt sich, dass Rechtsgrundlagen klar und präzise ausgestaltet und ihre Anwendung vorhersehbar sein müssen. Deklaratorisch stellt Art. 6 Abs. 3 S. 2 und 4 DSGVO klar, dass die Rechtsgrundlage die Zwecke der dazu erforderlichen Verarbeitung festlegen muss.[61] Die rechtliche Verpflichtung muss sich unmittelbar auf die Datenverarbeitung beziehen, und der Zweck muss spezifisch bestimmt sein. Allein der Umstand, dass ein Verantwortlicher, um eine rechtliche Verpflichtung erfüllen zu können, auch personenbezogene Daten verarbeiten muss, reicht nicht aus.[62] In den Vorschriften der Artt. 34 ff. DSA wird indes an keiner Stelle ausdrücklich erwähnt, dass personenbezogene Daten verarbeitet werden dürfen. Somit muss den Artt. 34 ff. DSA eine Konturlosigkeit attestiert werden, die verschiedenste Datenverarbeitungen möglich erscheinen lässt (z. B. den Abgleich personenbezogener Daten verschiedener Nutzer, die dauerhafte Speicherung, ggf. sogar das Anlegen umfassender Nutzerprofile). Dies ist mit grundrechtlichen Bestimmtheitsanforderungen nicht vereinbar.

Weiterhin besteht zwar das nach Art. 6 Abs. 3 S. 4 DSGVO geforderte im öffentlichen Interesse liegende Ziel, indem Artt. 34 ff. DSA die Schaffung eines sicheren und vertrauenswürdigen Online-Umfelds bezwecken (vgl. ErwG 75 DSA). Dieses legitime Ziel ist fraglos gewichtig, jedoch kann es unter Verhältnismäßigkeitsgesichtspunkten nicht sämtliche, heute ggf. noch gar nicht absehbare für Artt. 34 ff. DSA sinnvolle Datenverarbeitungen legitimieren.

Dies wird besonders deutlich, wenn es um sensible, also besondere Kategorien personenbezogener Daten geht, deren Verarbeitung Art. 9 Abs. 1 DSGVO grundsätzlich untersagt. Von den Ausnahmen in Art. 9 Abs. 2 DSGVO kommt lit. g in Betracht, da die Bekämpfung von Desinformation zu den „Gründen eines erheblichen öffentlichen Interesses" zählt. Die Norm verlangt jedoch, dass die entsprechende Rechtsgrundlage „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen" regelt. Diese enthält der DSA nicht.

60 *Roßnagel*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, Art. 6 DS-GVO, Rn. 52.

61 *Frenzel* in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 6 DS-GVO, Rn. 45; *Heberlein* in: Ehmann/Selmayr (Hrsg.), DS-GVO, Art. 6 DS-GVO, Rn. 15 m.w.N.

62 *Albers/*Veit in: Wolff/Brink (Hrsg.), BeckOK Datenschutzrecht, Art. 6 DS-GVO, Rn. 48; *Roßnagel*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, Art. 6 DS-GVO, Rn. 29; a.A. *Frenzel* in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 6 DS-GVO, Rn. 41.

Besonderheiten der Netzwerkanalyse

Auch die Anwendung der Netzwerkanalyse birgt Gefahren für den Schutz personenbezogener Daten, da diese Personen zugeordnet werden, um zu Diagrammen verarbeitet zu werden. Dies ist unter anderem deswegen problematisch, da bei der Analyse der Nachrichteninhalte regelmäßig Daten verarbeitet werden, die in den Katalog des Art. 9 Abs. 1 DSGVO fallen. Beschränkt sich die Analyse allerdings auf Metadaten, bei denen dies nicht der Fall ist, ist es möglich, andere Rechtsgrundlagen heranzuziehen, insbesondere berechtigte Interessen der Anbieter, wenn diese gegenüber Grundrechten und Grundfreiheiten der betroffenen Personen überwiegen (Art. 6 Abs. 1 UAbs. 1 DSGVO lit. f).

Greift Art. 9 Abs. 1 DSGVO, kommt von den Ausnahmen des Art. 9 Abs. 2 DSGVO zwar nicht lit. g (s.o.), ggf. aber lit. e in Betracht, wenn die Daten offensichtlich durch die betroffene Person veröffentlicht wurden.[63] Indes wird gerade beim Anwendungsbeispiel Telegram deutlich, dass die Einstufung als „veröffentlicht" von den jeweils genutzten Kommunikationsfunktionen (Kanal, Gruppe) als auch anderen Faktoren, wie der Gruppengröße, abhängt und im Einzelfall beurteilt werden muss.[64] Ohnehin veröffentlichen Nutzer auf den Plattformen vielfach auch Daten Dritter, die diese dann nicht selbst öffentlich gemacht haben; insgesamt bleibt die Verarbeitung öffentlicher Massendaten damit ein teilweise ungelöstes Problem,[65] für das Rechtsgrundlagen geschaffen werden sollten. Losgelöst von der grundsätzlichen Frage der Verarbeitungsbefugnis müssen bei Anwendung der Netzwerkanalyse Anonymisierung, Pseudonymisierung oder andere Maßnahmen des Datenschutzes durch Technikgestaltung (Art. 25 DSGVO) vorgenommen werden.[66] Zu bedenken ist allerdings, dass eine Anonymisierung oder Pseudonymisierung bei Inhaltsdaten nur schwer zu erreichen ist, da z. B. Texte durch eine einfache Web-Suche Personen zugeordnet und prominente Personen anhand ihres Schreibstils identifiziert werden können.

63 Schutzlos gestellt ist die betroffene Person durch eine Veröffentlichung jedoch nicht. Vorausgesetzt ist immerhin das Vorliegen ein Erlaubnistatbestands nach Art. 6 Abs. 1 UAbs. 1 DSGVO, vgl. *Petri*, in: *Simitis/Hornung/Spiecker gen. Döhmann*, DSGVO, Art. 9, Rn 57; *Hornung/Gilga*, CR 2020, 367 (374).

64 *Petri*, in: *Simitis/Hornung/Spiecker gen. Döhmann*, DSGVO, Art. 9, Rn 58.

65 Näher *Hornung/Gilga*, CR 2020, 367ff.

66 Weitere grundrechtliche und medienrechtliche Probleme thematisieren *Berberich/Seip*, GRUR-Prax 2021, 4 (6).

5.2 Technische Herausforderungen

Für die Erkennung von Desinformation müssen die Faktizität (enthält die Nachricht eine nicht faktengemäße Aussage?) und die Absicht (zielt sie darauf ab, Menschen in die Irre zu führen oder Menschen zu schaden?) analysiert werden.[67] Faktizität kann über sogenanntes Fact-Checking untersucht werden. Dieses ist jedoch von der Domäne abhängig und in Echtzeit momentan aufgrund der Schnelligkeit der Verbreitung von Nachrichten nicht anwendbar. Auch die Irreführungs- oder Schädigungsabsicht ist kaum zu ermitteln und nachzuweisen. Der gute Glaube des Verbreiters würde eine solche Absicht an sich entfallen lassen, ist aber ebenso schwer zu ermitteln. Ein Ansatz besteht darin, die Irreführungs- oder Schädigungsabsicht durch das Verhalten der Nutzer zu ermitteln, z. B. durch das Weiterleiten oder Veröffentlichen von Nachrichten.[68] Shu u.a.[69] klassifizieren z. B. auf der Basis von Weiterleitungen Nutzer, die wiederholt Desinformationen weiterleiten, als eher geneigt Desinformation zu glauben. Dieses beobachtbare Verhalten in sozialen Medien spiegelt jedoch nicht zwangsläufig den Glauben oder die Absicht des Nutzers wider.[70] Sowohl für die Analyse der Faktizität als auch der Absicht und damit für die Erkennung von Desinformation ist ein tieferes Verständnis des Inhalts, der zugrundeliegenden Logik und des menschlichen Verhaltens erforderlich.

In der Literatur lassen sich Methoden zur Desinformationserkennung in wissensbasierte (Überprüfung, ob Wissen im Nachrichtentext mit Fakten übereinstimmt), stilbasierte (wie sind Nachrichten geschrieben, Bsp. Analyse der Emotionen/Intentionen), propagationsbasierte (Untersuchung der Verbreitungswege) und quellbasierte Ansätze (Untersuchung der Nachrichtenquelle, Bsp. Nutzer) unterscheiden.[71] Mittels der Netzwerkanalyse wurden hier vor allem propagationsbasierte (die Verbreitungswege von Weiterleitungen) und quellbasierte Ansätze (Analyse der Akteure) dargestellt. Die Netzwerkanalyse bietet die Möglichkeit, Akteure und ihre Verbindungen untereinander zu beschreiben, stellt aber keine alleinige Methode zur automatisierten Desinformationserkennung dar. Durch eine Analyse der Verbreitungswege können Akteure mit meinungsbildendem Einfluss, d. h.

67 *Zhou/Zafarani,* ACM Comput. Surv. 2020, 3 (4f.); *Baptista/Gradim*, Encyclopedia 2022, 640; *Lazer* u.a., Science 2018, 1094.
68 *Pennycook* u.a., Nature 2021, 590.
69 *Shu* u.a., IEEE MIPR 2018, 3.
70 *Ellison* u.a., Journal of Computer-Mediated Communication 2020, 402 (403f.).
71 *Zhou/Zafarani,* ACM Comput. Surv. 2020, 7 (8f.).

Ursprünge von vielen Weiterleitungen, identifiziert werden. Wurde eine Vorauswahl an Akteuren vorgenommen, kann deren Inhalten näher untersucht werden, z. B. durch wissensbasierte und stilbasierte Methoden oder selbstdefinierten Netzwerkstrukturen.

6. Fazit und Ausblick

Die rechtliche Analyse der risikobezogenen Pflichten des DSA zeigt, dass diese grundsätzlich zu einem sicheren und vertrauenswürdigen Online-Umfeld beitragen können. Durch die jährlich zu erfüllenden Pflichten können systemische Risiken langfristig evaluiert werden, was sukzessiv ermöglicht, die bestehende Regulierung – auch hinsichtlich einer effektiveren Desinformationsbekämpfung – adäquat anzupassen.

Zugleich offenbart der DSA eine Fülle offener Rechtsfragen. Beim Anwendungsbereich (Online-Plattform vs.„sehr große Online-Plattform“) zeigt das Beispiel Telegram, dass die Berechnungsmaßstäbe für Hybrid-Medien weiterer Konkretisierung bedürfen. Der DSA enthält überdies etliche unbestimmte Gesetzesformulierungen und verursacht neue medien- und datenschutzrechtliche Probleme.

Als ein Instrument der Risikoabschätzung ermöglicht die Netzwerkanalyse, Kanäle/Gruppen und ihre Verbindungen untereinander zu bestimmen und zu beschreiben. Angesichts der großen Datenmengen kann eine Vorauswahl relevanter Akteure für eine weitergehende Analyse hilfreich sein.

Hierdurch können z. B. die folgenden Fragen untersucht werden:

- Von welchem Kanal/welcher Gruppe werden besonders viele Nachrichten verbreitet?
- Welche Art von Nachrichten (Medientyp,[72] Thema etc.) wird viral verbreitet?
- Liegt der Ursprung der Nachrichten in Telegram oder bei anderen Plattformen?
- Existieren erste Merkmale, die auf Desinformation hindeuten (Eigenschaften der Nachrichtenkaskade)?
- Welche Standpunkte werden zu bestimmten Themen in den Kanälen/Gruppen vertreten?

72 Dies kann z. B. ein Bild, Video oder auch eine Nachricht mit oder ohne URL sein.

- Welche Nutzer sind besonders aktiv und welche Inhalte verbreiten sie?
- Welche Nutzer sind wie häufig in mehreren Kanälen/Gruppen aktiv?

Antworten auf diese Fragen können ein wichtiger Bestandteil einer Analyse der einzelnen in Art. 34 Abs. 1 S. 3 DSA genannten systemischen Risiken sehr großer Online-Plattformen sein, indem sie beispielsweise als solche erkennen lassen, wie sich bestimmte rechtswidrige Inhalte verbreiten (S. 3 lit. a) oder die Grundlage für weitergehende, vertiefte Risikobewertungsmaßnahmen bilden.

Bei der Risikobewertung nach Art. 34 DSA muss auch auf die Verbreitung von Desinformation eingegangen werden. Hierbei kann die Netzwerkanalyse als erste Übersicht dienen und Akteure mit großer Reichweite (Einfluss) identifizieren. Zu diesen einflussreichen Akteuren können dann nähere Untersuchungen auf Desinformation (z. B. durch NLP, Fact-Checking) durchgeführt werden. Die Netzwerkanalyse kann damit als erstes, aber nicht abschließendes Instrument zur Erkennung und Bekämpfung von Desinformation verwendet werden.[73]

Angesichts der Bedeutung, die der europäische Gesetzgeber dem Risikomanagement im DSA beimisst, bleibt abschließend allerdings auf das erläuterte regulatorische Defizit hinzuweisen. Datenschutzrechtlich steht die Verarbeitung personenbezogener Daten zur Risikobewertung und Risikominderung auf tönernen Füßen, da der DSA keine Befugnis enthält, die Umfang und Grenzen der zulässigen Verarbeitung erkennen lässt. Diese sowohl für die Anbieter als auch für die betroffenen Nutzer schwer erträgliche Situation sollte der Gesetzgeber beheben.

Literatur

Achleitner, Ranjana Andrea (2022): Der Digital Services Act als risikobasierte Regulierung. *Medien und Recht International (MR-Int)*, 18(4), S. 114-121.

Albers, Marion und Veit, Raoul-Darius (2022): Artikel 6 Datenschutz-Grundverordnung. In: Wolff, Amadeus und Brink, Stefan (Hrsg.): *Beck'scher Online-Kommentar zum Datenschutzrecht*. München: C.H.Beck.

Balser, Markus (11. Feb. 2022): *Telegram sperrt 64 Kanäle*. URL: https://www.sueddeutsche.de/politik/telegram-kanaele-sperrung-l.5527255.

73 Neben der Netzwerkanalyse werden auch andere Verfahren vorgeschlagen, um Artt. 34 ff. DSA zu erfüllen; vgl. z. B. den Szenarien-basierten Ansatz von *Meßmer/Degeling*, Auditing Recommender Systems – Putting the DSA into practice with a risk-scenario-based approach, 2023; *Achleitner*, MR-Int 2022, 114 (116), schlägt die Heranziehung des internationalen Standards ISO 31000 vor.

Baptista, João P. und Gradim, Anabela (2022): A working definition of fake news. *Encyclopedia,* 2(1). doi: 10.3390/encyclopedia2010043.

Berberich, Matthias und Seip, Fabian (2021): Der Entwurf des Digital Services Act. *Praxis im Immaterialgüter- und Wettbewerbsrecht (GRUR-Prax)*, 13(1), S. 4- 7.

Borschert, Nils und Wolter, Daphne (April 2022): *Ort der Meinungsfreiheit und Verschwörungsplattform*. Berlin: Konrad-Adenauer-Stiftung.

Buri, Ilaria; van Hoboken, Joris (2021): *The Digital Services Act (DSA) proposal: a critical overview*, URL: https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf.

Castillo, Carlos; Mendoza Marcelo und Poblete Barbara (2011): Information credibility on twitter. *Proceedings of the 20th international conference on World wide web,* S675-684. doi: 10.1145/1963405.1963500.

Chandrasekaran, Dhivya und Mago, Vijay (2021): Evolution of semantic similarity—a survey. *ACM Computing Surveys*, 54(2), S. 1-37. doi: 10.1145/3440755.

Churchill, Rob und Singh, Lisa (2022): The evolution of topic modeling. *ACM Computing Surveys*, 54(10s), S.1-35. doi: 10.1145/3507900.

Denga, Michael (2021): Plattformregulierung durch europäische Werte: Zur Bindung von Meinungsplattformen an EU-Grundrechte. *Europarecht (EuR)*, 56(5), S. 569-595.

Eisenreich, Georg (2021): Digital Services Act – ein wirksames Instrument gegen Hass und Hetze im Netz. *Recht Digital (RDi)*, 1(6), S. 289-293.

Ellison, Nicole B.; Triệu, Penny; Schoenebeck, Sarita; Brewer, Robin und Israni, Aarti (2020): Why we don't click: Interrogating the relationship between viewing and clicking in social media contexts by exploring the "non-click". *Journal of Computer-Mediated Communication*, 25(6), S.402-426. doi: 10.1093/jcmc/zmaa013.

Europäische Kommission (2018): Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen – Bekämpfung von Desinformationen im Internet: ein europäisches Konzept. COM(2018) 236 final. Brüssel: Europäische Kommission.

Europäische Kommission (2023): Presseerklärung vom 17.02.2023 – Digital Services Act: Commission starts collecting platform's user numbers and consults on its monitoring and investigatory procedures. URL: https://digital-strategy.ec.europa.eu/en/news/digital-services-act-commission-starts-collecting-platforms-user-numbers-and-consults-its

Flamme, Florian (2021): Schutz der Meinungsvielfalt im digitalen Raum. Transparenzpflichten für Intermediäre im nationalen und europäischen Vergleich, *Multimedia und Recht (MMR)*, 24(10), S. 770-774.

Frenzel, Michael (2021): Artikel 6 Datenschutz-Grundverordnung. In: Paal, Boris und Pauly, Daniel A. (Hrsg.), *Kommentar DS-GVO/BDSG*. München: C.H.Beck.

Gielen, Nico und Uphues, Steffen (2021): Digital Markets Act und Digital Services Act – Regulierung vonn Markt- und Meinungsmacht durch die Europäische Union. *Europäische Zeitschrift für Wirtschaftsrecht (EuZW)*, 32(14), S. 627-637.

Grootendorst, Maarten (2022): BERTopic: Neural topic modeling with a class-based TF-IDF procedure. *arXiv preprint*. doi: 10.48550/ARXIV.2203.05794.

Heberlein, Horst (2018): Artikel 6 Datenschutz-Grundverordnung. In: Ehmann, Eugen und Selmayr, Martin (Hrsg.), *Kommentar DS-GVO*. München: C.H.Beck.

Holznagel, Daniel (2021): Chapter II des Vorschlags der EU-Kommission für einen Digital Services Act Versteckte Weichenstellungen und ausstehende Reparaturen bei den Regelungen zu Privilegierung, Haftung & Herkunftslandprinzip für Provider und Online-Plattformen, *Computer und Recht (CR),* 37(2), S. 123-132.

Hornung, Gerrit und Gilga, Carolin (2020): Einmal öffentlich – für immer schutzlos? Die Zulässigkeit der Verarbeitung öffentlicher personenbezogener Daten, *Computer und Recht (CR),* 36(6), S. 367-379.

Inter-Parliamentary Union (Oktober 2018): Sexism, harassment and violence against women in parliaments in Europe. Genf: Inter-Parliamentary Union.

Janal, Ruth (2021) Haftung und Verantwortung im Entwurf des Digital Services Acts, *Zeitschrift für Europäisches Privatrecht (ZEuP*), 29(2), S. 227-271.

Jin, Zhiwei; Cao, Juan; Zhang, Yongdong und Luo, Jiebo (2016): News verification by exploiting conflicting social viewpoints in microblogs. *Proceedings of the AAAI conference on artificial intelligence,* 30(1). doi: 10.1609/aaai.v30i1.10382.

Jung, Laura (2023) Schutz der Demokratie durch inhaltsneutrale Regulierung digitaler Medien, *Die Öffentliche Verwaltung (DÖV)*, 76(4), S. 141-150.

Jünger, Jakob und Gärtner, Chantal (November 2020): Datenanalyse von Rechtsverstoßenden Inhalten in Gruppen und Kanälen von Messengerdiensten am Beispiel Telegram. Durchgeführt von der Universität Greifswald. Düsseldorf: Landesanstalt für Medien NRW.

Jünger, Jakob und Gärtner, Chantal (März 2021): Die Verbreitung und Vernetzung Problembehafteter Inhalte auf Telegram. Düsseldorf: Landesanstalt für Medien NRW.

Kalbhenn, Jan (2022): Medien- und wettbewerbsrechtliche Regulierung von Messenger-Diensten. *Zeitschrift für Urheber- und Medienrecht (ZUM)*, 66(4), S. 266-277.

Klimpel, Lena (1. Mai 2021): Wie Politikerinnen im Netz diskreditiert werden. URL: https://www.tagesschau.de/faktenfinder/geschlechtsspezifische-desinformation-101.html.

Kühling, Jürgen (2021): Die Verantwortung der Medienintermediäre für die demokratische Diskursvielfalt. Algorithmenregulierung für Facebook, Twitter & Co.?, *Juristen Zeitung (JZ)*, 76(6), S. 529-530.

Kuhlmann, Simone/Trute, Hans-Heinrich (2022): Die Regulierung von Desinformationen und rechtswidrigen Inhalten nach dem neuen Digital Services Act, *Zeitschrift für das gesamte Sicherheitsrecht* (GSZ), 5(3), 115-123.

Kuß, Christian und Lehmann, Daniel (2021): Digital Services Act – Entwurf eines einheitlichen Rechtsrahmens für die EU-Digitalwirtschaft. *Der Betrieb (DB)*, 74(12), S. 605-610.

Kwon, Sejeong; Cha, Meeyoung; Jung, Kyomin; Chen, Wei und Wang, Yajun (2013): Prominent features of rumor propagation in online social media. *2013 IEEE 13th international conference on data mining,* S.1103-1108. doi: 10.1109/ICDM.2013.61.

Lazer, David; Baum, Matthew; Benkler, Yochai; Berinsky, Adam; Greenhill, Kelly; Menczer, Filippo; Metzger, Miriam; Nyhan, Brendan; Pennycook, Gordon; Rothschild, David; Schudson, Michael; Sloman, Steven; Sunstein, Cass; Thorson, Emily; Watts, Duncan und Zittrain, Jonathan (2018): The science of fake news. *Science*, 359, S. 1094-1096. doi:10.1126/science.aao2998.

Löber, Lena (2022): Der Forschungsdatenzugang nach dem neuen Art. 40 DSA, *Zeitschrift für Datenschutz Aktuell (ZD-Aktuell)*, 01420.

Meßmer, Anna-Katharina und Degeling, Martin (2023): *Auditing Recommender Systems – Putting the DSA into practice with a risk-scenario-based approach*. Berlin: Stiftung Neue Verantwortung.

Pennycook, Gordon; Epstein, Ziv; Mosleh, Mohsen; Arechar, Antonio A., Eckles, Dean und Rand, David G. (2021). Shifting attention to accuracy can reduce misinformation online. *Nature*, 592(7855), S.590-595. doi: 10.1038/s41586-021-03344-2.

Rau, Jan; Kero, Sandra; Hofmann, Vincent; Dinar, Christina; Heldt, Amélie Pia (2022): *Rechtsextreme Online-Kommunikation in Krisenzeiten. Herausforderungen und Interventionsmöglichkeiten aus Sicht der Rechtsextremismus- und Platform-Governance-Forschung*. Hamburg: Leibniz-Institut für Medienforschung/Hans-Bredow-Institut.

Regionales Informationszentrum der Vereinten Nationen (UNRIC): *UN und Partner fordern Länder auf "Infodemie" zu bekämpfen*. URL: https://unric.org/de/24092020-infodemie/.

Roßnagel, Alexander (2019): Artikel 6 Datenschutz-Grundverordnung. In: Simitis, Spiros; Hornung, Gerrit und Spiecker genannt Döhmann, Indra (Hrsg.), *Kommentar Datenschutzrecht*. Baden-Baden: Nomos.

Setz, Tahireh (2022): Desinformation in Messenger-Diensten und Hybrid-Medien – Sind NetzDG und MStV geeignete Blaupausen für die EU? In: Bernzen, Anna K; Grisse Oliveira, Karina und Kaesling, Katharina (Hrsg.): *Immaterialgüter und Medien im Binnenmarkt*. Baden-Baden: Nomos.

Shu, Kai; Wang, Suhang und Liu, Huan (2018): Understanding user profiles on social media for fake news detection. *2018 IEEE conference on multimedia information processing and retrieval (MIPR)*, S.430-435. doi: 10.1109/MIPR.2018.00092

Shu, Kai; Bernard, Russell H. und Liu, Huan (2019): Studying fake news via network analysis: detection and mitigation. *Emerging research challenges and opportunities in computational social network analysis and mining*, S.43-65. doi: 10.1007/978-3-319-94105-9_3.

Spindler, Gerald (2021): Der Vorschlag für ein neues Haftungsregime für Internetprovider – EU-Digital Services Act. *Gewerblicher Rechtsschutz und Urheberrecht (GRUR)*, 123(5), S. 653-662.

Telegram: Fragen und Antworten (FAQ). URL: https://telegram.org/faq/de.

Vosoughi, Soroush; Roy, Deb und Aral, Sinan (2018): The spread of true and false news online. *science*, 359(6380), S.1146-1151. doi: 10.1126/science.aap9559.

Wu, Ke; Yang, Song und Zhu, Kenny Q. (2015): False rumors detection on sina weibo by propagation structures. *2015 IEEE 31st international conference on data engineering,* S. 651-662. doi: 10.1109/ICDE.2015.7113322.

Zeit Online (21. Mär. 2022): *Brasiliens oberstes Gericht nimmt Telegram-Sperrung zurück*. URL: https://www.zeit.de/politik/ausland/2022-03/telegram-messenger-sperrung-brasilien-aufhebung

Zhou, Xinyi und Zafarani, Reza (2019): Network-based fake news detection: A pattern-driven approach. *ACM SIGKDD explorations newsletter*, 21(2), S.48-60. doi:10.1145/3373464.3373473.

Zhou, Xinyi und Zafarani, Reza (2020): A survey of fake news: Fundamental theories, detection methods, and opportunities. *ACM Computing Surveys*, 53(5), S.1-40. doi:10.1145/3395046.

Teil V: Technische Unterstützung beim Daten- und Identitätsmanagement

Die Vision eines Personal Information Management-System (PIMS) durch automatisierte Datenschutzselbstauskunft

Sebastian Wilhelm, Dietmar Jakob, Armin Gerl und Sascha Schiegg

Zusammenfassung

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) und der Novelierung des Bundesdatenschutzgesetzes (BDSG) wurden Regelungen zum Schutz *personenbezogener Daten (pbD)* verstärkt und in einem europäischen Framework implementiert. Dies beinhaltet ein gestärktes Recht auf Auskunft über *pbD*, das jeder betroffenen Person mindestens einmal jährlich die Möglichkeit gibt, eine *Datenschutzselbstauskunft (DSA)* bei der datenverarbeitenden Stelle anzufordern (vgl. Art. 12-15 DSGVO). Die Umsetzung dieser Rechte stellt jedoch Herausforderungen für beide Seiten, Betroffene und Datenverarbeitende, dar.

Um diese Herausforderungen zu überwinden, wird in diesem Artikel ein zweiteiliges Framework eines *Personal Information Management Systems (PIMS)* vorgestellt. Dieses System soll sowohl Betroffenen als auch Datenverarbeitenden dabei helfen, *DSA-Auskünfte* anzufordern bzw. zu bearbeiten. Ein sogenanntes *Monitoring Tool for Personal Data (MoP)* unterstützt Betroffene dabei, DSA-Anfragen automatisiert zu stellen und die Datenkopien zu interpretieren. Ein Komplementärsystem namens *Tool for automated Data Self-Disclosure Request Processing (TaP)* hilft den Datenhaltenden, *DSA-Anfragen* voll-/teilautomatisch zu beantworten.

Zusammenfassend zielt das Framework auf die Wahrung der informationellen Selbstbestimmung der Bürger:innen durch eine erleichterte Anforderung einer *DSA* sowie eine ökonomischere Bearbeitung solcher Ersuchen seitens der Datenhaltenden ab.

1 Motivation und Problemstellung

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) und der Novelierung des Bundesdatenschutzgesetzes (BDSG) wurden die Regelungen zum Schutz von *personenbezogenen Daten (pbD)* gestärkt, indem insbesondere die Betroffenenrechte weiter präzisiert wurden. Dies betrifft

unter anderem spezifizierte Regelungen zur Informations- und Transparenzpflicht (Art. 12-15 DSGVO) sowie Regelungen zur Berichtigung und Löschung, Einschränkung der Verarbeitung, Mitteilungspflicht und Datenübertragbarkeit (Art. 16-20 DSGVO). Bei der Wahrnehmung der Betroffenenrechte nach den Art. 16-20 DSGVO bzw. §§ 32-37 BDSG ergeben sich jedoch Herausforderungen für die Bürger:innen (van Ooijen und Vrabec 2018; Petrlic 2019). Im Fokus dieses Aufsatzes steht insbesondere das Recht auf Auskunft nach Art. 15 DSGVO bzw. § 34 BDSG. Nach diesen Bestimmungen haben Betroffene das Recht, eine Bestätigung darüber zu erhalten, ob *pbD* verarbeitet werden. Wenn dies der Fall ist, haben Betroffene ein Recht auf Auskunft über diese *pbD* und ergänzende Informationen darüber, mit der sog. *Datenschutz-Selbstauskunft (DSA)*. Für die betroffene Person stellen sich hier u. a. folgende Fragen: Wie und in welcher Form muss eine *DSA* angefordert werden, welche Inhalte muss diese enthalten, wie oft kann eine *DSA* angefordert werden und in welcher Form hat das datenverarbeitende Unternehmen bzw. die datenverarbeitende Organisation (im Folgenden als *Datenhaltende (DH)* bezeichnet) die Datenkopien bereitzustellen.

Im Gegensatz dazu ergeben sich für die *DH* Fragen nach der eindeutigen Identität der anfragenden Person (Petrlic 2019), in welcher Form und Frist die Auskunft zu erteilen ist, ob die Anfrage begründet ist, welche Rechte Dritter beachtet werden müssen und welche Rechtsfolgen eine Unterlassung oder unvollständige Auskunft nach sich ziehen (DSK - Datenschutzkonferenz 2017). Die wesentlichen Probleme bei der Erstellung von *DSA-Anfragen*, sowohl bei den Betroffenen als auch bei den *DH*, kann in nachfolgende drei Problemklassen zusammengefasst werden:

- *Problemklasse A: Hemmnisse bei der Erstellung von DSA-Anfragen*
  Bürger:innen müssen sich zunächst einmal daran erinnern, bei welchen *DH* potenziell Daten zur eigenen Person vorhanden sein könnten. Durch eine zunehmend datengetriebene Lebenswelt wird dies für die Bürger:innen jedoch zunehmend unüberschaubarer. Wurden die relevanten *DH* identifizieren, müssen die Bürger:innen die *DSA-Anfrage* formulieren und den *DH* mitteilen (schriftlich oder mündlich). Dabei müssen sich Bürger:innen entscheiden, ob sie konkret von Ihrem Recht gem. Art. 15 oder gem. Art. 20 DSGVO Gebrauch machen möchten (Heinemann und Straub 2019). Wenngleich es dazu zwar zahlreiche Formulierungshilfen gibt, stellt dies für die Bürger:innen eine deutliche Hemmschwelle dar, da sich zusätzlicher Aufwand in Form mit der aktiven Beschäftigung mit

den persönlichen Rechten, der Erstellung der Anfrage und dem Stellen der Anfrage manifestiert (Buchmann und Eichhorn 2019).

- *Problemklasse B: Komplexer Prozess zur Bearbeitung einer DSA-Anfrage bei den DH*
  Die Bearbeitung von *DSA-Anfragen* ist für *DH* ein komplexer Sachverhalt, da die *pbD* i. d. R. dezentral in verteilten (IT-)Systemen gespeichert werden, wodurch eine isolierte Bereitstellung einzelner Datensätze nicht ohne weiteres möglich ist (Geminn 2020). Hierbei müssen die in Informationssystemen abgelegten Daten einer Person eindeutig zugeordnet und dabei auch Verbindungen zu weiteren Personen des Datums beachtet werden. Abhängig von der Natur des digitalen Mediums birgt dies unterschiedliche Herausforderungen. So kann zum Beispiel auf einem digitalen Bild eine Personengruppe abgebildet sein, welche mehreren Personen zugeordnet werden kann bzw. auch hierbei Abgrenzungen geschaffen werden müssen. Bei Daten eines sozialen Netzwerks sind die Daten, welche eine Relation zwischen zwei Personen bilden inhärent mehreren Personen zuzuordnen. Eine Anschrift oder Adresse kann ggf. mehreren Personen zugeordnet sein. Man muss hier weiterhin unterscheiden zwischen strukturiert abgelegten Daten (z. B. in einer Datenbank) und unstrukturiert abgelegten Daten (z. B. verteilt in einem oder mehreren Text-Dokumenten in mehreren Ordnern auf mehreren PCs und Servern abgelegt), wodurch sich eine umfangreiche Komplexität ergeben kann.
  Zu berücksichtigen sind zudem Daten, die zwar strukturiert, aber nicht digital vorliegen. Diese Daten sind im Vergleich zu digitalen strukturierten Daten in Informationssystemen oder Datenbanken mit einem, um einen erheblichen Faktor größeren Aufwand zu sichten, zu erheben und an den Anfragenden zu melden. Aus Sicht der Autoren stellt dies insbesondere kleine und mittelständische Unternehmen, die häufig keine dedizierten Ressourcen hierfür aufbringen können, vor eine erhebliche Herausforderung.
  Eine weitere Herausforderung im Rahmen der Bearbeitung von *DSA-Anfragen* ergibt sich in der Identitätsprüfung der anfragenden Person (Petrlic 2019; Buchmann und Eichhorn 2019), sowie in der sicheren Übermittlung der Datenkopie.
- *Problemklasse C: Schwierigkeiten bei der Interpretation der Datenkopien*
  Bürger:innen die eine Datenkopie von einem *DH* erhalten haben, müssen diese Informationen zu interpretieren wissen. Eine erste Hürde, um die Datenkopie zu interpretieren, ist das Öffnen der Datei, wobei das

Dateiformat eine essenzielle Rolle darstellt. Der Gesetzgeber sieht zwar vor, dass die Datenkopie in einem „gängigen elektronischen Format" (Art. 15 Abs. 3, S. 3 DSGVO) zur Verfügung gestellt werden muss, dies wird jedoch nicht näher spezifiziert. *DH* können also Daten in einem (branchenüblichen) Format bereitstellen (z. B. .sql, .indd). Nicht jede betroffene Person verfügt jedoch über Mittel, um diese Dateien öffnen zu können, wodurch erhebliche Probleme verursacht werden. Die Fragestellung sollte hierbei ebenfalls beachten, dass die übermittelten Daten sowohl vom Menschen als auch von der Maschine verarbeitbar sind. Hiermit möchten wir darauf hinweisen, dass auch eine Bilddatei (.jpeg) als gängiges elektronisches Format gelten kann, jedoch ein Screenshot (im .jpeg-Format) von Datenbankeinträgen sicherlich nicht ein angemessenes Format zur Übertragung dieser Daten ist, auch wenn sie vom Menschen leicht zu öffnen, lesen und interpretieren sind. Ein besseres Format zur Übertragung wäre in Form einer, durch frei zugängliche Software, zu verarbeitendes Tabellendokument.

Eine zweite Hürde für die Bürger:innen bei der Interpretation der Datenkopien stellt die Bewertung der Daten selbst dar. Die Bürger:innen müssen einschätzen, inwieweit beispielsweise die Zwecke der ursprünglichen Datenerhebung noch vorliegen, oder ob ggf. eine Löschung oder Berichtigung der Daten sinnvoll ist (Heinemann und Straub 2019). Nur dadurch können die Bürger:innen informierte Entscheidungen treffen, wie sie mit den Ergebnissen der Abfrage weiter umgehen möchten, um gegebenenfalls von weiteren ihrer persönlichen Datenschutzrechte Gebrauch zu nehmen.

Weiterhin ist zu beachten, dass durch die uneinheitliche Art der Datenkopien, auch ein Vergleich verschiedener *DH* untereinander für die Bürger:innen schwierig ist. So kann durch die unterschiedliche Bezeichnung der Datenfelder und Datenkategorien, da sie z. B. aus unterschiedlichen Informationssystemen stammen, ein Abgleich dieser nicht oder nur erschwert erfolgen. Würden die Datenfelder und Datenkategorien eine einheitliche Semantik besitzen, so könnten diese leichter verglichen werden und möglicherweise Datenflüsse zwischen verschiedenen *DH* nachvollziehbar gemacht werden.

Um diesen Problemklassen zu begegnen, stellen wir in diesem Aufsatz ein Konzept für ein *PIMS-Framework* mit zwei Hauptkomponenten vor. Mithilfe des Frameworks kann auf Betroffenenseite das Recht auf Auskunft durch Automatisierung vereinfacht werden, indem Bürger:innen dabei un-

terstützt werden, potenziell relevante *DH* zu identifizieren, bei welchen Daten zur eigenen Person potenziell vorhanden sein könnten. Bei diesen *DH* kann dann mithilfe des Frameworks eine *DSA-Anfrage*, in einem regelmäßigen Zyklus (z. B. jährlich), automatisiert elektronisch angefragt werden. Auf Seiten der *DH* kann die Anfrage mithilfe des Frameworks automatisiert entgegengenommen werden und an die Verantwortlichen weitergeleitet bzw. sogar vollautomatisiert beantwortet werden. Dies inkludiert neben der Erstellung der Datenkopie selbst, auch die Verifizierung der anfragenden Personen und die sichere/verschlüsselte Übertragung der Datenkopie. Die Datenkopie kann anschließend in standardisierter Form aufbereitet und verschlüsselt an die betroffene Person übermittelt werden. Daraufhin kann die Datenkopie bei der betroffenen Person automatisiert entschlüsselt und für den/die Bürger:in verständlich, visuell aufbereitet werden. Somit können die Hemmnisse bei der Erstellung von *DSA-Anfragen* bei den Bürger:innen und die Schwierigkeiten bei der Interpretation reduziert werden.

Mithilfe des vorgestellten Lösungsansatzes können zudem zeit- und kostenaufwändige Vorgänge zur Bearbeitung von *DSA-Anfragen* automatisiert und für beide Beteiligte (Betroffene und *DH*) effizient und auf einfache Art und Weise abgewickelt werden. Dieses übergreifende Informationssystem ermöglicht ein intuitives Datenselbstmanagement auf Betroffenenseite und stellt einen Kontrollmechanismus in Bezug zu Vollständigkeit und Rechtssicherheit auf Seiten der *DH* dar.

Zusammenfassend zielt das vorgestellte *PIMS-Framework* auf die Wahrung der informationellen Selbstbestimmung der Bürger:innen durch eine erhebliche Vereinfachung zur Anforderung einer *DSA*, sowie einer ökonomischen Bearbeitung solcher Ersuchen seitens der *DH* ab. Zudem leistet der Ansatz damit einen gewinnbringenden Beitrag zur Wahrung der Grundrechte zur Selbstbestimmung einerseits, und der Wahrung der marktwirtschaftlichen Interessen andererseits.

Der Aufsatz ist wie folgt aufgebaut: Zunächst zeigen wir in Abschn. 2 die Auswirkungen der eben genannten Problemklassen in der Praxis, indem wir eine beispielhaft durchgeführte *DSA-Anfrage* vorstellen und die Probleme bei der Bearbeitung darlegen. Anschließend gehen wir in Abschn. 3 auf die generellen Herausforderungen bei der Bearbeitung von *DSA-Anfrage* aus technischer Perspektive ein. In Abschn. 4 beleuchten wir verwandte Arbeiten und bestehende Lösungsansätze zur Umsetzung von *DSA-Anfragen*. Den von uns vorgeschlagenen Lösungsansatz zur Adressierung der genannten Problemklassen, bestehend aus einem Framework mit zwei

Hauptkomponenten, präsentieren wir in Abschn. 5 und diskutieren den Ansatz in Abschn. 6. Der Aufsatz endet mit einer Zusammenfassung und einem Ausblick in Abschn. 7.

2 Anwendungsfall aus der Praxis

Um die in Abschn. 1 aufgeführten Problemklassen, insbesondere seitens der *DH*, zu untermauern, haben wir im Rahmen dieses Aufsatzes exemplarisch eine *DSA-Anfrag*e an eine Behörde gestellt. Die Anfrage erfolgte per E-Mail. Auf den Forschungshintergrund der Anfrage wurde dabei zunächst nicht hingewiesen, um eine neutrale bzw. übliche Bearbeitung der Anfrage zu garantieren.

Als erste Reaktion auf unsere *DSA-Anfrage* bat die verantwortliche Person der Behörde, die Anfrage einzuschränken, um den Aufwand bei der Bearbeitung zu reduzieren. Anschließend forderte die Behörde eine Verifikation der Identität der anfragenden Person. Dazu sollte ein Scan des Personalausweises übermittelt werden. Es wurde betont, dass nicht-wesentliche Merkmale (z. B. Bild, Personalausweisnummer, Gültigkeitsdatum) geschwärzt werden dürften. Im Forschungsfeld der Informatik, insbesondere im Fachbereich der Informationssicherheit, werden zumeist jegliche Angriffszenarien bedacht, um sie proaktiv zu mitigieren und somit das Risiko einer zukünftigen Gefährdungslage zu minimieren. Unter diesem Gesichtspunkt, ist diese Art der Identifikation als unzureichend einzustufen, da sich mit der Methodik theoretisch jeder, der einen Scan des Personalausweises besitzt oder fälschen kann, sich als eine Person identifizieren und somit eine Datenkopie anfordern könnte. Wir möchten hiermit aufzeigen, dass es sich hier um ein mögliches Problem in der Methodik handelt, jedoch davon abgrenzen, dass diese mögliche Schwäche grundsätzlich ausgenutzt wird.

Einige Tage nach der Identifizierung erfolgte die Übermittlung einer Datenkopie. Diese Datenkopie wurde passwortgeschützt/verschlüsselt per E-Mail übermittelt. Die Übermittlung des Passwortes erfolgte per SMS. Die SMS ging an diejenige Handynummer die ursprünglich beim Stellen der *DSA-Anfrage* angegeben wurde. Mit dieser Maßnahme kann sichergestellt werden, dass neben der Person, welche die *DSA-Anfrage* gestellt hat, niemand die Datenkopie einsehen kann (*Man-in-the-Middle-Angriff*). Aufgrund der unzureichenden Identitätsprüfung im Vorfeld ist jedoch nicht sichergestellt, dass es sich bei der anfragenden Person, auch um die betroffene Person handelt.

Bei einer inhaltlichen Überprüfung der Datenkopie fiel auf, dass die Daten in verschiedenen Formaten vorlagen. Teilweise wurden Screenshots einer internen Software als Bild übermittelt, teilweise CSV-Dateien. Die Semantik der Dateien, insbesondere der CSV-Dateien ist jedoch nur begrenzt interpretierbar; eine Erläuterung dazu fehlte.

Die Vollständigkeit der übermittelten Datenkopie können wir nicht bewerten. Es fällt jedoch auf, dass auch Daten über Personen enthalten sind, die nicht der anfragenden Person entsprachen (siehe Abb. 1). Es wurden also auch (personenbezogene) Daten von Dritten übermittelt.

Eine Nachfrage im Nachgang zur Anfrage bei der verantwortlichen Person der Behörde zeigte, dass die Behörde erheblichen zeitlichen Aufwand zur Bearbeitung einer entsprechenden Anfrage betreiben musste. So seien sechs Personen über mehrere Tage in die Bearbeitung der *DSA-Anfrage* involviert gewesen.

Die exemplarische Anfrage zeigt bereits deutlich die Existenz der Problemklassen in der Praxis (insb. Problemklasse B und C).

Wohingegen viele große Technologie-Konzerne wie Facebook, Google oder Amazon automatisierte Methoden entwickelt haben, um *DSA-Anfragen* zu bearbeiten, haben andere *DH* – insb. KMUs oder Behörden – regelmäßig Probleme mit der Bearbeitung solcher Anfragen. Somit ergibt sich die Notwendigkeit und der Bedarf, die Prozesse zur Stellung und Beantwortung von *DSA-Anfragen* zu unterstützen.

In dieser vorgestellten Arbeit wird die Unterstützung mit Hilfe von bewährten Technologien in einem *PIMS-Framework* vorgeschlagen, wobei aber auch organisatorische Mittel zur Verbesserung der Prozesse gewählt werden können. Aus Sicht der Autoren bieten aber insbesondere technologische Ansätze erhebliche Vorteile für die Automatisierung und damit Reduktion des Aufwands in allen Prozessschritten.

previous_hospitalizations

previous	previoushospitalization	previoushospitalization	previousnos	previoushospital	previoushospitalization	previoushospitalization	previoushospitalization
id	uuid	changedate	isolated	hospitalization_id	description	hospitalizationreason	otherhospitalizationreason
2533	TEZQT6-2SKPTV-WHDFB5	2021-01-04 12:51:25.437		2464			
8068	XJWIBJ-KLNQHD-LEMNAK	2021-01-19 09:19:54.009	YES	7999	[redacted] liegt auf der Station 1 in Isolation		
9308	WYPKKX-QPTVO4-XGYZP5	2021-01-20 14:03:01.929	YES	5356			
5030	TFUMHK-IXZSSA5-BLSNPZ	2021-01-20 14:22:36.827		3511	hat Lungenentzündung, keine Beatmung, nur Sauerstoff, Arzt sagt sie kann bald nach Hause		
10820	VQFAHQ-H2GOXK-UUVKFE	2021-01-22 10:53:18.866	UNKNOWN	10757			
12007	UMVB7A-O2VFMH-2XKEMA	2021-01-24 09:54:46.428		11731			
12269	UFPJ3X-Y2ET5O-4BKJLW	2021-01-24 13:09:56.421	UNKNOWN	12237	befindet sich in der Neurologie		
13154	TAHKJG-APNHK-G5GUX2	2021-01-26 10:57:30.156	YES	12775	[redacted] 26.01.2021 Einzelzimmer auf Station 5 - nur eine Untersuchung - Bauchsonographie - ansonsten nur Essensvergabe mit Vollschutz		
14452	WD3DPH-WRJQ6U-6HKRAI	2021-01-27 11:20:24.324	YES	12796	Wegen Atemluftbeschwerden eingeliefert		
15727	SYRAXR-CSJYJO-23DIDO	2021-01-28 15:28:35.98	YES	8926	Wird Beatmet		
27482	QRYVF4-67BQZG-XRYCCA	2021-02-14 10:38:56.986	YES	27345	Atemnot, Fieber		
27606	UOJITX-CZ6MIF-DBUEVF-K	2021-02-15 08:51:15.288	YES	27770	Index liegt im KH [redacted]		
35220	VY5PTZ-LYVCY7-YKEHEA	2021-02-23 09:01:42.178	YES	21483			
35311	QTGNMV-PPH6IU-SJPOCB	2021-02-23 09:45:28.31	YES	24476			
38684	XNWB4X-CGK47R-JQ4TXZ	2021-02-26 10:19:10.179		38697	Wurde lt. Info des Patienten gleich nach der Testung im KH [redacted] ins KH [redacted] verlegt.		
69018	QWAD2B-ON6OQS-UK5DBA	2021-03-23 07:36:08.84		53598			
69024	TELJ5X-WKKFV2-SPCYDA	2021-03-23 07:39:00.208	YES	64937		OTHER	Gefäßstörung
70449	UWJKCY-5BRMPS-VWZYTA	2021-03-23 14:55:51.451	NO	70388		OTHER	Bösartiger Tumor an der Blase
71571	XJCKRJ-MVAOOU-4MPPUA	2021-03-24 13:35:53.389	YES	70388		OTHER	OP an der Prostata
77606	RXZHFJ-AHH5R7-4NDEVC	2021-03-29 08:59:49.82	YES	67270		REPORTED_DISEASE	
116988	UJE5SM-FTMUY4-EYW2BA	2021-04-17 11:03:58.487	YES	102416		OTHER	
117104	WYTAFN-H76AJQ-27CNJB	2021-04-17 11:46:40.039	YES	106744		OTHER	Wasser im Körper,
117162	QAIQNF-7TALXU-NXGLIA	2021-04-17 12:06:00.098		116203	Patientin war vom [redacted] 2021 im Krankenhaus [redacted] stationär auf der Inneren Station	OTHER	rapide AZ verschlechterung
118586	TASG2I-W6AQHB-PFANZH	2021-04-18 10:40:19.597	YES	100677		OTHER	Verdacht auf Bandscheibenvorfall
128144	VFTUR-EEU8NO-YITY4K	2021-04-22 11:42:14.776	UNKNOWN	125830		OTHER	Schwäche, Appetitlosigkeit
131764	UM8HMC-WOVG5I-2MHPIK	2021-04-24 09:17:03.096	YES	81887		REPORTED_DISEASE	
132097	TSVZI5-DETPYQ-LTCJP7	2021-04-24 10:29:37.546	YES	65842		OTHER	Offene Füße
132523	VBXCZR-VZCS47-V2GFJE	2021-04-24 12:28:40.49	YES	102448		REPORTED_DISEASE	
144041	W5RMXO-USU45C-HDYRK	2021-05-01 14:21:31.384		144632			

Abb. 1. Auszug aus einer übermittelten Datei der Datenkopie mit unklarer Semantik sowie Daten von Personen, welche nicht der anfragenden Person entsprechen. Schwärzungen durch die Autoren.

3. Herausforderungen in der praktischen IT-Umsetzung

Globalisierung, Big-Data-Ansätze und Cloud-Technologien verändern das Konzept der klassischen Datenverarbeitung in einzelnen voneinander getrennten Systemen. Der historische Ansatz einzelner Akteure, die dezentral pbD beinhalten, z. B. eine Arztpraxis, ist längst zu einem multinational verknüpften, zentralem System verschmolzen, in dem Daten wie eine Ware gehandelt, zwischen erhebenden Stellen verknüpft und darauf aufbauend analysiert werden können. Um beim Beispiel der Arztpraxis zu bleiben, wäre die Zusammenführung der dezentral vorgehaltenen Daten in eine zentrale Patientendatenbank einer bundesweit agierenden Krankenversicherung technologisch denkbar. Um die Bürger:innen vor dieser unüberblickbaren Datensammlung zu schützen und ihnen Handhabe zur Verwirklichung ihres Rechts auf informationelle Selbstbestimmung zu geben, instanziierte der Gesetzgeber Betroffenenrechte, die jedem Individuum zustehen (Hintze and El Emam 2018). Diese Individualrechte beeinflussen, welche Anforderungen an Software gestellt werden, die diese gespeicherten Daten verarbeitet.

Anhand einfacher Prozesse kann gezeigt werden, welche Problemstellungen sich in der Informatik durch die Anforderungen des Gesetzgebers entwickeln. Ein erstes Beispiel ist die Sicherung von Daten zum Schutz vor Informationsverlust bei technischen Störungen. Beruft sich ein Individuum auf sein Betroffenenrecht zur vollständigen Löschung seiner Daten, kann dies zwar im Operativsystem zeitnah erfolgen, die Datensicherung müsste jedoch ebenfalls aktualisiert werden, da sonst eine Wiederherstellung der Daten gleich gesetzt werden kann mit einer Revidierung des Löschvorgangs. Dies stört sich mit dem Ziel, eine Datensicherung so sicher wie möglich abgespalten vom Operativsystem zu betreiben. Gleichzeitig werden Sicherungen zur Speichereffizienz oft komprimiert und inkrementell aufgebaut. Da Datenpunkte somit voneinander abhängen, müssen spezielle Prozesse eingesetzt werden, um Verkettungen nicht zu zerstören, was einen allgemeineren Datenverlust zur Folge hätte.

Um die Herausgabe, Korrektur oder sonstige Verwendung von pbD eines Individuums zu autorisieren, muss sich dieses als betroffene Person zuletzt genannter pbD ausweisen. In einem Fernabwicklungsverfahren, wie dem hier beschriebenen, stellt dies den/die Sachbearbeiter:in vor ein Problem, da die betroffene Person und dessen Ausweismedium nicht direkt in Person validiert werden kann, ohne erheblichen Aufwand zu verursachen. Ein üblicherweise genutztes Verfahren ist das Übermitteln einer Personalaus-

weis-Kopie (siehe Abschn. 2). Dieses Verfahren ist jedoch hoch problematisch, da die besonders zu schützenden Daten des Personalausweises dann unkontrolliert in Umlauf gebracht werden und der Empfänger zudem nicht verifizieren kann, dass die versendende Person nicht auf sonstigem Wege an die Kopie gelangt ist. Ein vom Gesetzgeber vorgeschlagenes Verfahren stellt der digitale Personalausweis dar.

Datenverbindungen bzw. deren zugrundeliegenden Protokolle sind offene Transportkanäle, wie zum Beispiel TCP oder UDP, die von allen übermittelnden Zwischenstellen im Internet mitgelesen, also abgehört und manipuliert werden können. Um die Integrität einer übermittelten Nachricht sicherzustellen, wird auf Transportverschlüsselung gesetzt, d. h. die Information wird vom Versender mit einer vorher von beiden Seiten vereinbarten Chiffre kodiert und dann vom Empfänger mit diesem dekodiert. Nutzende kennen dies vor allem aus Anwendungsbereichen wie Online-Banking oder VPN-Verbindungen. Eine Veränderung der Nachricht von Zwischenstellen würde die Chiffrierung brechen. Der Empfänger wüsste, dass der Information nicht mehr zu vertrauen ist. Dieses Verfahren nennt sich auch symmetrische Verschlüsselung, da beide Seiten dieselbe Chiffre verwenden. Um die Chiffre zwischen zwei sich nicht vorher kennenden Parteien auszutauschen, wird typischerweise asymmetrische Verschlüsselung zum Einsatz kommen. Dabei erzeugt eine Seite ein Schlüsselpaar, das besondere Eigenschaften aufweist. Ein Schlüssel, der sog. *Private Key*, darf nur dem Aussteller bekannt sein. Der andere Schlüssel, der sog. *Public Key*, kann vom Aussteller herausgegeben werden. Ein mit dem *Public Key* verschlüsseltes Objekt ist nur noch durch den *Private Key* wiederherstellbar (Simmons 1979). Um die Vertrauenswürdigkeit des Ausstellers zu verifizieren, setzt man zumeist voraus, dass eine der beiden Seiten sich von einer allgemein anerkannten Stelle zertifizieren lässt. Im Internet übernehmen diese Aufgabe Zertifizierungsstellen (Aas et al. 2019). Um nicht auf private Zertifizierungsstellen angewiesen zu sein, gäbe es auch die Möglichkeit, sich mittels des digitalen Personalausweises zu autorisieren und somit indirekt die Zertifizierung durch den Bund zu verwenden. Der *Public Key* kann dann an den *DH* gesendet werden. Der *DH* kann die herauszugebenden Informationen mit dem *Public Key* verschlüsseln und theoretisch sogar über ungeschützte Transportkanäle versenden, da nur noch der Anfragende die Informationen entschlüsseln kann. Hierdurch ist sichergestellt, dass nach erfolgter Verschlüsselung nur noch die anfragende Person selbst ihre zur Verfügung gestellten Daten lesen kann und keine etwaige Zwischenstelle

(vgl. *Man-in-the-Middle* Angriff Szenarien (Callegati, Cerroni, and Ramilli 2009)) einen Nutzen daraus ziehen kann.

Um die Sicherheit der Authentifizierung eines im Internet veröffentlichten Systems zu verstärken, wird zunehmend auf einen zweiten Faktor als Erweiterung zum herkömmlichen Passwortverfahren gesetzt (*Zwei-Faktor-Authentifizierung* bzw. *Multi-Faktor-Authentifizierung* (Dasgupta, Roy, and Nag 2017)). Dabei muss der/die Nutzer:in im Besitz eines zuvor registrierten zweiten Geräts (z. B. Smartphone), einer Empfangsmöglichkeit (z. B. Telefon) oder eines Dateischlüssels (z. B. USB-Stick) sein, um sich nach Eingabe des Passworts zu autorisieren. Da dieser zweite Faktor vorab vom Nutzenden registriert wird, ist ausgeschlossen, dass ein Angreifer aus der Ferne Zugang erhält, wenn er, entweder durch Ausprobieren von Kombinationen oder eines sonstigen Abhandenkommens, etwa durch Phishing, in Besitz des Passworts gelangt.

Auch der schon erwähnte digitale Personalausweis verwendet die oben beschriebenen Verfahren (Bundesamt für Sicherheit in der Informationstechnik 2018). Der Personalausweis selbst ist mit einem Sicherheitschip versehen, der mittels *Near Field Communication (NFC)* abgefragt werden kann. Da diese Technologie in vielen heute gängigen Smartphones integriert ist, können Nutzer:innen mit ihrem Ausweis interagieren, ohne zusätzliche Geräte beschaffen zu müssen. Der Chip ist, ähnlich dem einer Bankkarte, mit einem, hier sechs-stelligen, PIN geschützt. Nur Personen, die Kenntnis vom persönlich zu setzenden PIN haben, können die auf dem Chip hinterlegten Informationen abrufen. Dadurch ergibt sich ein Zwei-Faktor-Autorisierungssystem, da zusätzlich zum physischen Merkmal – der Karte – auch das Wissensmerkmal – die PIN – bereitgestellt werden muss. Mit beiden in Kombination kann eine Software, die mittels NFC mit dem Personalausweis kommuniziert, sich gegenüber eines vom Bund betriebenen eID-Servers ausweisen. Der eID-Server bestätigt einer anfragenden Partei daraufhin die Validität der Person. Man spricht auch von einer vertrauten Drittpartei, einer *Trusted Third Party (T3P)*, in diesem Fall dem Betreiber des eID-Servers, gleichgestellt mit der Bundesdruckerei, deren Erzeugnisse sonst anhand des Drucks einzigartiger Schutzmerkmale vertrauenswürdig erscheinen (vgl. Verordnung (EU) 2019/1157 des Europäischen Parlaments und des Rates vom 20. Juni 2019). Weitere Daten wie Name, Vorname, Adresse usw. können dann vom Personalausweis über den eID-Server an die Drittpartei übermittelt werden. Die Übermittlung der Information durch den eID-Server ist mittels Transportverschlüsselung geschützt. Der eID-Server weist sich durch das Zertifikat einer anerkannten

Zertifizierungsstelle aus. Zur Verwendung des eID-Servers muss sich eine Drittpartei zuvor registrieren lassen. Durch eine Überprüfung wird sichergestellt, dass Daten nicht an Drittparteien abfließen, die den Bürger:innen unter dem Vorspielen falscher Tatsachen zur Herausgabe der Informationen auf ihrem digitalen Ausweis drängen. Die von den Nutzer:innen des Systems verwendete Applikation kann vor Autorisierung am eID-Server darstellen, wer die Informationen mit welchem Detailgrad zugesandt bekommt.

4. Verwandte Arbeiten

Der Schutz der Privatsphäre sowie das Recht auf informationelle Selbstbestimmung durch die Regelungen der DSGVO wird in der wissenschaftlichen Literatur mehrfach diskutiert. Die Beiträge beschäftigen sich mit einem Vergleich von Datenschutzerklärungen vor und nach dem Inkrafttreten der DSGVO (Zaeem and Barber 2021), mit der Gültigkeit von Einwilligungen zu Verarbeitung von *pbD* (Sinclair and Jamal 2021) oder mit dem Datenschutz-Paradoxon (Dienlin, Masur, and Trepte 2021; Barth and de Jong 2017). Andere Arbeiten beschreiben die Vorteile und Nachteile der Einhaltung der DSGVO für die *DH*, (Këllezi 2021; Kröger, Lutz, and Ullrich 2021) oder beschäftigen sich mit der Frage, ob die DSGVO die Kontrolle der Verbraucher:innen über *pbD* aus einer Verhaltensperspektive verbessert (van Ooijen and Vrabec 2018).

Die Literatur-Recherche konnte nur wenige Beiträge identifizieren, die sich vorrangig mit der Wahrung der Betroffenenrechte durch die Einforderung einer *DSA* nach Art. 15 DSGVO befassen. Diese Bestimmung gestattet Einzelpersonen die Kontrolle über ihre *pbD* im Rahmen ihres Auskunftsrechts, zur Offenlegung aller gespeicherten *pbD* und deren Verarbeitung (di Martino et al. 2022). Buchmann und Eichhorn (2019) vertreten die Meinung, dass gerade der Art. 15 DSGVO von zentraler, datenschutzrechtlicher Bedeutung für Kund:innen von Online-Unternehmen istKlicken oder tippen Sie hier, um Text einzugeben.. Dabei können jedoch Probleme auftreten.

Nach Geminn (2020) hängt das Recht auf Auskunft, bezogen auf seine Zielerreichung wesentlich von zwei Faktoren ab: (1) Die betroffene Person muss wissen, an wen sie ein Auskunftsersuchen richten kann, und (2) die ihr gegenüber bereitgestellten Informationen müssen für sie verständlich und nützlich seinKlicken oder tippen Sie hier, um Text einzugeben.. Heine-

mann und Straub (2019) argumentieren, dass sich die Betroffenen daran erinnern müssen, welche *DH* ihre Daten (unter welchem Erlaubnistatbestand) verarbeiten. Schließlich müssen sie entscheiden, ob sie konkret von ihrem Recht gem. Art. 15 oder gem. Art. 20 DSGVO Gebrauch machenKlicken oder tippen Sie hier, um Text einzugeben.. Wie die Beiträge zeigen, ergeben sich bereits auf der Seite der Bürger:innen Probleme bei der Umsetzung des Art. 15 DSGVO. Aber auch auf der Seite der *DH* sind Schwierigkeiten in der Umsetzung dieser Vorschrift beobachtbar (Buchmann and Eichhorn 2019).

Für die *DH* stellt ein Auskunftsersuchen einen erheblichen wirtschaftlichen Aufwand dar. Buchmann und Eichhorn (2019) vermuten, dass *DH* durch komplizierte Prozesse oder aufwändige Identitätsprüfungen deshalb versuchen, ihre Kund:innen von Auskunftsersuchen abzubringen. Speziell die Form der Darstellung der gespeicherten *pbD* scheint, nach einigen Autor:innen, den *DH* Schwierigkeiten zu bereiten.

Erhebliche Unsicherheiten für die Bürger:innen bestehen, insbesondere bezogen auf die Reichweite des Rechts auf Erhalt einer Kopie aus Art. 15 Abs. 3 DSGVO. Umstritten sind sowohl die Stellung des Rechts auf Erhalt einer Kopie als auch Inhalte und Reichweite, nicht zuletzt, weil die Verordnung selbst zu all diesen Aspekten schweigt – von der Möglichkeit der Erhebung eines angemessenen Entgelts für weitere Kopien und der Pflicht zur Bereitstellung in einem gängigen elektronischen Format bei elektronischer Antragstellung abgesehen (Geminn 2020). In einer Studie von Bowyer u.a. (2022) mit zehn Teilnehmenden, in der jede Person vier bis fünf *DSA-Anfragen* stellte, wurde beobachtet, dass die erhaltenen Daten in frustrierenden Formaten, darunter Screenshots, Ausdrucke oder Dateien, die mit Akronymen übersät waren, an Betroffene übermittelt wurden. Die Daten waren zu technisch, um sie zu verstehen und die Informationen waren nicht verwendbar. Des Weiteren kamen die Autor:innen zu dem Ergebnis, dass die Qualität der erhaltenen Informationen unvollständig, ungenau, unbrauchbar und als nicht nützlich von den Studienteilnehmenden beurteilt wurdenKlicken oder tippen Sie hier, um Text einzugeben..

Zu ähnlichen Ergebnissen kommen Kroeger, Lutz und Ullrich (2021). in ihrer Studie, in der sie *DSA-Anfragen* an Anbieter von 225 beliebten mobilen Apps versandten. Die von den Anbietern übermittelten Informationen enthielten Formatierungsfehler, in einigen Fällen bestanden die Daten sogar aus einem kontinuierlichen Block alphanumerischer Zeichen ohne Überschriften, Leerzeichen und Zeilenumbrüche und waren damit unbrauchbar. In den meisten Fällen wurden *pbD* in Anhängen in ver-

schiedenen Dateiformaten (nämlich .pdf, .html, .json, .csv, .jpeg, .png, .docx und .txt) und als Klartext im E-Mail-Text bereitgestellt. Buchmann und Eichhorn (2019) stellten in ihrer Studie fest, dass von insgesamt 14 angefragten *DH*, nur sieben vollständige Auskünfte erteilten. Die Autor:innen berichten zudem von wenig datenschutzfreundlichen Identitätsprüfungen. Des Weiteren stellen sie fest, dass auf Nachfragen bei unvollständigen Informationen von den *DH* keine Rückmeldungen mehr erfolgten

Die dargestellten Probleme im Zusammenhang mit der Anforderung einer *DSA* durch die betroffene Person einerseits, sowie die Bearbeitung durch die *DH* andererseits, verlangen nach Lösungen. Bowyer u.a. (2022) schlagen diesbezüglich vor, den Betroffenen Zusammenfassungen über die gespeicherten *pbD* zur Verfügung zu stellen, damit diese einen Überblick über vorhandene Daten bekommenKlicken oder tippen Sie hier, um Text einzugeben.. Nach Geminn (2020) fehlen standardisierte Formatvorgaben seitens des Gesetzgebers und eine speziell für die Betroffenen erstellte digitale Akte", in der alle gespeicherten Informationen ersichtlich" sindKlicken oder tippen Sie hier, um Text einzugeben.. Dashboards könnten nach Heinemann und Straub (2019) auch ein Mittel sein, um den Betroffenen alle relevanten Informationen übersichtlich und gebündelt zu präsentierenKlicken oder tippen Sie hier, um Text einzugeben.. Buchmann und Eichhorn (2019) verweisen auf die Internetseite *selbstauskunft.net*, auf der *DSA* auch für Laien auf einfache Art und Weise angefordert werden könnenKlicken oder tippen Sie hier, um Text einzugeben..

Zusammenfassend ist festzustellen, dass speziell die Ausübung des Betroffenenrechts nach Art. 15 DSGVO in der wissenschaftlichen Literatur noch weitestgehend unerforscht ist, und deshalb Handlungsbedarf besteht.

5. Lösungsansatz MoP und TaP

Um Bürger:innen die Möglichkeit zu geben, eine automatisierte *DSA-Anfrage* an Unternehmen, Behörden oder sonstige *DH* zu stellen, schlagen wir ein Framework mit zwei Hauptkomponenten vor. Auf der Seite der Betroffenen ist es erforderlich, Unterstützung bei der Erstellung und Übermittlung von *DSA-Anfragen* zu bieten, hierfür schlagen wir das Modul *Monitoring Tool for Personal Data (MoP)* für Betroffene vor (siehe Abschn. 5.1). Um die Anfragen auf Seite des *DH* aufzunehmen und (teil-)automatisiert zu verarbeiten, schlagen wir das Modul für die Datenverantwortlichen *Tool for automated Data Self-Disclosure Request Processing (TaP)* vor (siehe

Abschn. 5.2). Durch die Zusammenarbeit beider Komponenten können die beschriebenen Problemklassen systematisch und holistisch gelöst werden. So unterstützt das *MoP* dabei die Hemmnisse bei der Erstellung von DSA-Anfragen bei Bürger:innen abzubauen (Problemklasse A), da eine zentrale Schnittstelle für die Erstellung ebendieser sowie für die Rückübermittlung der pbD geschaffen wird. Das *TaP* fokussiert sich hierbei insbesondere auf die Lösung der Problemklasse B, wobei die Beantwortung der *DSA-Anfragen* unterstützt wird. Um einen Lösungsansatz für die Problemklasse C zu bieten, sind beide Komponenten *MoP* und *TaP* notwendig, bzw. die Schaffung der Schnittstellen dieser. So kann die Interpretation von Datenkopien für die Bürger:innen durch technische Systeme am besten unterstützt werden, falls einheitliche Austauschformate im „gängigen elektronischen Format" (Art. 15 Abs. 3 S.3 DSGVO) genutzt werden. Diese müssen von *MoP* bereitgestellt werden und von *TaP* verarbeitet werden. Weiterhin kann basierend auf einheitlichen Formaten mit *TaP* eine Aufbereitung und Visualisierung vorgenommen werden, damit die Bürger:innen die übermittelte Antwort auf ihre *DSA-Anfrage* transparent und verständlich präsentiert bekommen. Dadurch können nur durch das Zusammenspiel, der im Folgenden weiter präzisierten Komponenten des vorgeschlagenen Frameworks, die Problemklassen adressiert werden.

Schematisch ist das Gesamtsystem in Abb. 2 dargestellt.

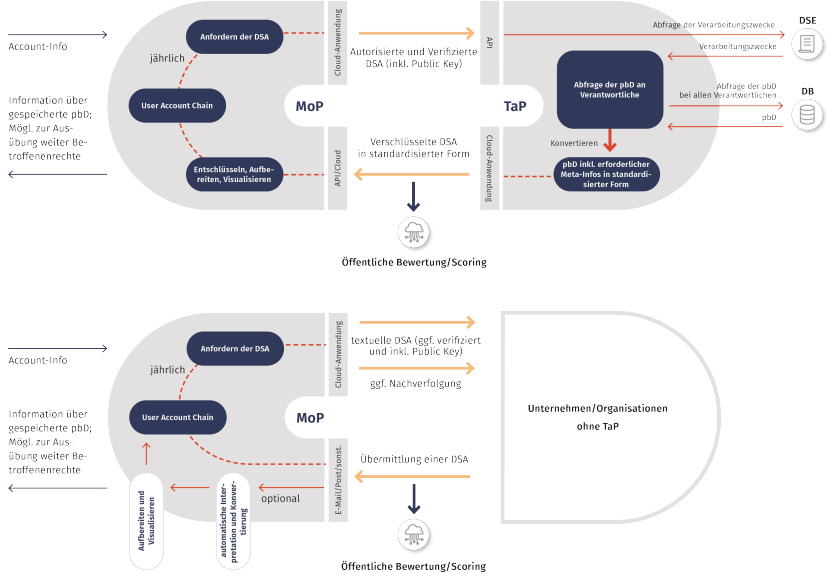

Abb. 2. Schematische Darstellung des PIMS bestehend aus der Bürger:innen-Einheit Monitoring Tool for Personal Data (MoP) und dem Komplementärsystem für DH: Tool for automated Data Self-Disclosure Request Processing (TaP).

5.1 Monitoring Tool for Personal Data (MoP)

Mithilfe des sog. *Monitoring Tool for Personal Data (MoP)* werden Bürger:innen dabei unterstützt, automatisiert *DSA-Anfragen* zu erstellen und diese an die *DH* zu übermitteln. Ferner werden die Bürger:innen unterstützt, die erhaltenen Rückantworten zu interpretieren.

Für die Bürger:innen ist die zentrale Schnittstelle mit *MoP* eine sog. *User Account Chain*. Diese *User Account Chain* enthält, angelehnt an einen digitalen Schlüsselbund, Informationen darüber, bei welchen *DH* potenziell Daten zur Person vorhanden sein könnten. Der Aufbau dieser *User Account Chain* ist zentraler Baustein für die Funktionalität. Es muss hierbei ein geeignetes Datenschema entwickelt werden, welches definiert, welche Informationen gespeichert werden. Unter anderem sollten hierbei in Anlehnung an die DSGVO, insbesondere die benötigten transparenten Informationen für die Informationspflicht – Datengruppen, Zwecke, Löschfristen, etc. –

(vgl. Art. 12 - 14 DSGVO) und ggf. weitere notwendige Daten und Informationen zur Inanspruchnahme der Betroffenenrechte, insbesondere für die *Datenschutz-Selbstauskunft (DSA)* in diesem Kontext. Als Grundlage für eine derartige *User Account Chain* können *Domain Specific Languages*, insbesondere *Privacy Languages*, dienen. Beispiele hierfür sind die *Layered Privacy Language* mit Framework, welches sich darauf fokussiert, Datenschutzerklärungen für Maschinen und Menschen lesbar strukturiert abzubilden und mit Hilfe des Frameworks die Möglichkeit bietet, automatisiert Techniken zur Anonymisierung und Pseudonymisierung auf die Rohdaten zweckgebunden anzuwenden, oder das *SPECIAL* Projekt, welches ebenfalls einen Vorschlag für die Abbildung von Datenschutzerklärungen erstellt hat und Forschung zur Visualisierung dieser durchgeführt hat. Weiterhin bietet das im *World Wide Web Consortium (W3C)* vorgeschlagene *Data Privacy Vocabulary (DPV)* Ansatzpunkte zur semantischen Vereinheitlichung der Terminologie im Datenschutzbereich. Somit können *Privacy Languages* als Basis für ein Austauschformat dienen und semantische Standards wie das *Data Privacy Vocabulary (DPV)* verwendet werden, um die Inhalte mehrheitlich einheitlich zu standardisieren. Auf Basis dieser Technologien kann die *User Account Chain* aufgebaut werden, um möglichst viele Informationen zu speichern, welche *DH* potenziell Daten zu einer Person besitzen könnten; u. a. auch Daten von *DH*, bei denen die Person keinen direkten User Account besitzt (z. B. Akte in der Arztpraxis; Kund:innenkartei in der Kfz-Werkstatt). Die Informationen zu den potenziellen *DH* aus der *User Account Chain* kann als Grundlage dienen, um periodisch (i. d. R. jährlich) eine *DSA-Anfrage* an den *DH* zu stellen. Dabei können folgende zwei Fälle betrachtet werden:

- *DSA-Anfrage an DH, die TaP verwenden:* Die *DH* erhalten eine voll-elektronische und standardisierte *DSA-Anfrage* über die in *TaP* dafür vorgesehene API. Die anfragende Person wird durch *MoP* direkt verifiziert (z. B. mithilfe des digitalen Personalausweises). Ferner wird durch *MoP* ein *Public-Key* der *DSA-Anfrage* hinzugefügt, welcher später zur sicheren Übertragung der *pbD* dient.
- *DSA-Anfrage an DH, die TaP nicht verwenden:* Die *DH* erhalten über *MoP* automatisiert eine textuelle *DSA* per E-Mail. *MoP* überwacht anschließend auf Seiten der Bürger:innen den Bearbeitungsstand der *DSA-Anfrage*. Sollten *DH* innerhalb der (gesetzlichen) Frist die *DSA-Anfrage* nicht beantworten, so wird dies durch *MoP* moniert.

Unabhängig von der Art der *DSA-Anfrage* werden die Rückantworten der *DH* anschließend wieder in *MoP* gesammelt. Bei *DH*, die *TaP* verwenden, werden die Daten durch die *DH* direkt in das *MoP* System mittels einer Schnittstelle übertragen. Bei *DH* ohne *TaP* kann weiterhin eine manuelle Import-Funktion für die Bürger:innen bereitgestellt werden, bei denen die relevanten Informationen mittels einer Benutzeroberfläche eingegeben werden können und damit manuell übertragen werden. Die automatisierte Übertragung mittels einer Schnittstelle ist hier jedoch zu präferieren, da sie weniger fehleranfällig ist und auch keinen zusätzlichen Aufwand verursacht. Die *pbD* werden anschließend durch *MoP* intelligent aufbereitet, visualisiert und in der *User Account Chain* abgespeichert. Bei der Visualisierung sind hierbei unterschiedliche Ansichten für den Nutzenden denkbar, z. B. können die Informationen nach unterschiedlichen Prioritäten dargestellt werden, wie eine Ansicht, welche basierend auf den Verarbeitungszwecken die Daten gruppiert, während eine andere Ansicht basierend auf den Datengruppen gruppiert. Weitere Filter- und Sortierfunktionen sind durch eine derartige elektronische Aufbereitung und Visualisierung ebenfalls realisierbar, um Mehrwerte zu generieren.

Das Konzept könnte weiterhin mit den persönlichen Datenschutz-Präferenzen der Nutzenden erweitert werden, bei denen diese Präferenzen in einem strukturierten Format persistent gespeichert werden und mit den im *MoP* vorhandenen Daten verglichen werden. Dadurch könnten die Nutzenden, mit Hilfe einer geeigneten Darstellung, eigene datenschutzbezogene Verhalten, anhand zuvor definierter Präferenzen, reflektieren und ggf. anpassen.

5.2 Tool for automated Data Self-Disclosure Request Processing (TaP)

Mithilfe des sog. *Tool for automated Data Self-Disclosure Request Processing (TaP)* werden *DH* dabei unterstützt, voll-/teil-automatisiert *DSA-Anfragen* systematisch zu bearbeiten. *TaP* ist als Komplementärsystem zu *MoP* zu betrachten und setzt voraus, dass die *DSA-Anfragen* auch über ein *MoP* bzw. einer Schnittstelle gestellt werden.

Eine Schlüsselinnovation von *TaP* ist, dass die durch *MoP* erzeugten *DSA-Anfragen* direkt über eine API entgegengenommen werden. Durch eine Standardisierung des Anfrageformats und einer direkten, bereits in der Anfrage integrierten Autorisierung der Anfrage, ermöglicht *TaP* eine voll-automatisierte Bearbeitung der *DSA-Anfrage*.

Zur Umsetzung der Autorisierung sollte hierbei auf bestehende und bewährte Standards zurückgegriffen werden; auch die Nutzung des elektronischen Personalausweises zur Authentifizierung wäre als geeignetes Verfahren möglich.

Zur inhaltlichen Bearbeitung der *DSA-Anfrage* und zur Erstellung der Datenkopie sind mehrere Prozessschritte notwendig. Zunächst identifiziert *TaP* aus *elektronischen Datenschutzerklärungen (DSE)* alle für die Bearbeitung der *DSA-Anfrage* relevanten Verarbeitungszwecke. Anschließend werden die *pbD* aus allen Verarbeitungszwecken abgefragt. Dies kann entweder voll-automatisiert durchgeführt werden, z. B. durch eine Abfrage aus bestehenden Datenbanken, oder manuell durch eine Abfrage bei den jeweiligen Verfahrensverantwortlichen. Eine Herausforderung bei der voll-automatisierten Abfrage aus Datenquellen besteht darin, dass eine Verknüpfung bzw. ein Mapping zwischen den abgefragten Daten und Datengruppen zu den einzelnen Daten (in der Terminologie von Datenbanken: *Attributen*) der Datenquellen hergestellt werden muss. Dadurch ergibt sich ebenfalls eine Klassifizierung der Daten in den Datenquellen in persönliche Daten und nicht persönliche Daten, wobei man aus Sicht der Informatik persönliche Daten noch weiter differenzieren würde in (Sweeney 2002; Venkataramanan and Shriram 2016):

- *Explizite Identifikatoren (EI)* definiert Attribute, die Bürger:innen eindeutig identifizieren. Beispiele für *EI* sind die Reisepass-ID, der Name oder die Sozialversicherungsnummer, wobei der Name auch für die folgende Datenkategorie zugeordnet werden könnte, da Namen bei großen Datensammlungen möglicherweise nicht eindeutig sind und zusätzliche Attribute zur eindeutigen Identifizierung eines/einer Benutzer:in erfordern.
- *Quasi-Identifikatoren (QI)* definiert Attribute, die in Kombination mit anderen *QI* die Identifizierung eines Benutzers ermöglichen. Beispiele für *QI* sind IP-Adresse, Postleitzahl, Geburtstag, Alter, Geschlecht und andere demografische Informationen. *QI* sind oft öffentlich zugänglich, zum Beispiel in Telefonbüchern, Wählerdatenbanken oder anderen Quellen.
- *Sensitive Data (SD)* definiert Attribute, die für Benutzer:innen vertraulich sind. Beispiele für *SD*-Attribute sind Gesundheitsdaten, Finanzdaten oder andere Informationen, die je nach Zweck nicht mit dem/der Nutzer:in in Verbindung gebracht werden sollten.

- *Non-Sensitive Data (NSD)* definiert Attribute, die weder Benutzer:innen identifizieren noch für Benutzer:innen sensibel sind. Daher sind *NSD*-Attribute alle Attribute, die nicht einer der anderen Datenkategorien *EI*, *QI* oder *SD* zugeordnet werden können und entsprechen nicht persönlichen Daten.

Die Zuordnung der Attribute der Datenquellen zu den Datengruppen, kann in den Datenquellen „*by Design*" durchgeführt werden, oder bei bestehenden Systemen durch den Einsatz von zusätzlicher Middleware umgesetzt werden.

Informationen aus den *DSE*, wie Zweck und Rechtsgrundlage sowie Löschfristen, werden gemeinsam mit den *pbD* aus den unterschiedlichen Verarbeitungszwecken in ein standardisiertes Schema konvertiert, zusammengefasst und mit relevanten Zusatzinformationen, bspw. Hinweisen auf das Beschwerderecht, ergänzt. Als Grundlage für das standardisierte Schema können *Privacy Languages* genutzt werden. Abschließend stellt *TaP* der anfragenden Person über eine Cloud-Schnittstelle von *MoP* verschlüsselt die Daten aus der *DSA* im vereinheitlichten Austauschformat zur Verfügung. Die Bearbeitung der *DSA-Anfrage* ist damit für den *DH* vollständig abgeschlossen.

6. Diskussion

Der vorgeschlagene Lösungsansatz mit *Monitoring Tool for Personal Data (MoP)* und *Tool for automated Data Self-Disclosure Request Processing (TaP),* als zwei Komponenten eines *PIMS-Frameworks*, ist ein technischer Ansatz, um die beschriebenen Problemklassen zu bewältigen.

Um die Problemklasse A, die Hemmnisse der Bürger:innen bei der Erstellung von *DSA-Anfragen*, entgegenzuwirken wird insbesondere das *MoP* eingesetzt, das Informationen über mögliche *DH* mit vorliegenden *pbD* verwaltet und es vereinfacht, Anfragen zu stellen. Das vorgestellte *MoP* fokussiert sich hierbei nur auf einen Aspekt der Problemklasse, dem Stellen von *DH-Anfragen*, jedoch können diese Hemmnisse auch mit weiteren Mitteln abgebaut werden. So könnten die Bürger:innen bereits bei der Registrierung bei Web-Anwendungen durch eine geeignete Benutzeroberfläche bzw. Visualisierung darüber informiert werden, welche ihrer Daten für welche Zwecke und Verarbeiter genutzt werden (Tran-Van, Anciaux, and Pucheral 2017). Weiterhin kann den Bürger:innen dargestellt werden, welche Risiken mit der Verwendung einer Web-Anwendung einhergehen

(Yee 2007). Damit können vor der Nutzung der Daten Hemmnisse der Bürger:innen abgebaut werden, bzw. diese ausreichend informiert werden, wobei das vorgestellte *MoP* komplementär als Werkzeug nach der Verarbeitung der Daten genutzt werden kann.

Um der Problemklasse B, die Komplexität des Prozesses zur Bearbeitung von DSA-Anfragen, entgegenzuwirken wird insbesondere das *TaP* eingesetzt, wobei Informationen über gespeicherte *pbD* gehalten werden, und diese strukturiert abgerufen und übermittelt werden können. In diesem Konzept wird die grundlegende Funktionsweise des *TaP* erläutert, jedoch muss auch beachtet werden, dass die technischen Systeme und organisatorischen Maßnahmen der *DH* angemessen gestaltet werden. Die zugrundeliegenden technischen Systeme müssen dahingehend gestaltet sein, dass sie es dem *TaP* ermöglichen, die angemessenen Daten für den Zweck der *DSA-Anfrage* zu erheben, jedoch sollten diese technischen Systeme diese Daten auch grundsätzlich nur an Personen oder Drittsysteme für die Zwecke weitergeben, die in der Datenschutzerklärung festgelegt sind. Hierbei gibt es den Ansatz des *Purpose-based Access Control* (Ji-Won Byun, Bertino, and Li 2005), wobei dieser bereits in verschiedene Datenbanksysteme experimentell integriert wurde (Ji-Wonand Byun and Li 2008; Colombo and Ferrari 2017). Das *TaP* sollte nicht nur als Werkzeug zur Verbesserung des Datenschutzes für Bürger:innen dienen, sondern auch selbst unter Aspekten der Privatheit (*Privacy by Design*) und Informationssicherheit gestaltet werden. Hierfür wurden außerhalb Europas bereits Richtlinien und Standards geschaffen, wie der *AS 27701 PIMS-Standard*, welcher auf der *ISO/IEC 27001* und *ISO/IEC 27002* aufbaut und den Zweck verfolgt, die Compliance von Unternehmen bezüglich des komplexen Themas Datenschutz zu steigern (Christie 2022).

Neben technischen Standards müssen auch die organisatorischen Maßnahmen des Unternehmens zur Verbesserung des Datenschutzes beachtet werden. Neben der Sensibilisierung des Führungspersonals als auch der Mitarbeitenden, welche mit den Daten und Informationen in ihrer täglichen Arbeit umgehen, müssen insbesondere die Prozesse angemessen gestaltet werden, um Datenschutz und Informationssicherheit zu garantieren, wobei ggf. auch mit unerwarteten Konsequenzen umgegangen werden muss (Parks et al. 2017).

Um der Problemklasse C, den Schwierigkeiten bei der Interpretation der Datenkopien, entgegenzuwirken werden Schnittstellen und strukturierte Datenformate zwischen *MoP* und *TaP* definiert, sowie in *MoP* die übermittelten Daten visuell aufbereitet und präsentiert. Dies umfasst damit einen

technischen Lösungsansatz, wobei auch ethische und juristische Fragestellungen betrachtet werden müssen (Grout 2019; Balthasar and Gerl 2019). So könnten verbindliche Richtlinien für die Übertragung von verschiedene Datenformaten (Daten, welche Texte, Bilder, Audio, etc. repräsentieren) geschaffen werden, welche zum einen eine technische Umsetzung schaffen aber zum anderen auch den Aufwand zur Umsetzung für *DH* minimieren. Hierbei müssen unterschiedliche technologische, ethische, juristische und ökonomische Gesichtspunkte miteinander abgewogen werden.

Zusammenfassend bietet der vorgestellte Lösungsansatz mit *MoP* und *TaP* einen technologischen Lösungsansatz, um *DSA-Anfragen* strukturiert umzusetzen. Weiterhin bietet dieser Lösungsansatz eine Grundlage auf welcher weitere technologische, juristische, ethische und ökonomische Lösungsansätze angewendet werden können, um diesen *PIMS-Ansatz* zu erweitern und zu erforschen.

7. Zusammenfassung und Ausblick

In diesem Aufsatz haben wir uns mit dem Recht auf Auskunft gemäß Art. 15 DSGVO bzw. § 34 BDSG auseinandergesetzt und die Umsetzungsperspektive näher beleuchtet. Dabei haben wir aus der Literatur drei wesentliche Problemklassen identifiziert, die im Zusammenhang mit dem Recht auf Auskunft auftreten können (siehe Abschn. 1 und Abschn. 4). Auf Seite der Bürger:innen sind diese Probleme zum einen, dass Hemmnisse bei der Erstellung von *DSA-Anfragen* existieren (Problemklasse A) und dass die von den *DH* erhaltenen Datenkopien für die Bürger:innen teilweise schwierig zu interpretieren sind (Problemklasse C). Auf der Seite der *DH* ist der Prozess zur Bearbeitung einer *DSA-Anfrage* komplex und zeitaufwändig (Problemklasse B). Die *DH* müssen aus oft historisch gewachsenen IT-Systemen sämtliche *pbD* extrahieren, was eine Herausforderung darstellen kann, da viele IT-Systeme darauf nicht ausgelegt sind (siehe Abschn. 3). Zudem gestaltet sich die eindeutige Identifizierung der anfragenden Person und die sichere Übermittlung der Datenkopien häufig schwierig.

Um die genannten Probleme zu adressieren, stellt dieser Aufsatz ein Framework für ein zweiteiliges *PIMS* vor, welches zum einen Bürger:innen bei der Erstellung von *DSA-Anfragen* sowie bei der Interpretation der Datenkopien unterstützt. Zum anderen erlaubt das vorgestellte Framework, eine (voll-)automatisierte Bearbeitung von *DSA-Anfragen* bei *DH*.

Auf Seiten der Bürger:innen soll ein sogenanntes *Monitoring Tool for Personal Data (MoP)* eingesetzt werden, das Informationen über mögliche *DH* enthält, bei denen *pbD* vorliegen könnten. Das *MoP* fordert periodisch eine *DSA* bei allen potenziell relevanten *DH* ein. Die Antworten/Datenkopien werden dann im *MoP* erfasst und die gespeicherten *pbD* in Bürger:innen-Interesse aufbereitet und visualisiert. Dadurch kann die betroffene Person ein besser informiertes Datenselbstmanagement betreiben und das Grundrecht auf informationelle Selbstbestimmung wird gestärkt.

Auf Seiten der *DH* schlagen wir ein Komplementärsystem namens *Tool for automated Data Self-Disclosure Request Processing (TaP)* vor, dass die *DH* bei der Bearbeitung von *DSA-Anfragen* unterstützt. Mit *TaP* soll es möglich sein, *DSA-Anfragen*, die über *MoP* gestellt werden, (voll-)automatisiert zu bearbeiten. Dabei ist in *TaP* (in Verbindung mit *MoP*) die Identifikation der anfragenden Person und ein Kanal zur sicheren Übermittlung der Datenkopien bereits enthalten. Wird *TaP* in die IT-Systeme des *DH* integriert, kann auch die Datenkopie vollautomatisiert erstellt werden. Ansonsten unterstützt *TaP* den *DH* auf Grundlage von Informationen aus den elektronischen *DSE* bei der Erstellung einer vollständigen und rechtssicheren *DSA*. Mithilfe von *TaP* kann die Erteilung von *DSA* ökonomischer erfolgen.

In künftigen Arbeiten gilt es, ein Teilfunktionsmuster des skizzierten Frameworks zu entwickeln und die Funktionsweise beider Komponenten (*TaP* und *MoP*) praktisch zu evaluieren sowie zu prüfen, welche organisatorischen und personellen Rahmenbedingungen bei der Einführung und Umsetzung dieses Systems zu berücksichtigen sind. Insbesondere die Integration des *TaP* in die bestehenden Systeme der *DH* gilt es dabei genauer zu untersuchen. Ferner soll ein Standard zum Datenaustausch zwischen *MoP* und *TaP* definiert werden.

Für den Einsatz von *MoP* ohne das Komplementärsystem *TaP* , sollte durch den Gesetzgeber zudem das Format der Datenkopien (siehe Art. 15 Abs. 3 S. 3 DSGVO) näher spezifiziert werden.

Literatur

Aas, Josh; Barnes, Richard; Case u. a. (2019): Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web. In: *CSS'19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. New York, NY, USA: ACM, S. 2473-2487. doi: 10.1145/3319535.3363192.

Balthasar, Mandy und Gerl, Armin (2019): Privacy in the toolbox of freedom. In*: 2019 12th CMI Conference on Cybersecurity and Privacy (CMI)*. Kopenhagen: IEEE, S. 1-4. doi: 10.1109/CMI48017.2019.8962146.

Barth, Susanne und de Jong, Menno D.T. (2017): The privacy paradox -Investigating discrepancies between expressed privacy concerns and actual online behavior - A systematic literature review. *Telematics and Informatics*, 34 (7), S. 1038–1058. doi: 10.1016/j.tele.2017.04.013.

Bowyer, Alex; Holt, Jack u.a. (2022): Human-GDPR Interaction: Practical Experiences of Accessing Personal Data. New Orleans, LA, USA: *CHI'22*. doi: 10.48550/ARXIV.2203.05037.

Buchmann, Erik und Eichhorn, Susanne (2019): Auskunftsersuchen nach Art. 15 DSGVO. *Datenschutz und Datensicherheit – DuD*, 43 (2), S. 65–70. doi: 10.1007/s11623-019-1065-y.

Bundesamt für Sicherheit in der Informationstechnik (2018): Technische Richtlinie TR-03127: eID-Karten mit eID- und eSign-Anwendung basierend auf Extended Access Control. Bonn: Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03127/BSI-TR-03127.pdf.

Byun, Ji-Won; Bertino, Elisa und Li, Ninghui (2005): Purpose Based Access Control of Complex Data for Privacy Protection. In: *SACMAT'05: Proceedings of the Tenth ACM Symposium on Access Control Models and Technologies*. New York, NY, USA: Association for Computing Machinery, S. 102-110. doi: 10.1145/1063979.1063998.

Byun, Ji-Won und Li, Ninghui (2008): Purpose based access control for privacy protection in relational database systems. *The VLDB Journal*, 17 (4), S. 603-619. doi: 10.1007/s00778-006-0023-0.

Callegati, Franco; Cerroni, Walter und Ramilli, Marco (2009): Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security & Privacy Magazine*, 7 (1), S. 78–81. doi:10.1109/MSP.2009.12.

Christie, Alec (2022): AS 27701: the PIMS standard you can't afford to ignore. *Privacy Law Bulletin*, 19 (5), S. 92–95. doi: 10.3316/agispt.20220830073173.

Colombo, Pietro und Ferrari, Elena (2017): Enhancing MongoDB with Purpose-Based Access Control. *IEEE Transactions on Dependable and Secure Computing*, 14 (6), S. 591–604. doi: 10.1109/TDSC.2015.2497680.

Dasgupta, Dipankar; Roy, Arunava und Nag, Abhijit (2017): Multi-Factor Authentication. In: *Advances in User Authentication*. Cham: Springer, S. 185-233. doi: 10.1007/978-3-319-58808-7_5.

Dienlin, Tobias; Masur, Philipp K. und Trepte, Sabine (2021): A longitudinal analysis of the privacy paradox. *New Media & Society*, 15 (5), S. 1043-1064. doi: 10.1177/14614448211016316.

DSK - Datenschutzkonferenz (2017): Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO. Kurzpapier Nr. 6. https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf.

Geminn, Christian L. (2020): Betroffenenrechte verbessern. *Datenschutz und Datensicherheit – DuD*, 44 (5), S. 307–11. doi: 10.1007/s11623-020-1273-5.

Grout, Vic (2019): No More Privacy Any More? *Information*, 10 (1), doi: 10.3390/info10010019.

Heinemann, Andreas und Straub, Tobias (2019): Datenschutz muss benutzbar sein. *Datenschutz und Datensicherheit – DuD*, 43 (1), S. 7–12. doi: 10.1007/s11623-019-1052-3.

Hintze, Mike und El Emam, Khaled (2018): Comparing the benefits of pseudonymisation and anonymisation under the GDPR. *Journal of Data Protection & Privacy*, 2 (2), S. 145–58.

Këllezi, Pranvera (2021): Consumer Choice and Consent in Data Protection. Antitrust Chronicle. https://www.competitionpolicyinternational.com/category/antitrust-chronicle.

Kröger, Jacob Leon; Lutz, Otto Hans-Martin und Ullrich, Stefan (2021): The myth of individual control: Mapping the limitations of privacy self-management. *SSRN Electronic Journal*. doi: 10.2139/ssrn.3881776.

Di Martino, Mariano; Meers, Isaac u.a. (2022): Revisiting Identification Issues in GDPR `Right Of Access' Policies: A Technical and Longitudinal Analysis. *Proceedings on Privacy Enhancing Technologies*, 2022 (2), S. 95–113. doi: 10.2478/popets-2022-0037.

Ooijen, I. van und Vrabec, Helena U. (2018): Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, 42 (1), S. 91–107. doi: 10.1007/s10603-018-9399-7.

Parks, Rachida; Xu, Heng; Chu, Chao-Hsien und Lowry, Paul Benjamin (2017): Examining the intended and unintended consequences of organisational privacy safeguards. *European Journal of Information Systems*, 26 (1), S. 37–65. doi: 10.1057/s41303-016-0001-6.

Petrlic, Ronald (2019): Identitätsprüfung bei elektronischen Auskunftsersuchen nach Art. 15 DSGVO. *Datenschutz und Datensicherheit – DuD*, 43 (2), S. 71–75. doi: 10.1007/s11623-019-1066-x.

Simmons, Gustavus J. (1979): Symmetric and Asymmetric Encryption. *ACM Computing Surveys*, 11 (4), S. 305–330. doi: 10.1145/356789.356793.

Sinclair, David und Jamal, Arshad (2021): Does the GDPR Protect UK Consumers from Third Parties Processing Their Personal Data for Secondary Purposes? A Systematic Literature Review. In: *Cybersecurity, Privacy and Freedom Protection in the Connected World*. Cham: Springer. S. 379-394. doi: 10.1007/978-3-030-68534-8_24.

Sweeney, Latanya (2002): k-Anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10 (05), S. 557–570. doi: 10.1142/S0218488502001648.

Tran-Van, Paul; Anciaux, Nicolas und Pucheral, Philippe (2017): SWYSWYK: A Privacy-by-Design Paradigm for Personal Information Management Systems. In: *International Conference on Information Systems Development (ISD)*. Cyprus. https://hal.inria.fr/hal-01675090.

Venkataramanan, Nataraj und Shriram, Ashwin (2016): *Data privacy: principles and practice*. Chapman and Hall/CRC.

Yee, George (2007): Visual Analysis of Privacy Risks in Web Services. In: *IEEE International Conference on Web Services (ICWS 2007)*. S. 671–78. Doi: 10.1109/ICWS.2007.189.

Zaeem, Razieh Nokhbeh und Barber, Suzanne K. (2021): The Effect of the GDPR on Privacy Policies. *ACM Transactions on Management Information Systems*, 12 (1), S. 1–20. doi: 10.1145/3389685.

Privacy Management mit Self-Sovereign Identity: Potenziale zur Erhöhung der informationellen Selbstbestimmung

Gunnar Hempel und Jürgen Anke

Zusammenfassung

Dieser Beitrag zeigt einen Ausblick für ein Privacy Management auf Basis von Self-Sovereign Identity (SSI). Dafür genutzte digitale Brieftaschen (SSI-Wallets) bieten konzeptionelle Eigenschaften, die die Privatheit der Nutzer besser als bisherige Ansätze schützen können und die Selbstbestimmtheit der Nutzer über ihre Daten erhöhen. Diese Verbesserungen entstehen jedoch nicht automatisch. Vielmehr sind ein wertegeleiteter Umgang mit der Technologie und zusätzliche Werkzeuge erforderlich, um diese Potenziale zu nutzen. Die mit dem Ansatz mögliche Neugestaltung der Beziehungen zwischen Nutzer und Serviceanbieter hat einen disruptiven Charakter. Mit Verfahren und Werkzeugen für digitale Interaktionen wie Selective Disclosure, Verifiable Presentations, Zero-Knowledge Proofs, nicht-korrelierbaren Identifikatoren und Filterfunktionen eröffnen SSI-Wallets vollkommen neue Möglichkeiten für die Organisation des Datenmanagements.

1. Einführung

Die Kommerzialisierung von Internet-Diensten und die Verlagerung behördlicher Dienstleistungen schaffen zunehmend eine Verknüpfung von realer und virtueller Identität. Bei so gut wie jedem Online-Angebot wird eine digitale Identität erzeugt und mit Nutzerdaten verknüpft. Der Identitätsnachweis ist für natürliche Personen oft erforderlich, wenn es um Interaktionen mit Staat und Verwaltung geht oder wenn Finanz- und Zahlungsdienstleistungen involviert werden. Für zahlreiche weitere privatwirtschaftliche Dienste werden gleichfalls Identitätsnachweise verlangt. Auf den Identitätsnachweis folgt in den meisten Fällen eine Verarbeitung von Nutzerdaten und Nachweisen. Serviceanbieter haben oftmals ein berechtigtes Interesse daran zu wissen, wer ihre Nutzer sind, und Informationen über ihre Nutzer in möglichst guter Qualität zu verarbeiten, sei es für das Kun-

denbeziehungsmanagement und um Services zu verbessern, um Marketing zu betreiben oder um zusätzliche Wertschöpfung und Mehrwertdienste anzubieten. Nutzer digitaler Dienstleistungen hingegen haben das Recht, die wesentlichen Informationen über die beabsichtigte Verarbeitung zu erfahren, grundsätzlich selbstbestimmt über die Verarbeitung ihrer personenbezogenen Daten zu entscheiden, und müssen prinzipiell nur solche Daten preisgeben die für die Nutzung des Dienstes erforderlich sind.

In der Umsetzung entstehen für die Akteure oftmals rechtlich komplizierte und nicht sauber lösbare Situationen sowie ein unbefriedigendes Handling der technischen und organisatorischen Prozesse. Die Verwendung digitaler Ausweise gibt oft mehr Daten preis als erforderlich. Zudem schafft das Ausfüllen von Onlineformularen und das Erstellen von immer wieder neuen Passwörtern überflüssige Aufwände. Halbdigitale Verfahren, bei denen Dokumente eingescannt oder in Video-Anrufen vorgezeigt werden, sind lästige Zwischenschritte, welche die Customer Journey beeinträchtigen und die Sicherheit der Verarbeitung oftmals herabsetzen. Zahlreiche weitere Szenarien lassen sich hier aufreihen. Die Digitalisierung von Services stellt die beteiligten Akteure immer wieder vor interdisziplinäre Herausforderungen. Dedizierte Ansätze und neue Werkzeuge sind erforderlich, um interessengerechte Lösungen zu schaffen.

Zu beobachten ist indes auf verschiedenen Gebieten, dass sich sowohl die Art und Weise verändert, wie Identitäten verwaltet werden als auch wie der Zugang zu Daten vermittelt wird. Ansätze wie Self-Sovereign Identity ermöglichen eine Transformation von einem isolierten oder föderierten Identitätsmanagement hin zu einem selbstbestimmten Identitätsmanagement. Technische Entwicklungen wie digitale SSI-Wallets können die Speicherung von Nutzerdaten in „Datensilos" zunehmend ersetzen und in ein „On Demand"-Modell überführen.

Damit öffnen sich neue Gestaltungsräume, wie Identitätsnachweise und Authentifizierung, aber auch der Austausch von Daten und die Legitimierung von Datenverarbeitung für Services zukünftig ausgestaltet werden können.

Rückenwind bekommt der SSI-Wallet-Ansatz indes durch die EU-Gesetzgebung und nationale Gesetzgebung, sowie durch gesellschaftliche Entwicklungen. Es ist davon auszugehen, dass Wallets für Nutzer und Dienstanbieter im öffentlichen und privaten Bereich eine zunehmende Rolle spielen werden.

Mit dem vorliegenden Beitrag soll skizziert werden, wie ein durch ein SSI-Wallet unterstütztes Privacy Management aussehen kann und welche

Potentiale dieser Ansatz im Sinne einer Data Governance bietet. Ziel dieser Arbeit ist es überdies aufzuzeigen, welche Themenfelder noch tiefgreifender zu untersuchen sind und an welchen Stellen konkreter Forschungs- und Entwicklungsbedarf besteht. Hierfür wird der Ansatz elaboriert und potentielle Herausforderungen identifiziert.

2. Ansatz und Thesen für ein SSI-Privacy Management

Für die Konzeption eines SSI-gestützten Privacy-Managements wurden drei initiale Fragen vorangestellt: Welche Bestandteile von SSI können zu einem fortschrittlichen Privacy-Management beitragen? Welche potentiellen Auswirkungen und Verbesserungen bietet ein SSI-Privacy-Management für die Selbstbestimmtheit und für eine interessengerechte Datenverarbeitung? Welche Werkzeuge und Maßnahmen sind für die Umsetzung erforderlich?

2.1 Self-Sovereign Identity

Self-Sovereign Identity, bzw. selbstbestimmte Identität, ist ein Ansatz, der es einer Person, einer Organisation oder einer Maschine erlaubt, eine digitale Identität zu erzeugen und selbst, also ohne einen Vermittler oder eine zentrale Partei, zu kontrollieren.[1] Die Identitätsverwaltung mittels SSI-Wallets funktioniert, wie der Name es schon sagt, ähnlich wie eine Brieftasche mit verschiedenen Ausweisen und Dokumenten darin. Je nach Anwendungsfall stellt der Nutzer Identitätsdaten oder auch nur Nachweise über bestimmte Eigenschaften seiner Person über einen verschlüsselten Kanal für einen anfragenden Akteur bzw. Dienstanbieter bereit (s. Abb. 1).[2]

1 *Allen*, The path to self-sovereign identity, 2016.
2 *Anke / Richter*, HMD 2023, S. 261ff.

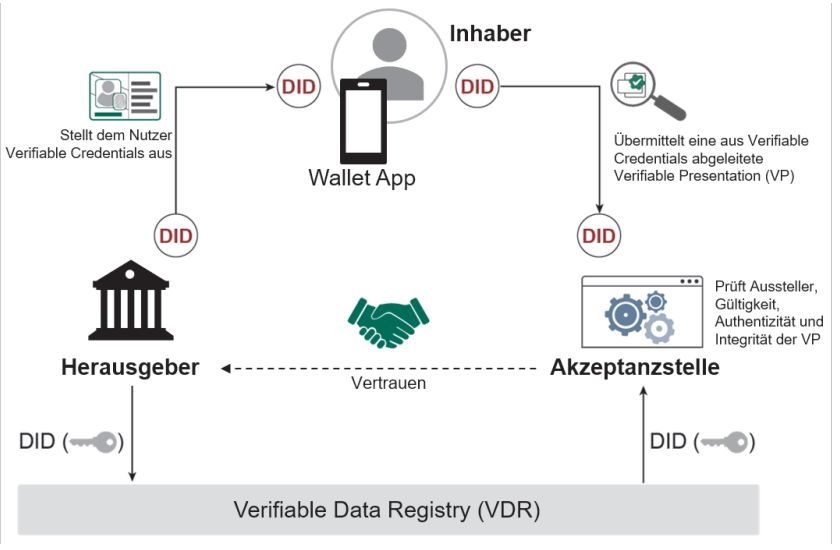

Abb. 1: Architektur von Self-Sovereign Identity Systemen (Quelle: Anke / Richter, HMD 2023, S. 269)

Während die Nutzer durch SSI von einer besseren Transparenz und Selbstbestimmtheit über ihre Daten profitieren, erhalten Dienstanbieter automatisch prüfbare Nachweise zum Nutzer und für die Verarbeitung nachweisbar autorisierte Daten.[3] In Zukunft können so, durch interoperable Nachweise, digitale Ökosysteme entstehen, in denen Kommunikation, Informationsaustausch und Datenverarbeitung einfacher und interessengerechter im Sinne eines Privacy-Managements umgesetzt werden können.

2.2 SSI als Basis für ein wirksames Privacy Management

Die folgende Darstellung zeigt einen Ausblick, wie ein SSI-Privacy-Management und eine Data Governance in einem digitalen Ökosystem neugestaltet werden könnte:

Ein Nutzer wird über eine Sammlung digitaler Nachweise in Form einer digitalen Identität repräsentiert. Die Nachweise werden von vertrauenswürdigen Stellen herausgegeben und vom Nutzer in der Wallet verwaltet. Die Wallet wird in eine technische und organisatorische Infrastruktur einge-

3 *Preukschat / Reed*, Self-sovereign identity, 2021, S. 248f.

bunden, der Nutzer kann darüber digitale Nachweise empfangen, speichern und präsentieren. Bereitgestellt wird die Wallet beispielsweise als Smartphone-App. Die Speicherung der Daten kann auf dem Gerät selbst oder über eine Cloud-Anbindung erfolgen.

Will der Nutzer einen digitalen Service verwenden, wird eine Peer-to-Peer-Verbindung zwischen der SSI-Wallet und dem Service aufgebaut. Dies erfolgt beispielsweise durch das Aufrufen eines Webservices oder Scannen eines QR-Codes. Über die Verbindung können Nutzer und Serviceanbieter Nachweise, Anforderungen und Datensätze empfangen und präsentieren. Beispielsweise können sich Dienstanbieter und Nutzer gegenseitig über Verifiable Credentials (VC) identifizieren, die Nutzungsbedingungen für die Inanspruchnahme des Services sowie für die Verarbeitung der Nutzerdaten (Terms of Use), als auch die Daten selbst durch Verifiable Presentations (VP) austauschen.

Anstatt seine Daten beim Aufrufen eines Services in Webformularen einzugeben oder Nachweise hochzuladen, gibt der Nutzer auf Anfrage die Daten aus seiner Wallet frei und legitimiert die Datenverarbeitung für den angefragten Anwendungsfall. Dabei kann über ein feingranulares Rechtemanagement bestimmt werden, welche Daten im Rahmen der Nutzungsbedingungen verarbeitet werden dürfen.

Diese Neugestaltung erfordert jedoch noch technische Weiterentwicklungen der Wallets und geeigneter Privacy-Werkzeuge, sowie organisatorische Anpassungen der Datenhaltung und Bereitstellung. Wenn solche Mechanismen praktisch einsetzbar sind, besitzen alle Nutzer eine Historie aller Empfänger ihrer Daten, sowie den damit verbundenen Nutzungsbedingungen. Dies ist die Grundlage, um Wallets mit einem mit PIMS (Personal-Information-Management-Service[4], an anderer Stelle auch „Personal Information Management-Systeme“[5]) vergleichbaren Ansatz für das Einwilligungs-Management zu erweitern. Konkret könnten Wallets auf diese Weise die Rechte auf Auskunft, Korrektur und Löschung von Daten nicht nur praktisch nutzbar machen, sondern teilweise automatisieren. Für Dienstanbieter, die Daten empfangen und verarbeiten, entsteht gleichzeitig der Effekt, dass die Herkunft und berechtigte Nutzung von Daten (durch die Signatur des Betroffenen) jederzeit nachgewiesen werden kann. Perspektivisch ist die technische Abbildung von Regelwerken als „Machine-Readable

4 *Stiftung Datenschutz*, Neue Wege bei der Einwilligung im Datenschutz, 2017.
5 *European Data Protection Supervisor*, Personal Information Management-System, 2021.

Governance" ein Weg, um allen Beteiligten in einer Vertrauensdomäne den Umgang mit Nachweisen automatisiert zu gewährleisten.[6]

Der Leitgedanke ist, dass verlässliche Informationen über einen Nutzer mit dem Voranschreiten digitaler Geschäfts- und Servicemodelle für eine datenorientierte Wertschöpfung zunehmend an Bedeutung gewinnen. Die Bereitstellung, Legitimierung und Beweisbarkeit der Informationen muss rechtlichen Anforderungen entsprechen und sollte möglichst interessengerecht und schwer korrumpierbar sein.

Die Reorganisation der Datenhaltung und Bereitstellung hin zu einem „On-Demand"-Modell könnte gewichtige Vorteile für eine interessengerechte Verarbeitung personenbezogener Daten in digitalen Ökosystemen schaffen. In erster Linie betrifft dies datenschutzrechtliche Aspekte wie Transparenz und Selbstbestimmtheit der Verarbeitung, ökonomische Fragen bezüglich der Datenqualität, Kosten für die Datenhaltung und Pflege sowie Aspekte der Accountability und Compliance. Gleichfalls ist denkbar, dass sich durch den Ansatz zum SSI-Privacy-Management auch datenschutzfreundliche Angebote und ökonomische Marktprozesse besser unterstützten lassen.

2.3 Eigenschaften von Technik und Organisation

Die Wirkweise des SSI-Privacy-Managements ist in zwei Perspektiven zu betrachten. Zum einen die technisch-inhärenten Fähigkeiten von SSI für den Schutz der Privatsphäre und zum anderen die daraus abgeleitete Handhabung von personenbezogenen Daten durch Dienstanbieter.

Technische Fähigkeiten von SSI für den Schutz der Privatsphäre

SSI enthält konzeptionelle Merkmale, die Privatsphäre der Nutzer besser als bisherige Ansätze schützen können und die Selbstbestimmung über Daten erhöhen. Für den grundlegenden Umgang mit digitalen Nachweisen sind folgende Mechanismen für den Schutz der Privatsphäre relevant:

- *Vermeidung von Korrelation:* Voraussetzung für den Austausch von Nachweisen ist der Aufbau einer verschlüsselten Peer-to-Peer-Verbindung. Die dabei verwendeten Decentralized Identifiers (DIDs) können für jede Verbindung neu erzeugt werden. Somit ist eine Zusammenfüh-

6 *Hardmann*, Aries RFC 0430, 2020.

rung (Korrelation) von Datensätzen über eine Person aus verschiedenen Organisationen erschwert. Ausgeschlossen ist sie jedoch nicht, da bei Vorliegen ausreichend spezifischer anderer Attribute, eine Korrelation über diese stattfinden kann.

- *Selektive Freigabe*: Zentral für den Datenschutz ist das Konzept der VP. Diese stellen die Antwort der Wallet des Inhabers auf die Anfrage einer Akzeptanzstelle dar. Durch die selektive Freigabe von Attributen entsteht eine Datenminimierung, die ein Privacy Pattern ist.[7] Hierbei ist durch die Anfrage kenntlich zu machen, welche Attribute für den betreffenden Vorgang nach dem Grundsatz der Erforderlichkeit verpflichtend und welche optional sind, damit der Inhaber eine entsprechende Entscheidung treffen kann.
- *Kontrolle*: Der Inhaber der Wallet bekommt nicht nur den Anfragenden angezeigt, sondern auch die Liste der gewünschten Daten in Form einer Liste von Attributen. Nur wenn der Inhaber die Freigabe erteilt, werden die Daten übertragen.
- *Zurechenbarkeit*: Jede VP wird spezifisch auf die jeweilige Anfrage ausgestellt. Damit kann zum einen vermieden werden, dass eine VP an anderer Stelle erneut verwendet wird. Zum anderen kann die Akzeptanzstelle auch kryptografisch beweisen, dass der Inhaber ihr diese Daten bereitgestellt hat.
- *Transparenz*: Die mit verschiedenen Akteuren ausgetauschten Daten werden in einigen Wallets bereits heute in Form einer Historie gespeichert. Damit ist im Gegensatz zum heutigen Umgang mit digitalen Identitäten jederzeit nachvollziehbar, wer wann welche Daten erhalten hat, was die Ausübung von Rechten zur informationellen Selbstbestimmung erleichtert. Dies erfüllt gleichermaßen eine zentrale Forderung des Bundesverfassungsgerichts an die Gesellschafts- und Rechtsordnung, wonach der Bürger mit dem Recht auf informationelle Selbstbestimmung in der Lage sein soll zu beurteilen, wer was wann und bei welcher Gelegenheit über ihn weiß.[8]

Derzeit sind weitere Teilaspekte für SSI in Entwicklung, die für den Schutz der Privatsphäre genutzt werden können. Ein wichtiges Mittel zur weiteren Datenminimierung sind Zero-Knowledge Proofs (ZKP), die kryptografisch überprüfbare Aussagen ohne Offenlegung der zugrundeliegenden Daten möglich machen. Ein häufig bemühtes Beispiel ist die Altersprüfung, die

7 https://privacypatterns.org/patterns/Support-Selective-Disclosure.
8 BVerfGE 65, 1 (43).

gegen einen bestimmten Schwellwert (z. B. 18 oder 21 Jahre) durchführbar ist, ohne das Geburtsdatum der Person offenzulegen. Andere Anwendungsmöglichkeiten wären eine bestimmte Mindestnote in Zeugnissen, Mindestwohndauer in einer Kommune oder schlicht die Existenz eines gültigen Nachweises (z. B. Wohngeldbescheid, Sozialpass, Ticket). Bislang ist noch nicht festgelegt, welche konkreten kryptografischen Verfahren für ZKP in der Praxis Anwendung finden. Allerdings stellen sowohl die eID-Funktion des Personalausweises als auch die geplante EU Digital Identity Wallet entsprechende Funktionen bereit.

Handhabung von personenbezogenen Daten durch Dienstanbieter

Für Dienstanbieter bietet die Nutzung von digitalen Nachweisen mittels SSI folgende Vorteile:

- Die vom Nutzer eingesetzte Technik kann Daten automatisiert bereitstellen, statt sie in ein Formular einzugeben. Damit ist die Erfassung deutlich effizienter und kann anlassbezogen erfolgen, statt eigene Datenbestände zu führen.
- Die gelieferten Daten haben eine hohe Qualität, d. h. sie sind unverfälscht, aktuell und geprüft. Aufwändige Verfahren zur Verifizierung von Daten durch externe Dienste können damit entfallen.
- Die bereitgestellten Daten enthalten kryptografisch prüfbare Einwilligungen für die Verarbeitung der Daten, die für den anfragenden Dienstanbieter ausgestellt wurden. Damit ist es gegenüber Aufsichtsbehörden leichter möglich, die korrekte Handhabung von personenbezogenen Daten zu beweisen.

Offen ist jedoch, ob und in welchem Maße Dienstanbieter SSI verwenden, um die Privatsphäre von Betroffenen zu schützen. Die oben aufgeführten Möglichkeiten stellen lediglich Potenziale dar, die durch die Anwendung des Paradigmas der selbstbestimmten Identitäten entstehen können. Damit diese Potenziale im Sinne der Privatsphäre wirksam werden, müssen Dienstanbieter diese technischen Möglichkeiten auch ausschöpfen. Dies bedeutet konkret:

- Für alle Interaktionen dürfen nur die Daten erfragt werden, die für den jeweiligen Zweck unbedingt erforderlich sind.
- Alle nicht erforderlichen Daten sollten deutlich als optional gekennzeichnet werden, so dass Nutzende frei entscheiden können, ob sie diese teilen

möchten. Hier ergeben sich u. U. Ansätze für Anreize und Kompensationen in Form einer selbstbestimmten Datenökonomie.
- Sobald praktisch einsetzbar, sollten Daten in Form von Zero-Knowledge Proofs abgefragt werden, so dass lediglich ja/nein Aussagen zu bestimmten Sachverhalten anstatt der zugrundeliegenden Daten offengelegt werden müssen.
- Die in den Anfragen vermerkten Nutzungsbedingungen (Terms of Use) sollten einfach verständlich und im Sinne des Nutzenden ausgestaltet sein. Dies betrifft insbesondere die Speicherdauer sowie eventuelle Maßnahmen zur Anonymisierung und Pseudonymisierung für weiterführende Auswertungen wie Marktforschung.
- Schnelle Beantwortung von Anfragen für die Ausübung von Datenschutzrechten, idealerweise automatisiert.
- Die Löschung der Daten nach abgelaufener Aufbewahrungsfrist sollte den Wallets der Nutzer mitgeteilt werden, damit diese ihre Historie aktualisieren können und keine unnötigen Löschanfragen stellen.

Die sich hierbei ergebenden Möglichkeiten und Potentiale sind zwar deutlich erkennbar, stehen jedoch im Widerspruch zur bisherigen Praxis des Umgangs mit Daten. Es stellt sich die Frage, warum Dienstanbieter die von SSI bereitgestellten Fähigkeiten nutzen sollten, um damit die Privatsphäre der Nutzer zu schützen und ihre Machtposition stärken. Hier kommt die Gesetzgebung der EU ins Spiel. Mit der Novellierung der eIDAS-VO sind Regulierungen zur Attributbestätigung über eine European Digital Identity Wallet (EUid-Wallet) in der Planung, die die Souveränität des Nutzers in den Vordergrund stellen soll (vgl. Abschn. 3.2).

Gegenstand der weiteren Forschung muss es sein, die tatsächlichen Anforderungen der Akteure als auch die rechtlichen und technischen Herausforderungen zu untersuchen:

3. Hausforderungen

Für Tragfähigkeit des Privacy-Management-Ansatzes sind sowohl verhaltensökonomische, rechtliche, als auch technische und organisatorische Fragestellungen zu berücksichtigen. Im Folgenden werden wichtige Herausforderungen aus diesen Bereichen benannt und andiskutiert.

3.1 Verhaltensökonomie

Die SSI-Wallet befähigt den Nutzer zur selbstorganisierten und selbstbestimmten Verwaltung der Daten und damit auch zu Transparenz und Steuerung über die Verarbeitungen.

Das selbstbestimmte Verwalten der Daten und der Datenverarbeitungen, sowie die Ausübung der Datenhoheit erfordern ein grundlegendes Verständnis und Fähigkeiten im Hinblick auf Informations- und Telekommunikationstechnologie (IKT). Das Bearbeiten der Interaktionen und das damit verbundene Verwalten von Informationen, von Anfragen und das Erteilen von Einwilligungen schafft Aufwände und stellt erhöhte Anforderungen an den Nutzer. Aus der Verhaltensforschung ist hinreichend bekannt,[9] dass ein Zuwachs an Informationen nicht gleichzeitig einer leichteren Entscheidungsfähigkeit oder zu besseren Entscheidungen beiträgt. Es kann davon ausgegangen werden, dass der Nutzer nach seinen individuellen Fähigkeiten und Interessen bereit ist, eine gewisse Informationsmenge zu erfassen, darüber hinaus jedoch die Informationsaufnahme abbricht. Für Nutzer ist es darüber hinaus eine große Herausforderung, die Sicherheitsaspekte der Technologie einzuschätzen und damit verbundene Risiken, wie durch Datendiebstahl und oder durch Profilbildung, zu bewerten.

Ziel der Technik muss es daher sein, eine Konfigurationsmöglichkeit anzubieten, die den Nutzer dort abholt, wo er sich mit seinen Fähigkeiten und seiner Bereitschaft befindet und ihn von dort aus bestmöglich unterstützt. Die Forschung zu Usable Security und Privacy untersucht und entwickelt auf diesem Gebiet bereits einschlägige Lösungsansätze. So könnte die Interaktions- und Informationsmenge beispielsweise über ein gestuftes Komplexitätsniveau auf die Bedürfnisse des Nutzers angepasst werden. Zu untersuchen wäre, welche Schemata und Methoden für eine solche Stufung geeignet wären, um für den Nutzer einen Mehrwert bei der Interaktion über SSI-Wallets zu bieten.

Grundlegend für die Akzeptanz der Technologie beim Anwender wird es sein, dass dieser einen möglichst unmittelbaren Nutzen aus der Anwendung ziehen kann. Generell bestehen in der Breite bei Anwendern Barrieren für das Anwenden von Neuerungen und das Anpassen an neue Prozesse. Diese Hürde lässt sich möglicherweise überwinden, wenn nicht nur ein positiver Anreiz zu einer theoretischen Verbesserung der Gesamtsituation besteht, sondern wenn möglichst zusätzlich auch ein unmittelbarer Nutzen

9 Weiterführend hierzu: *Roetzel*, Business Research 2019, 479.

für den Anwender entsteht, der als Treiber für die Reorganisation eines Prozesses dient.

Inwieweit Dienstanbieter bereit sind, eine Neuorganisation der Datenhaltung und Bereitstellung zu akzeptieren, dürfte zu einem großen Teil von ökonomischen Aspekten abhängen. Hier wird es darauf ankommen, ob sich Aufwände für die Datenhaltung und Datenpflege sowie Schutz- und Compliance-Maßnahmen reduzieren lassen und inwieweit Verbesserungen für die Datenqualität und für das Kundenbeziehungsmanagement umgesetzt werden können.

Im Hinblick darauf, dass die aktuelle EU-Gesetzgebung mit der Novellierung der eIDAS-VO vorsieht die Mitgliedsstaaten zu verpflichten, eine einheitliche Online- und Offline Identifizierung von Bürgern innerhalb der EU per EUid-Wallet bereitzustellen, lohnt es sich besonders zu analysieren, wie und welche Methoden geeignet sind, den Nutzer dahingehend zu befähigen, Privacy-Risiken einzuschätzen, Rechte wahrzunehmen und durchzusetzen, aber auch einen interessengerechten und wertstiftenden Austausch von Daten und eine Interaktion mit Dienstanbietern zu unterhalten.

3.2 Recht

SSI-Wallets sind ein Instrument, um die Verwaltung digitaler Identitäten in bestimmten Anwendungsszenarien durch Nutzer selbst zu steuern.

Welcher Rechtsnatur eine digitale Identität ist und inwieweit ein Recht auf und an einer solchen besteht, wird an zahlreichen Stellen diskutiert, es soll jedoch im Rahmen der vorliegenden Arbeit nicht vertieft untersucht werden. Zu betrachten sind in erster Linie die datenschutzrechtlichen Perspektiven für den Ansatz des SSI-Privacy-Managements und mögliche Spannungsfelder mit anderen Rechtsgebieten, insbesondere den Vorschriften zur elektronischen Identifizierung und Vertrauensdiensten, sowie den allgemeinen Vorschriften.

Die digitale Identität ist zunächst eine Repräsentation einer Person in der digitalen Informationstechnologie um diese auszuweisen.[10] Sie wird in Prozesse eingebettet und im Geschäftsalltag verwendet, wodurch ihr eine rechtliche Funktion und Geltung zukommt, die mehr und mehr an Bedeu-

10 Weiterführend hierzu *Hornung*, Die digitale Identität, 2005, S. 29f.

tung gewinnt. Soll ein Rechtsgeschäft z. B. im digitalen Raum[11] abgeschlossen werden, ist es in einer Vielzahl der Fälle[12] im Interesse mindestens einer beteiligten Partei, den Geschäftspartner zu identifizieren. Die zivilrechtlichen Vorschriften lassen ein rechtswirksames Handeln auf diesem Wege bis auf Ausnahmen zu. Rechtswirksames Handeln im Behördenverkehr richtet sich nach den einschlägigen Verfahrensvorschriften und ist unter den dortigen Bedingungen möglich. Bedeutung erlangen digitale Identitäten derzeit für die öffentliche Verwaltung besonders im Rahmen des Onlinezugangsgesetzes (OZG), wonach Bund, Länder und Kommunen verpflichtet werden, ihre Verwaltungsleistungen über Verwaltungsportale digital anzubieten.

Die Basis für die Möglichkeit einer vertrauenswürdigen elektronischen Identifizierung und die Nutzung von Vertrauensdiensten wurde durch die Verordnung „(EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“ (eIDAS-VO) geschaffen. Die eIDAS-VO legt Bedingungen fest, unter denen die EU-Mitgliedsstaaten elektronische Identifizierungsmittel und notifizierte elektronische Identifizierungssysteme gegenseitig anerkennen. Nach dem aktuellen Kommissionsvorschlag zur Novellierung der eIDAS-VO[13] wird auch die Umsetzung einer EUid-Wallet geplant.[14] Jeder Mitgliedsstaat der EU soll nach Art. 6a Abs. 1 der Novellierung verpflichtet werden eine EUid-Wallet für natürliche und juristische Personen anzubieten. Die EUid-Wallets sollen dem Nutzer das sichere, transparente und nachvollziehbare Anfordern und Erhalten, Speichern, Auswählen, Kombinieren und Weitergeben der erforderlichen gesetzlichen Personenidentifizierungsdaten und elektronischen Attributsbescheinigungen ermöglichen, um sich online und offline zur Nutzung öffentlicher und privater Online-Dienste zu authentifizieren (Art. 6a Abs. 3a). Sie muss zudem das Unterschreiben mit einer qualifizierten Signatur ermöglichen (Art. 6a Abs. 3b) und insbesondere Schnittstellen für Vertrau-

11 Digitaler Raum ist ein unscharfer Begriff, der sinngemäß für digitale Dienstleistungen und Internetanwendungen steht, vgl.: https://www.bmwk.de/Redaktion/DE/Schlaglichter-der-Wirtschaftspolitik/2021/11/05-im-fokus-digitale-identit%C3%A4ten.html.

12 Nicht betroffen sind z.B. Bargeschäfte des täglichen Lebens.

13 Europäische Kommission, COM (2021) 281 final.

14 Am 10.02.2023 hat die EU Kommission die erste EUID-Toolbox als Grundlage für die eID-Wallet veröffentlicht. URL: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework?utm_source=piano&utm_medium=email&utm_campaign=22038.

ensdiensteanbieter aufweisen, die Attributsbescheinigungen herausgeben (Art. 6a Abs. 4a). Die Attributsbescheinigungen können in verschiedenen technischen Formen, beispielsweise in Form von VC, ausgegeben werden. Neben der hoheitlichen, nationalen Identität sollen auch weitere Nachweise, wie der Führerschein, Hochschulzeugnisse und Bescheinigungen in die EUid-Wallet abgelegt werden können. Durch Art. 12b Abs. 2 werden Unternehmen und Behörden verpflichtet die Verwendung der EUid-Wallet zu akzeptieren, sofern diese auch Dienste erbringen, die eine Online-Identifizierung mit starker Nutzerauthentifizierung erfordern. Ausdrücklich betrifft dies die Anwendungsfelder Verkehr, Energie, Bank- und Finanzdienstleistungen, soziale Sicherheit, Gesundheit, Trinkwasser, Postdienste, digitale Infrastrukturen, Bildung oder Telekommunikation. Darüber hinaus werden neue Anwendungsfelder auch dadurch erschlossen, dass die großen Online-Plattformanbieter dazu verpflichtet werden, für den Zugang zu ihren Online-Diensten die EUid-Wallet für die Nutzer-Authentifizierung zu akzeptieren, (Art. 12b Abs. 3).[15] Es ist daher davon auszugehen, dass Wallets mit digitalen Nachweisen für Bürger und Verwaltung bei der elektronischen Identifizierung in der digitalen Kommunikation eine zunehmende Rolle spielen.

Der elektronische Identitätsnachweis erfolgt durch die Verarbeitung personenbezogener Daten über eine (natürliche) Person, weshalb datenschutzrechtliche Vorschriften zu beachten sind. Die DSGVO schreibt in Art 5 Abs. 1 die Grundsätze der Verarbeitung personenbezogener Daten vor. Die Verarbeitung hat u. a. auf rechtmäßige Art und Weise, nach Treu und Glauben und für die betroffene Person in einer nachvollziehbaren Weise zu erfolgen und erfordert immer eine Rechtsgrundlage nach Art. 6 Abs. 1 UAbs. 1 DSGVO. Die Verarbeitung ist an festgelegte, eindeutige und legitime Zwecke gebunden, sie ist auf das notwendige Maß und die notwendige Dauer zu beschränken und bedarf angemessener Sicherheitsvorkehrungen, um die Integrität und Vertraulichkeit zu gewähren.

Dem SSI-Ansatz selbst ist immanent, dass er die Grundsätze der Transparenz und Selbstbestimmtheit unterstützt, was aus datenschutzrechtlicher Sicht positiv zu werten ist. ZKP adressieren zum einen den Grundsatz der Datenminimierung sowie durch die Pseudonymisierung auch die Grundsätze des „Data Protection by Design" und „Data Protection by Default".

15 Vgl. *Fiedler / Granc*, DuD 2022, S. 27f.

Die Möglichkeiten mittels SSI-Wallets über einen direkten Kanal Informationen auszutauschen, eröffnet zusätzliche Potentiale für Transparenz und Selbstbestimmtheit.

Rechtliche Fragestellungen ergeben hierbei insbesondere bezüglich der Legitimierung der Datenverarbeitung. Grundsätzlich legitimiert Art. 6 Abs. 1 UAbs. 1 lit b DSGVO die Verarbeitung der Daten, die für die Erfüllung des Vertrags oder die Vermittlung von Diensten erforderlich sind. Für eine weitergehende Verarbeitung von Daten, über das vertraglich vereinbarte, oder das für die Vertragserfüllung erforderliche Maß hinaus, kommt eine Einwilligung als Rechtsgrundlage in Betracht.

Nach Art. 6 Abs. 1 UAbs.1 lit. a DSGVO kann die betroffene Person in die Datenverarbeitung für einen bestimmten Zweck einwilligen. Die Erklärung der Einwilligung muss freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich erklärt werden (Art 4 Nr. 11 DSGVO). Freiwilligkeit liegt nur dann vor, wenn die betroffene Person eine echte und freie Wahl hat (Erwägungsgrund 42, Art. 7 Abs. 4) und nicht etwa an einen bestimmten Vorgang gekoppelt ist. Informiertheit liegt vor, wenn die betroffene Person vor der Abgabe der Einwilligungserklärung über den beabsichtigten Zweck der Verarbeitung ihrer personenbezogenen Daten im Einzelnen informiert werden (vgl. Art. 13, 14 DSGVO).

Weiter ist die betroffene Person vor Abgabe der Einwilligungserklärung über ihr Widerrufsrecht aufzuklären (Art. 7 Abs. 3; Art. 13 Abs. 2 lit. b, c; Art. 14 Abs. 2 lit. c, d DSGVO).

Für das SSI-Privacy-Management bedeutet dies, dass für jeden Verarbeitungszweck für den eine Einwilligung als Rechtsgrundlage erforderlich ist, eine Anfrage an den Nutzer zu senden ist, er sich über die Verarbeitungsbedingungen zu informieren hat und in diese freiwillig einwilligen muss.

Zu untersuchen ist, wie sich die Informiertheit in der Praxis umsetzen lässt. Vorauszuschicken ist, dass eine Generaleinwilligung in dem Sinne „Ich willige in alle Verarbeitungen ein, die der Serviceanbieter anfragt", nicht wirksam ist. Rechtsfolge einer fehlenden Informiertheit ist im Zweifel eine unwirksame Einwilligung und damit eine Datenverarbeitung ohne Rechtsgrund.

Die Herausforderung besteht darin, dass der Nutzer im Grunde für jeden „neuen" Verarbeitungszweck bezüglich einer Einwilligung angefragt wird und in diesen auch einwilligen muss. Je nach Anzahl der Touchpoints einer Customer Journey oder Anzahl der Interaktionspartner, die über die Wallet verwaltet werden, ist hier mit einer großen Zahl von Anfragen zu rechnen. Dieser Umstand würde die Usability des Ansatzes erheblich stören.

Die Problematik ist jedoch nicht neu. Bereits seit einigen Jahren stellt sich im Zusammenhang mit PIMS und Datentreuhändern die Frage, ob und wie eine Einwilligungsverwaltung rechtlich zulässig sein kann. Denkbar sind hier prinzipiell ein antizipiertes oder delegiertes Modell zur Einwilligungsverwaltung. Beim delegierten Modell ist die Frage, ob die Einwilligung z. B. an einen vertrauenswürdigen Dritten delegiert werden kann. Der Betroffene könnte dabei seine eigenen Datenschutzvorlieben benennen, damit Verarbeitungszwecke und Verarbeiter eingegrenzt und gefiltert werden können. Datenschutzrechtlich stellt dieser Teil im Grunde keine Hürde dar.

Weiter ist allerdings fraglich, inwieweit beispielsweise ein Datentreuhänder Empfehlungen für Einwilligungen aussprechen darf oder ob es sogar möglich ist, die Abgabe der Einwilligungserklärung nach definierten Parametern an eine solche Stelle zu delegieren.

Nach den gegenwärtigen Vorschriften ist eine solche Lösung für Einwilligungen allgemeingültig nicht wirksam umsetzbar. Es fehlt an der persönlichen und informierten Willensbildung, die immer an den bestimmten Zweck gekoppelt ist. Jenseits der DSGVO sind jedoch Entwicklungen zu beobachten, die in ausgewählten Bereichen und unter bestimmten Voraussetzungen eine Einwilligungsverwaltung oder Delegation zulassen können.

Mit dem TTDSG wurden in 2021 beispielsweise, in einem gewissen Rahmen, Verfahren zur Einwilligungsverwaltung in Verbindung mit unabhängigen Diensten zur Einwilligungsverwaltung anerkannt, §§ 26 Abs. 2, 25 TTDSG. Die Festlegung der technischen, organisatorischen und rechtlichen Anforderungen für diese unabhängigen Dienste ist gegenwärtig noch nicht erfolgt. Mit der Einwilligungsverwaltungsverordnung sollen diese Anforderungen für den Anwendungsbereich des TTDSG umrissen werden.[16] Der Ansatz zur Einwilligungsverwaltung ist jedoch nicht auf Konstellationen außerhalb des TTDSG anwendbar und somit nicht allgemeingültig auf die Einwilligungen in Datenverarbeitungen nach der DSGVO übertragbar. Ob und inwieweit zukünftig die EU-Privacy-Verordnung Neuerungen, z. B. im Hinblick auf privatsphärenfreundliche Modelle und Einstellungen in Browsern und Apps zulässt, ist bislang nicht klar ersichtlich und kann an dieser Stelle nicht eingeschätzt werden.

16 Letzter Stand Referentenentwurf des Bundesministeriums für Digitales und Verkehr vom 08.07.2022. URL https://www.itm.nrw/wp-content/uploads/220708_BMDV_RefE_EinwVO.pdf.

Fraglich wird sein, ob solche Entwicklungen zukünftig ein Türöffner in das allgemeine Datenschutzrecht sein können. Aktuell ist eine Einwilligungsverwaltung durch technische Agentensysteme oder die Delegation an Dritte aber nicht möglich.

Zu untersuchen ist jedoch, ob eine mögliche Lösung ein gestufter Prozess sein kann, bei dem Anfragen an den Nutzer in einem ersten Schritt entsprechend seiner Vorlieben und Voreinstellungen in der Wallet gefiltert werden. In einem zweiten Schritt könnte der Nutzer Bedingungen definieren, unter denen eine Einwilligungserklärung erklärt und über die Wallet automatisch umgesetzt werden kann.

Ein Ansatz wäre es beispielsweise ein Modell mit geeigneten Kategorien zu entwickeln, in welchen die „Art personenbezogener Daten", die „Art und Weise der Verarbeitung" und der „Zweck der Verarbeitung" geclustert und standardisiert werden. Standardisierte Kategorien würden zum einen den Nutzer unterstützen die beabsichtige Datenverarbeitung leichter zu erfassen. Zudem könnte das Modell maschinenlesbare Automatisierungen unterstützen.

Zum Beispiel könnten personenbezogenen Daten unterteilt werden in Kategorien K1 bis Kx, wobei K1 - wenig sensible Daten (nutzerdefiniert), Kx - hochsensible Daten enthält. Die Arten von beabsichtigten Datenverarbeitungen wären gleichfalls in Kategorien mit mehr oder weniger kritischen (nutzerdefiniert) Verarbeitungstätigkeiten zu clustern. Die besonderen Anforderungen nach Art. 9 DSGVO für besondere Kategorien personenbezogener Daten müssten zusätzlich noch gesondert berücksichtigt werden.

Eine Hürde dieses Ansatzes besteht darin, dass eine Kategorie nicht die Wirklichkeit abbildet. Generell gibt es z. B. keine klare Festlegung für eine Kategorie zu „Verarbeitungen". Vielmehr sind die Bezeichnungen eine eigenmächtige Festlegung des Serviceanbieters. Welche konkreten Anforderungen in diesem Fall an die Informiertheit der Betroffenen zu stellen sind, muss umfassend untersucht werden. Ob und inwieweit ein solcher Ansatz funktionieren kann, bedarf daher weiterer Forschung.

3.3 Technik

Wenngleich die technische Entwicklung von SSI-Wallets und -Infrastrukturen mit großer Geschwindigkeit voranschreitet, befinden sich die notwendigen Komponenten derzeit in sehr unterschiedlichen Reifegraden. Diese lassen sich in die Kategorien (1) Wallet-Funktionalität, (2) Governance Frameworks und (3) Usability unterteilen.

Der *Funktionsumfang von Wallets* erlaubt heute vor allem das Entgegennehmen, Speichern und Präsentieren von Verifiable Credentials. Zudem werden oft Historien angeboten, die Austauschzeitpunkte von Daten mit unterschiedlichen Partnern nachvollziehbar machen. Allerdings werden empfangene Nachweise auch wieder präsentiert, so dass zwar eine Kontrolle und Freigabe für den Benutzer gegeben ist, eine Datenminimierung jedoch nicht. Die Verwendung von Verifiable Presentations für die selektive Freigabe und Unterstützung von ZKP ist nur in Prototypen vorhanden. Zudem existiert bislang noch kein Standard für die Datenportabilität, um Nutzern zu ermöglichen, ihre bestehenden Nachweise gesammelt in eine neue Wallet eines anderen Anbieters übertragen zu können. Schließlich ist auch der Umgang mit Nachweisen für Dritte, z. B. im Kontext von Sorgeberechtigungen, Vertretungsberechtigungen und Vollmachten in bestehenden Systemen kaum adressiert. Dies betrifft nicht nur Dienstanbieter wie Unternehmen, Vereine und Kommunen, sondern auf der Nutzerseite auch Familien.

Beim konkreten Einsatz digitaler Nachweise offenbart sich eine der größten Herausforderungen für die Nutzung von SSI: Einerseits soll damit eine technisch interoperable Lösung für die flexible Nutzung von digitalen Nachweisen in verschiedenen Szenarien erlaubt werden, andererseits ist der Umgang mit ihnen sehr stark von den Regeln des Nachweises und des Einsatzkontexts abhängig. Zur Verbindung der technischen Perspektive von SSI mit den Sphären von Wirtschaft, Recht und Gesellschaft werden Regelwerke genutzt, die auch als *Governance Frameworks* bezeichnet werden.[17] Diese Regelwerke sind zum einen erforderlich, um bestehende Gesetze abzubilden. Zum anderen können sie dem Benutzer eine Unterstützung in seinen Entscheidungen bei seinen Interaktionen in der SSI-Wallet zu geben. Damit soll vermieden werden, dass Credentials von unberechtigten Herausgebern in den Verkehr gebracht werden (Fälschungssicherheit) oder Nutzer ihre Daten arglos unberechtigten Akzeptanzstellen übermitteln (Schutz vor Identitätsdiebstahl). Konkret sind damit u. a. folgende Herausforderungen verbunden:

- *Vertrauenswürdige Akzeptanzstellen***:** Die einfache Verfügbarkeit und Bereitstellung qualitativ hochwertiger Daten bergen das Risiko, dass Kriminelle über gefälschte Websites mittels Phishing-Daten von Nutzenden erbeuten. Daher sind Mechanismen erforderlich, die das Recht eines Ak-

17 *Preukschat / Reed*, Self-sovereign identity, 2021, S. 248f.

teurs zur Abfrage bestimmter Daten überprüfbar machen. Erste Ansätze dafür arbeiten mit SSL-Zertifikaten.[18] In Zukunft könnten dafür Trust Lists oder VCs genutzt werden.
- *Vertrauenswürdige Herausgeber:* Damit Vertrauen in Daten entsteht, muss nicht nur die Akzeptanzstelle, sondern auch der Inhaber sicher sein, dass nur autorisierte Herausgeber Nachweise erstellen.

Da Wallets ein zentrales Werkzeug für Interaktionen im digitalen Raum werden sollen, müssen sie ähnlich wie Web-Browser oder E-Mail-Programme für die breite Bevölkerung einfach nutzbar sein. Die Erweiterung von Wallets um Funktionen für die Wahrnehmung von datenschutzbezogenen Rechten sowie die differenzierte Nutzung von Nachweisen erfordert von Nutzern ein hohes Maß an Verständnis für die Interaktionen und ihrer Auswirkungen. Dafür ist eine hohe *Usability* erforderlich, die sich nicht nur auf die Wallet selbst, sondern auf die gesamte Interaktion z. B. mit einer Website, einer anderen Person oder einem öffentlichen Terminal erstreckt. Um einen Wechsel zwischen verschiedenen Wallets zu erleichtern, forderte Kim Cameron in seinen „Seven Laws of Identity" eine konsistente Nutzererfahrung in verschiedenen Einsatzkontexten.[19] Bislang hat die schnelle Entwicklung einer Vielfalt von Wallets nur sehr begrenzt zu übergreifenden Bedienkonzepten geführt.[20]

4. Forschungsbedarf und Realisierbarkeit

Zur Erschließung der Potenziale des SSI-Privacy-Managements ergeben sich Forschungs- und Entwicklungsbedarfe auf den Gebieten der Technologie, der Verhaltensökonomie und des Rechts. Die Technologie gibt dabei das Grundgerüst für den Ansatz vor, verhaltensökonomische und rechtlich Implikationen sind bei der Ausgestaltung des Ansatzes zu berücksichtigen. Nachfolgend werden die Forschungs- und Entwicklungsbedarfe kurz umrissen.

18 https://docs.lissi.id/lissi-wallet/verification-of-contacts-within-the-lissi-wallet.
19 *Cameron*, The Laws of Identity 2005.
20 *Krauß* u.a., HMD 2023, S. 344f.

4.1 Technisch-organisatorisch

Für die Realisierung der in Abschn. 2.2 beschriebenen Vision eines SSI-Privacy-Managements ist Forschungs- und Entwicklungsarbeit im Hinblick auf die technisch-organisatorischen Aspekte, die Datenminimierung, die Governance und Usable Security zu leisten.

Für die *Datenminimierung* sind die Mechanismen für selektive Freigabe im Rahmen von Verifiable Presentations sowie Zero-Knowledge Proofs von großer Bedeutung. Beide sind konzeptionell beschrieben und prototypisch implementiert. Für eine praktische Nutzbarkeit bedarf es jedoch noch Abstimmungen hinsichtlich der verwendeten Datenformate und kryptografischen Verfahren. Die Anforderungen an kryptografische Verfahren betreffen dabei insbesondere die möglichst weite Verbreitung effizienter Implementierungen sowie Ausführbarkeit auch in ressourcen-beschränkten Umgebungen wie Hardware-Sicherheitsmodulen. Für die Repräsentation der zugrundeliegenden Datenstrukturen sind ebenfalls geeignete Festlegungen zu treffen, die auf offenen Standards beruhen und plattformunabhängig sind. Schließlich sind ebenfalls Protokolle zu vereinbaren, die eine selektive Abfrage von Daten überhaupt möglich machen.

Der Aufbau dezentraler Systeme für den Nachweisaustausch erfordert *übergreifende Verzeichnisse*, in denen gemeinsam genutzte Informationen öffentlich abgelegt werden. Dazu gehören z. B. öffentliche DIDs von Dienstanbietern, Schemata für Credentials sowie der Gültigkeitsstatus ausgegebener Nachweise. Die dafür notwendigen Mechanismen sind derzeit im Entstehen. Im Umfeld regulierter Vertrauensdienste nach der eIDAS-VO werden dafür Trust Lists[21] verwendet. Ähnliche Konzepte werden von der „Decentralized Identity Foundation" sogenannte Trust Registries[22] vorgeschlagen, um vertrauenswürdige Herausgeber, Akzeptanzstellen, verwendete Schemata und akzeptierte Wallets zu hinterlegen. Bislang bestehen hierfür nur erste Schnittstellen-Spezifikationen. Konkrete technische Implementierungen, deren Nutzung in SSI-Ökosystemen sowie die Bewertung ihrer rechtlichen Implikationen müssen Gegenstand künftiger Forschung sein.

Damit SSI einen transparenten und datenschutzkonformen Datenaustausch sowie eine Ermächtigung der Nutzer erlaubt, ist eine Automatisierung von Regeln für ein Governance Framework erforderlich. Es bestehen

21 https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home.
22 https://wiki.trustoverip.org/display/HOME/Trust+Registry+Task+Force.

zwar erste Ansätze zur Systematisierung von Governance für SSI,[23] jedoch ist deren technische Umsetzung und praktische Nutzung weitgehend unerforscht. Für das hier betrachtete Privacy-Management sind insbesondere Credential Governance und Ecosystem Governance relevant: Die *Credential Governance* beschreibt u. a. Inhalte, Anwendungsbereich und Gültigkeit von Nachweisen. Weiterhin kann festgelegt werden, welche Akteure berechtigt sind, bestimmte Nachweise auszustellen, zu prüfen oder zu verändern. Der Einsatz von Nachweisen ist Gegenstand der *Ecosystem Governance*. Sie organisiert das Zusammenspiel von Akteuren, die gemeinschaftlich Wertschöpfung betreiben. Dazu können Verweise auf Regeln zu Nachweisen, zulässiger Technik, Vertrauensniveaus, Vergütungsmodellen und Regeln zum Schutz der Privatsphäre etabliert werden. Sie legen beispielsweise fest, welche Akteure in einem definierten Kontext berechtigt sind, Nachweise eines bestimmten Typs auszustellen.

Diese Regelwerke müssen in maschinenlesbarer Form formuliert und innerhalb des Gültigkeitsbereichs für alle Akteure zugänglich gemacht werden. Zudem wird die Einhaltung von Regeln prüfbar, so dass bei Verstößen entsprechende Sanktionen verhängt werden können. Dafür müssen u. a. für folgende Aspekte konzeptionelle und technische Entwicklungen durchgeführt werden:

- *Angemessenheit von Anfragen:* Über die Prüfung der Akzeptanzstelle hinaus sollte Nutzern ein Hinweis gegeben werden, ob die für eine bestimmte Interaktion angefragte Datenmenge angemessen ist. Dieses Konzept gibt es bei der eID in Form des „Berechtigungszertifikats", das Akzeptanzstellen beim Bundesverwaltungsamt beantragen müssen. Für eine kostengünstigere und niederschwellige Prüfung wären andere Mechanismen wie die Bewertung von „Presentation Schemas" durch Zertifizierungen oder aggregierte Rückmeldungen („Crowd Intelligence") von Nutzern denkbar.
- *Nutzungsbedingungen von Daten*: Die Spezifikation des Verifiable Credentials Data Model enthält ein Attribut „termsOfUse", in dem die Nutzungsbedingungen (Policies) der Daten festgehalten werden können.[24] Dieses kann Pflichten, Verbote und Berechtigung im Umgang der betreffenden Daten durch die Akzeptanzstelle (Verifier) festlegen. Die Spezifikation sieht vor, dass damit Policies vom Herausgeber an den Inhaber (im VC) sowie vom Inhaber an die Akzeptanzstelle (in der VP)

23 *Anke / Richter*, HMD 2023, S. 270ff.
24 https://www.w3.org/TR/vc-data-model/#terms-of-use.

übermittelt werden können. Damit kann die Akzeptanzstelle gegenüber Dritten nachweisen, dass er die Daten rechtmäßig erhalten hat. Weicht die Akzeptanzstelle von den angegebenen Regeln ab, muss sie dafür die Verantwortung übernehmen.
- *Zweck von Abfragen:* Die im DIDcomm Protokoll „PresentationExchange" verwendeten Presentation Schemas besitzen ein Attribut „purpose", in dem der Zweck einer Anfrage angegeben werden kann. Wie auch bei termsOfUse ist derzeit noch nicht spezifiziert, wie dieses Attribut jenseits eines Freitext-Felds genutzt werden soll.

Zur Steigerung der *Usability* von Wallets sollten einheitliche Bedienkonzepte sowie eine einheitliche Terminologie etabliert werden. Dafür sind Forschungsarbeiten zur Verständlichkeit und Akzeptanz verschiedener Gestaltungen von Wallets für unterschiedliche Zielgruppen erforderlich. Für die Entscheidungen zum Teilen von Daten an Dritte sollten Nutzer geeignet unterstützt werden. Inhaltlich müssen dafür die vorliegenden Informationen aus den jeweilig geltenden Governance Frameworks genutzt werden. Diese Informationen müssen in geeigneter Art in die Benutzeroberfläche integriert werden, um die Benutzerinteraktion zu führen. Ein möglicher Weg dazu ist es, Konzepte zur Usable Security aus anderen sicherheitsrelevanten Interaktionen wie z. B. Onlinebanking und Web-Browser auf Wallets zu übertragen.

4.2 Verhaltensökonomisch

Für die Steigerung der Usability von Wallets und die Konzeption von Usable Security Maßnahmen ist zu eruieren, welche verhaltensökonomischen Faktoren Einfluss auf die Verständlichkeit und die Akzeptanz haben.

In einem ersten Schritt sind mögliche Barrieren und Treiber seitens der Nutzer in qualitativen und quantitativen Verfahren der empirischen Sozialforschung zu untersuchen, die für eine Inanspruchnahme der Transparenz und Selbstbestimmungsoptionen des SSI Privacy Managements bedeutend sind.

Basierend auf diesen Ergebnissen ist zu analysieren, welche Methoden geeignet sind, den Nutzer dahingehend zu befähigen, Privacy-Risiken einzuschätzen, Rechte wahrzunehmen und durchzusetzen, aber auch einen interessengerechten und wertstiftenden Austausch von Daten und eine Interaktion mit Dienstanbietern zu unterhalten.

Gewichtige Faktoren für die Akzeptanz werden vermutlich positive Nutzererlebnisse in Bezug auf Handhabung der Wallet, Reduzierung von zu administrierenden Aufwänden bei der Nutzung von Services, aber auch das Durchsetzen von Interessen und Rechten im Sinne der Selbstbestimmtheit sein.

4.3 Rechtlich

In rechtlicher Hinsicht sind regulatorische Implikation für die Prozesse und Funktionalitäten des SSI Privacy-Management zu untersuchen sowie geeignete Governance-Strategien und Maßnahmen zu entwickeln, die die Umsetzung und Durchsetzung von Rechen unterstützen.

Im Hinblick auf das Governance Framework sind die rechtlichen Rahmen und Anforderungen umfassend zu untersuchen und zu bewerten. Unter Berücksichtigung der Vorschriften aus der eIDAS-VO Novellierung sind regulatorische Anforderungen an Nachweise (Credentials Governance) sind zu evaluieren und daraus Ecosystem Governance-Strategien und Policies abzuleiten. Aus den Ergebnissen sind Mechanismen und Standards für automatisierbare und maschinenlesbare Prozesse zu definieren und Gestaltungsmuster zu entwickeln, die in ein Gesamtregelwerk überführt werden können.

Für die Implementierung der regulatorischen Vorgaben sind geeignete Methoden und verschiedene Gestaltungsmuster interdisziplinär zu evaluieren.

4.4 Gegenstand weiterer Forschung

Der Forschungsbedarf für das SSI Privacy-Management stellt sich als interdisziplinär, eng miteinander verzahnt und komplex dar. Gegenstand der weiteren Forschung muss es sein, die tatsächlichen Präferenzen von Akteuren und deren Auswirkungen zu untersuchen:

- Empfinden Benutzer die Verwendung von SSI als ein höheres Maß an Selbstbestimmung?
- Sind komplexere Mechanismen für das Aushandeln von Datenumfang und -Nutzungsbedingungen erforderlich?
- Sind Dienstanbieter bereit, einen Teil ihrer bislang selbstverwalteten Datenbestände auf die Wallets der Kunden zu verlagern und dort bei Bedarf abzufragen?

- Haben Dienstanbieter einen Wettbewerbsvorteil (z. B. durch höhere Akzeptanz von Diensten, höhere Zahlungsbereitschaft von Nachfragenden oder Kostensenkung im Umgang mit personenbezogenen Daten), wenn sie ihre Datennutzung transparent machen und die angefragte Datenmenge minimieren?
- Unter welchen Bedingungen sind Nutzer bereit, Daten zu teilen, die nicht der Erbringung von angefragten Leistungen dienen?

5. Zusammenfassung und Fazit

Self-Sovereign Identity und Wallets sind Werkzeuge, um digitale Identität von Personen, Organisationen oder Maschinen zu verwalten, Identitäts- und Berechtigungsnachweise zu erbringen und zu kontrollieren, aber auch um Daten auszutauschen und die Verarbeitung zu legitimieren. Für Nutzer digitaler Services bieten sie neue Möglichkeiten im Hinblick auf Selbstbestimmtheit und Transparenz. Für digitale Ökosysteme eröffnen sich neue Gestaltungsräume, um die Aufwände für die Datenhaltung zu minimieren, die Qualität von Daten zu verbessern und Daten interessengerechter verarbeiten zu können.

Das SSI-Privacy-Management setzt auf diese Werkzeuge und Möglichkeiten auf und zeigt einen Ausblick darauf, wie ein SSI-Wallet unterstütztes Privacy-Management aussehen kann und welche Potentiale dieser Ansatz im Sinne einer Data Governance bietet. Dabei ist erkennbar, dass SSI und Wallets, durch neuartige Mechanismen für Identitäts- und Berechtigungsnachweise sowie für Datenbereitstellungen, einen Paradigmenwechsel herbeiführen können, hin zu einer verbesserten Selbstbestimmtheit und zu interessengerechterer Data Governance.

Positive Nutzererlebnisse und die Akzeptanz aller Akteure im Ökosystem können, neben den technischen Weiterentwicklungen, der Schlüssel zu diesen Verbesserungen und damit der Treiber für das SSI Privacy-Management werden. Diese Potentiale zu heben, muss Gegenstand weiterer interdisziplinärer Forschung sein.

Literatur

Allen, C. (25. April 2016): The path to self-sovereign identity. URL: http://www.lifewithalacrity.com/previous/

Anke, J. und Richter, D. (2023): Digitale Identitäten. *HMD Praxis der Wirtschaftsinformatik* 60(2), S. 261–282. https://doi.org/10.1365/s40702-023-00965-1.

Cameron, K. (May 2005): The Laws of Identity. URL: https://www.identityblog.com/?p=352.

Europäische Kommission (03. Juni 2021): Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität. COM(2021) 281 final. Brüssel. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52021PC0281

European Data Protection Supervisor (2021): Personal Information Management-System. Brussels. URL: https://edps.europa.eu/data-protection/our-work/subjects/systeme-de-gestion-des-informations-personnelles_de

Fiedler, A., Granc, F. (2022): Nationale und europäische Sicht auf eIDAS 2.0 – Aufwand und Nutzen. *Datenschutz und Datensicherheit (DuD),* 46, S. 27–31. https://doi.org/10.1007/s11623-022-1556-0

Hornung, G. (2005): *Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren*. Baden-Baden: Nomos.

Hardmann, D. (2020): Aries RFC 0430: Machine-Readable Governance Frameworks URL: https://github.com/hyperledger/aries-rfcs/blob/main/concepts/0430-machine-readable-governance-frameworks/README.md.

Krauß, A.-M. Sellung, R.A. und Kostic, S. (2023): Ist das die Wallet der Zukunft?. *HMD Praxis der Wirtschaftsinformatik* 60(2), S. 34-365. https://doi.org/10.1365/s40702-023-00952-6.

Preukschat, A. und Reed, D. (2021): *Self-sovereign identity: Decentralized digital identity and verifiable credentials*. Shelter Island, NY : Manning Publications.

Roetzel, P.G. (2019): Information overload in the information age: a review of the literature from business administration, business psychology, and related disciplines with a bibliometric approach and framework development. *Business Research*, 12, S. 479-522. https://doi.org/10.1007/s40685-018-0069-z.

Stiftung Datenschutz (2017): Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen. Leipzig: Stiftung Datenschutz. URL: https://stiftungdatenschutz.org/veroeffentlichungen.

Stand der Internetquellen in dieser Arbeit: 16.05.2023.

Zu Risiken und Anonymisierungen von Verhaltensbiometrie

Simon Hanisch, Julian Todt, Melanie Volkamer und Thorsten Strufe

Zusammenfassung

Die bestehenden Social-Media-Plattformen erweitern sukzessive die Art, Qualität und Quantität der Daten, die sie über ihre Nutzer:innen erheben. Zu bereits früher aufgezeichneten Daten kommen diverse neue Arten hinzu: Hierzu gehören Körperbewegungen, wie die Handgesten, mit denen die Geräte gesteuert werden, die Augenbewegungen, die von vielen Geräten erfasst werden, aber auch Faktoren wie die menschliche Stimme, oder Herzschläge und Gehirnaktivitäten.

Neben der simplen Identifizierung von Individuen erlauben diese verhaltensbiometrische Merkmale viele Rückschlüsse über Eigenschaften aufgenommener Personen, wie Alter, Geschlecht, Gesundheitszustand, aber auch die Persönlichkeit. Für die Nutzer:innen ist dabei nur noch sehr schwer zu erkennen, welche Rückschlüsse über persönliche Informationen möglich sind.

Als Gegenmaßnahme gegen diese Privatsphäreeinschnitte haben Nutzer:innen oftmals nur die Wahl, ob eine Anwendung auf einen bestimmten Sensor vollständig zugreifen darf, oder gar nicht; wobei Letzteres oftmals damit verbunden ist, dass die Anwendung nicht mehr wie gewünscht, oder gar nicht mehr funktioniert.

Um dieser Diskrepanz zwischen Datenschutz und immer weitreichenderer Datensammlung zu begegnen, bedarf es zunächst Untersuchungen über die in solchen biometrischen Daten enthaltenen Informationen. Zusätzlich werden neuartige Privatsphäre-Einstellungen nötig, in welchen die Nutzer:innen nicht nur wählen können, ob Daten geteilt werden (z.B. von bestimmten Sensoren), sondern auch ob private Eigenschaften durch Anonymisierungstechniken vor dem Teilen entfernt werden sollen.

1. Einleitung

Die Qualität und Quantität, mit welcher unser alltägliches Leben erfasst wird, hat sich bisher stetig erhöht. Von großen, dedizierten, digitalen Ka-

meras, die nicht mehr als 800x600 Pixel aufnehmen können, zu Megapixel-Kameras in Smartphones ist dieser Trend bis heute ungebrochen. Mit Augmented Reality (AR) and Virtual Reality (VR) steht der nächste Schritt in dieser Entwicklung an.

Die Vision von Technologiekonzernen wie Meta ist es, mit AR/VR ein Metaverse zu schaffen, eine digitale Welt, in der wir arbeiten, interagieren und leben werden. Für das Eintreten in diese digitale Welt ist es notwendig, ihre Nutzer:innen genau zu erfassen, um einen digitalen Zwilling zu erschaffen. Dazu werden die Nutzer:innen dauerhaft von einem AR/VR-Gerät aufgenommen, was die Quantität der erhobenen Daten erhöht. Durch den Einsatz neuer Sensorik wie Tiefenkameras, Inertial-Measurement-Units (IMU) und Lighthouse-Tracking werden die Nutzer:innen außerdem in einer noch nie dagewesenen Qualität erfasst.

AR/VR-Geräte zeichnen Körperbewegungen, Handbewegungen, Mimik und Augenbewegungen auf und auch erste medizintechnische Geräte wie Elektroenzephalografie (EEG) und Pulsoxymeter werden bereits integriert. Allen diesen Merkmalen ist gemeinsam, dass sie das Verhalten ihrer Nutzer:innen aufzeichnen. Man spricht von verhaltensbiometrischen Merkmalen.

Verhaltensbiometrische Merkmale erlauben wie physiologisch-biometrische Merkmale (z.B. Fingerabdruck, Gesicht, Iris) die Identifizierung der Nutzer:innen, da auch verhaltensbiometrische Merkmale für jede Person einzigartig sind. Im Gegensatz zu physiologischen Merkmalen lassen verhaltensbiometrische Merkmale jedoch weitere Rückschlüsse auf private Informationen einer Person zu. So lassen sich aus Körperbewegungen das Geschlecht und verschiedene medizinische Besonderheiten ableiten, und Augenbewegungen erlauben weitreichende Rückschlüsse über Charaktereigenschaften[1] und Interessen[2].

Diese Mischung aus dauerhafter Erfassung und Aufzeichnung von verhaltensbiometrischen Merkmalen bedeutet, dass AR/VR Geräte eine große Gefahr für die Privatsphäre ihrer Nutzer:innen darstellen. Zumal die meisten heute vertretenen Anbieter von AR/VR Plattformen ihr Geschäftsmodell auf der Kommerzialisierung der gesammelten Daten basieren und damit die Kommerzialisierung der Nutzer:innen im Mittelpunkt steht. Zum Schutz vor diesen Gefahren bedarf es guter Schutzmaßnahmen für die Nutzer:innen.

1 Kröger u.a., in: Friedewald u.a. (Hrsg.), Privacy and Identity Management, 2020
2 Hess/Polt, in: Science, 1960 (3423)

In dieser Ausarbeitung befassen wir uns daher mit den Risiken und Schutzmaßnahmen für verhaltensbiometrische Daten im Kontext von Mixed Reality (MR). Zum einen möchten wir aufzeigen, welche verhaltensbiometrischen Merkmale es gibt, wofür sie verwendet werden können und welche Risiken für die Privatsphäre damit verbunden sind. Darüber hinaus schlagen wir vor, die bestehenden Privatsphäre-Einstellungen für das Teilen von Daten mit Anwendungen auf mobilen Endgeräten für AR/VR-Plattformen zu erweitern. Abschließend stellen wir kurz zwei allgemeine Ansätze zur Anonymisierung verhaltensbiometrischer Daten vor.

Die Ausarbeitung ist wie folgt gegliedert. Im folgenden Abschnitt 2 beschreiben wir die verwendete Terminologie sowie das Szenario und die betrachteten Angreifer:innen. In Abschnitt 3 diskutieren wir verwandte wissenschaftliche Arbeiten. In Abschnitt 4 geben wir einen Überblick über existierende verhaltensbiometrische Merkmale und in Abschnitt 5 stellen wir unseren Vorschlag für eine datenschutzfreundlichere Datenfreigabe vor. In Abschnitt 6 stellen wir zwei allgemeine Ansätze zur Anonymisierung verhaltensbiometrischer Daten vor. Abschließend ziehen wir in Abschnitt 7 ein Fazit.

2. Terminologie und Szenario

In diesem Abschnitt beschreiben wir die Terminologie und das Szenario, das wir für unsere Ausarbeitung verwenden.

Biometrische Faktoren sind Merkmale die sich durch die Vermessung von Menschen ergeben und spezifisch für bestimmte Personen sind. Unterschieden werden biometrische Faktoren in physiologische und verhaltensbiometrische Faktoren. *Physiologische* biometrische Faktoren beschreibe direkte körperliche Merkmale eines Menschen. Beispiele für solche Faktoren sind das Gesicht, der Fingerabdruck, oder die Iris. Faktoren, die das Verhalten einer Person beschreiben werden als als *verhaltensbiometrische* Faktoren bezeichnet. Beispiele für diese Faktoren sind unser Gang, unsere Sprache oder unsere Augenbewegungen. Neben den biometrischen Faktoren, die eine Person direkt identifizieren können, gibt es auch so genannte *softbiometrische* Faktoren. Sie enthalten wenig Information und erlauben höchstens die Zuordnung von Individuen zu Gruppen. Für sich alleine genommen erlauben sie keine eindeutige Identifizierung und erst durch die Kombination von mehreren dieser Faktoren wird eine Person eindeutig

identifizierbar. Zu den softbiometrischen Faktoren zählen Merkmale wie das Gewicht, die Hautfarbe, das Alter oder das Geschlecht einer Person.

Für die Privatheit von Personen unterscheiden wir zwei Gefahren. Mit *Identifikation* bezeichnen wir den Prozess, der die biometrischen Daten eindeutig einer Person zuordnet. Und mit *Attributinferenz* bezeichnen wir das Ableiten von persönlichen Eigenschaften aus den biometrischen Daten.

Beim Schutz der Privatheit unterscheiden wir zwischen Anonymisierung und Attributsschutz. Mit *Anonymisierung* bezeichnen wir den Prozess, der die Zuordnung zwischen Identität und biometrischen Daten verhindert oder zumindest erschwert. Wichtig ist hier die Unterscheidung zwischen Anonymisierung und Pseudonymisierung. Bei der *Pseudonymisierung* wird die Zuordnung von Identität und biometrischen Daten durch eine Zuordnung mit einem anderen Identifikator ersetzt, während nach der Anonymisierung die biometrischen Daten keiner Identität mehr zugeordnet werden können. Unter *Attributsschutz* verstehen wir eine Methode, die die biometrischen Daten so verändert, dass bestimmte Attribute nicht mehr aus den biometrischen Daten abgeleitet werden können.

Wenn wir eine bestimmte Methode zum Schutz der Privatsphäre betrachten, dann können wir dies nur im Kontext einer konkreten Anwendung tun, für die die biometrischen Daten verwendet werden sollen. Die Anwendung gibt vor welche Informationen in den biometrischen Daten erhalten werden sollen, den Nutzwert der Daten. Ohne einen konkreten Nutzwert könnten die biometrischen Daten auch einfach nicht erhoben werden, um die Privatsphäre eine Person zu schützen. Eine Methode zum Schutz der Privatsphäre hat also immer zwei (oft konkurrierende) Ziele, den Schutz der personenbezogenen Daten und den Erhalt des Nutzwertes der Daten.

Privatsphäre ist etwas Subjektives: Was als privat empfunden wird und in welchem Kontext hängt einzig und allein von den Nutzer:innen ab. Davon hängen die Ziele für den Schutz der Privatsphäre und den Nutzwert ab, so kann es in einem Kontext für die Nutzer:innen das Ziel sein, ihre Identität zu verschleiern, während in einem anderen Kontext die Identifizierung der explizite Nutzen der Daten ist. Ein gutes Beispiel hierfür ist die medizinische Diagnose mit Hilfe biometrischer Daten. Während sie für eine Untersuchung beim Arzt nützlich sind, sollen sie in fast allen anderen Kontexten vermieden werden.

Als Kontext für unsere Ausarbeitung betrachten wird folgendes *Szenario*: Unsere Nutzer:innen wollen verhaltensbiometrische Daten mit einer AR/VR Anwendung teilen, damit diese ihnen selbst und anderen Nut-

zer:innen einen Nutzen bringt. Ein Beispiel für solch eine Anwendung ist ein VR-Chat, in dem sich Nutzer:innen mit ihren Freund:innen für ein Gespräch treffen. Ein weiteres Beispiel kann aber auch eine medizinische App sein, welche die Herzschläge von Nutzer:innen aufzeichnet und zur Analyse an den Hersteller der App übermittelt. Wichtig in diesem Szenario ist, dass die Nutzer:innen ihre biometrischen Daten in die Hände Dritter geben und somit die direkte Kontrolle über ihre Daten verlieren. Um ihre Privatheit in diesem Szenario zu schützen, nutzen die Nutzer:innen eine technische Methode, welche sensible persönliche Informationen aus den biometrischen Daten entfernt oder diese so verschleiert, dass sie nicht verwertet werden können.

Für unsere *Angreifer:innen* nehmen wir an, dass diese in den Besitz der Daten der Nutzer:innen kommen, entweder weil sie selbst die Dienstanbieter sind, oder weil sie anderweitig an die Daten gelangen (z.B. durch ein Datenleck beim Dienstanbieter). Ziel der Angreifer:innen ist es, die Person, zu der die verhaltensbiometrischen Daten gehören, zu identifizieren oder private Eigenschaften von dieser Person zu inferieren. Zur Durchführung ihrer Angriffe verfügen die Angreifer:innen über verhaltensbiometrische Datensätze, mit denen ein biometrisches Erkennungssystem trainiert werden kann, sowie für die Identifizierung über verhaltensbiometrische Referenzmuster der Nutzer:innen, mit denen die Angreifer:innen die Nutzer:innen identifizieren können.

3. Stand der Wissenschaft

Die Identifizierung und das Ableiten privater Informationen von Personen anhand ihrer biometrischen Daten ist ein Thema, das bereits umfassend erforscht wurde. Bekannte biometrische Faktoren sind hier das Gesicht[3], die Stimme[4], der Fingerabdruck[5] oder die Iris[6]. Es wurde auch schon gezeigt,

3 Deng u.a., in: Conference on Computer Vision and Pattern Recognition, 2019
4 Chandolikar u.a., in: International Mobile and Embedded Technology Conference (MECON), 2022
5 Ali u.a., in: *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016*
6 Patil u.a., in: *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), 2016*

dass die Kopf- und Handbewegungen von Nutzer:innen mit VR-Headsets ausreichen, um diese eindeutig zu identifizieren[7].

Für das Teilen von Daten in MR-Anwendungen gibt es bereits erste Arbeiten, die sich mit Aspekten des Problems beschäftigten. Lebeck et al.[8] untersuchten mit strukturierten Interviews in Verbindung mit einer Laborstudie welche Datenschutzbedenken Nutzer:innen von AR-Anwendungen haben. Des Weiteren haben Harborth und Frink[9] in einer Umfrage untersucht, welche Datenfreigaben für mobile AR-Anwendungen Nutzer:innen am gefährlichsten für ihre Privatheit empfinden.

Als Gegenmaßnahme zu diesen Datenschutzproblemen haben sich Raval et al.[10] mit der Verfeinerung der Datenfreigabe von Videodaten beschäftigt. Anstelle des ganzen Videos wird ein Bildausschnitt durch die Nutzer:innen markiert, welcher mit der Anwendung geteilt wird. Petracca et al.[11] schlagen ein Framework vor, welches das unbeabsichtigte Gewähren von Sensorberechtigungen verhindern soll.

Eine weitere vorgeschlagene Verbesserung beim Teilen von Sensordaten besteht darin, die Daten in einer abstrakteren Form mit Anwendungen zu teilen. Jana et al.[12] schlagen vor, anstelle von Videodaten nur Skelett und Posen mit Anwendungen zu teilen, welche die Körperbewegungen der Nutzer:innen benötigen. Für die gemeinsame Nutzung von Videos zur Szenenerkennung schlagen sie vor, diese auf ihre Umrisse zu reduzieren, wodurch sensible Daten wie Dokumenteninhalt und Schrift aus dem Video entfernt werden. Dieses Abstraktionskonzept wurde von Gunzman et al.[13] durch eine Objekterkennung ergänzt, die einzelne Objekte in der Szene erhält und den Rest ausblendet.

PrePose[14] verfolgt ein ähnliches Abstraktionskonzept, allerdings nicht für statische Objekte, sondern für Bewegungen. Über eine Modellierungssprache kann definiert werden, welche Gesten erkannt werden sollen, ent-

7 Pfeuffer u.a., in: Conference on Human Factors in Computing Systems (CHI), 2019
Miller u.a., in: Scientific Reports 10 no. 1, 2020
Liebers u.a., in: Conference on Human Factors in Computing Systems (CHI), 2021
8 Lebeck u.a., in: IEEE Symposium on Security and Privacy (SP), 2018
9 Harboth/Frink u.a., in: Seventeenth Symposium on Usable Privacy and Security, 2021
10 Raval u.a., in: 14th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys), 2016
11 Petracca u.a., in: 26th USENIX Security Symposium, 2017
12 Jana u.a., in: 22nd USENIX Security Symposium, 2013
Jana u.a., in: IEEE Symposium on Security and Privacy, 2013
13 Gunzman u.a., in: IEEE 44th Conference on Local Computer Networks (LCN), 2019
14 Figueiredo u.a., in: IEEE Symposium on Security and Privacy (SP), 2016

sprechend wird der Anwendung mitgeteilt, welche Grundgesten in welcher Reihenfolge ausgeführt werden.

Lehman et al.[15] schlagen vor, nicht die Daten selbst, sondern die darauf arbeitenden maschinellen Lernmodelle (ML-Modelle) zu verändern. In ihrem System müssen Anwendungsanbieter ihre ML-Modelle bei den Plattformanbietern einreichen, die diese auf ihre Funktionsfähigkeit prüfen und zertifizieren. Auf dem Gerät selbst können dann nur zertifizierte ML-Modelle genutzt werden, denen die Nutzer:innen eine Erlaubnis erteilt haben.

Um die Nutzung von MR-Geräten in sensiblen Bereichen einzuschränken haben Roesner et al.[16] vorgeschlagen die MR-Geräte auf physische Schilder reagieren zu lassen. Wenn die Geräte ein Verbotsschild erkennen, schränken sie ihre Aufnahmen automatisch ein.

Durch die Vermischung von realer und virtueller Welt entstehen neuartige Sicherheitsprobleme für die Nutzer:innen. Ruth et al.[17] haben untersucht, wie Berechtigungen für die Manipulation geteilter virtueller Welten realisiert werden können. Ein weiteres Problem für AR ist hingegen, dass virtuelle Objekte die Sicht der Nutzer:innen auf die reale Welt versperren und so z.B. zu Unfällen führen können. Lebeck et al.[18] haben weiter untersucht, wie ein Rechtesystem gestaltet werden kann, das gefährliche Einblendungen in AR verhindert, z.B. das Verdecken von Gefahren in der realen Welt.

Wir sehen in der Literatur, dass das Datenschutzproblem von verhaltensbiometrischen Daten bereits erkannt wurde und auch erste Vorschläge zur Lösung existieren. Was aber bisher fehlt, ist ein Ansatz, wie dieser verbesserte Privatheitschutz den Nutzer:innen einfach und intuitiv zur Verfügung gestellt werden kann und wie allgemeine Anonymisierungen aussehen können.

4. Chance und Risiken von Verhaltensbiometrie

Im Folgenden stellen wir verschiedene verhaltensbiometrische Faktoren vor und gehen auf ihre Nutzen und Gefahren für die Nutzer:innen ein. Wir präsentieren hier keine vollständige Liste verhaltensbiometrischer Faktoren,

15 Lehman u.a., in: ACM Transactions on Privacy and Security 25, no. 4, 2022
16 Roesner u.a., in: ACM SIGSAC Conference on Computer and Communications Security, 2014
17 Ruth u.a., in: 28th USENIX Security Symposium, 2019
18 Lebeck u.a., in: IEEE Symposium on Security and Privacy, 2017

sondern konzentrieren uns auf die wichtigsten Faktoren für Augmented Reality und Virtual Reality.

4.1 Gangerkennung

Der aufrechte Gang ist nicht nur im Vergleich zwischen Mensch und Tier einzigartig, auch zwischen Menschen gibt es große Unterschiede in der Art und Weise, wie sie gehen. Diese Gangmuster dienten in der Vergangenheit beispielsweise zur Erkennung von Freund und Feind[19] und ermöglichen es auch heute noch, vertraute Personen aus großer Entfernung zu identifizieren. Gangmuster können mit verschiedenen Technologien erfasst werden. Optisch durch Videoaufnahmen, durch die Veränderung der Beschleunigung während des Gangzyklus mit Beschleunigungssensoren oder durch die Gewichtsverlagerung beim Überqueren von Druckplatten. Aber auch Technologien wie Radar[20], LiDAR[21], oder WLAN[22] erlauben die Aufzeichnung von Gangmustern. Dabei ist zu beachten, dass die Aufzeichnung von Gangmustern meist nicht im Fokus steht, sondern ein Nebenprodukt anderer Aufzeichnungen wie z.B. Überwachungsvideos ist. Wichtig ist auch, dass Gangdaten relativ einfach ohne Einwilligung der aufgezeichneten Personen erhoben werden können und weniger Abhängig von der Qualität und Blickwinkel der Aufnahme sind als z.B. Gesichter.

Nutzen: Der Hauptnutzen von Gangdaten liegt in der Diagnose von Krankheiten wie Parkinson[23]. Hier werden meist Video- oder 3D-Motion-Capture-Verfahren eingesetzt, um eine genaue Ganganalyse zu ermöglichen. Ein weiterer Nutzen von Gangdaten ist das Zählen von Schritten. Da Gangdaten oft beiläufig bei der Aufzeichnung anderer Daten erfasst werden, ist auch die Erhaltung dieser Aufzeichnungen zu berücksichtigen. Im AR/VR-Kontext ist auch die Animation von digitalen Avataren eine mögliche Anwendung von Gangdaten.

Gefahren: Gangdaten haben ein hohes Identifikationspotenzial, da sie einfach zu erheben sind und bereits die Aufzeichnung eines einzelnen

19 Yovel/O'Toole, in: Trends in Cognitive Sciences 20, no. 5, 2016
20 Wan u.a., in: ACM Computing Surveys 51, no. 5, 2018
21 Gálai u.a., in: International Workshop on Computational Intelligence for Multimedia Understanding (IWCIM), 2015
22 Wang u.a., in: ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2016
23 Abdulhay u.a., in: Future Generation Computer Systems 83, 2018

Schrittes ausreicht, um Personen zu identifizieren[24]. Gangerkennung funktioniert auch mit Videos, die mit geringer Auflösung und aus einem ungünstigen Winkel (z.B. schräg von oben) aufgenommen wurden[25]. Auch lässt sich die Gangerkennung von Nutzer:innen nur schwer verhindern, da es anders als bei der Gesichtserkennung nicht möglich ist, das Gesicht einfach zu verdecken, um sie zu unterbinden. Neben der Identifikation von Personen ist es auch möglich, auf private Attribute wie Geschlecht[26] und Gewicht[27] zu schließen.

4.2 Handbewegungen

Die Fähigkeit, komplexe Handbewegungen auszuführen und damit Werkzeuge zu bedienen, ist ein herausragendes Merkmal des Menschen. In unserem heutigen Alltag benutzen wird unsere Handbewegungen hauptsächlich zur Steuerung von Computern. Damit einher geht die digitale Aufzeichnung unserer Handbewegungen. So sind unsere Bewegungen mit Computermäusen und unsere Tippmuster auf Tastaturen verhaltensbiometrische Faktoren, die ausgewertet werden können. Hinzu kommen Gesten auf mobilen Endgeräten und bei AR/VR-Geräten die Bedienung von Controllern[28] und Freihandgesten.

Nutzen: Handbewegungen spielen heute in der Mensch-Computer-Interaktion als Eingabemodalität eine wichtige Rolle. Aber auch für die nonverbale Kommunikation zwischen Menschen mittels Gebärdensprache oder einfachen Gesten sind Handbewegungen unersetzlich.

Gefahren: Personen können anhand ihrer Handbewegungen identifiziert werden, z. B. durch Tastatureingaben[29] oder Gesten[30]. Auch Krankheiten wie Parkinson[31] können anhand eines verstärkten Zitterns der Hände diagnostiziert werden. Darüber hinaus ist die Semantik von Handbewegungen in bestimmten Kontexten problematisch, z. B. kann aus einer Aufzeichnung der Fingerbewegungen bei der Eingabe eines Passworts auf das Passwort selbst geschlossen werden.

24 Horst u.a., in: Scientific reports 9.1, 2019
25 Wan u.a., in: CM Computing Surveys 51, no. 5, 2018
26 Pollick u.a., in: Human Perception and Performance 31, no. 6, 2005
27 https://www.biomotionlab.ca/html5-bml-walker/
28 Miller u.a., in: Scientific Reports 10, no. 1, 2020
29 Halunen/Vallivaara, in: Secure IT Systems, 2016
30 Clark/Lindqvist, in: IEEE Pervasive Computing 14, no. 1, 2015
31 Jankovic, in: Journal of Neurology, Neurosurgery & Psychiatry 79, no. 4, 2008

4.3 Augenbewegungen

Augenbewegungen bestehen im Wesentlichen aus zwei verschiedenen Bewegungen, den Fixationen, bei denen der Blick auf einen einzigen Punkt gerichtet wird, und den Sakkaden, bei denen die Augen sehr schnell umpositioniert werden. Die Muster, in denen sich diese beiden Grundbewegungen abwechseln, sind von Mensch zu Mensch verschieden und erlauben neben der Personenidentifikation viele weitergehende Rückschlüsse. Augenbewegungen werden mit optischen Verfahren, meist im Infrarotbereich, erfasst. Wichtig dabei ist, dass meist in zwei Richtungen aufgenommen wird, einmal in die Augen selbst, um die Position der Pupillen zu bestimmen, und einmal in die Blickrichtung der aufgenommenen Person. Durch das Zusammenfügen beider Aufnahmen kann festgestellt werden, auf welchen Punkt in einer Szene eine Person ihren Blick gerichtet hat. In der Vergangenheit wurde diese Eyetracking-Technologie vor allem in der Forschung eingesetzt, in den letzten Jahren wird Eyetracking aber auch zunehmend in AR/VR-Headsets integriert.

Nutzen: Augenbewegungen werden in verschiedenen wissenschaftlichen Disziplinen verwendet. In der Medizin liefern Augenbewegungen Informationen zur Diagnose von Krankheiten[32] und zur Untersuchung der visuellen Verarbeitung[33]. In der Psychologie liefern Augenbewegungen wichtige Anhaltspunkte für die Interessen von Proband:innen. Aber auch außerhalb der Wissenschaft werden Augenbewegungen genutzt: In der Werbeindustrie wird die Wirkung von Werbung anhand von Augenbewegungen untersucht. In AR/VR-Headsets werden Augenbewegungen als Eingabemodalität, für das selektive Rendering[34], bei dem der Fokuspunkt der Augen detaillierter gerendert wird als die Umgebung, sowie für die Animation digitaler Avatare[35] genutzt.

Gefahren: Wie bei anderen biometrischen Merkmalen können Personen anhand ihrer Augenbewegungen identifiziert werden[36]. Die Augenbewegungen enthalten ein weites Spektrum an Informationen über den Nut-

32 Harezlak/Kasprowski, in: Computerized Medical Imaging and Graphics, Advances in Biomedical Image Processing, 65, 2018
33 Harezlak/Kasprowski, in: Computerized Medical Imaging and Graphics, Advances in Biomedical Image Processing, 65, 2018
34 Patney u.a., in: ACM Transactions on Graphics 35, no. 6, 2016
35 John u.a., in: IEEE Transactions on Visualization and Computer Graphics 26, no. 5, 2020
36 Katsini u.a., in: Conference on Human Factors in Computing Systems (CHI), 2020

zer:in. So kann z.B. auf das Interesse einer Person[37] geschlossen werden oder auf die psychische Belastung[38]. Darüber hinaus sind Augenbewegungen ein Indikator für eine Vielzahl von psychischen Erkrankungen wie Schizophrenie[39], Autismus[40] oder Psychosen[41]. Auch Rückschlüsse auf die Persönlichkeit sind möglich[42].

4.4 Gehirnaktivitäten

Gehirnaktivitäten werde heutzutage hauptsächlich zu Forschungszwecken oder medizinischen Diagnosen erhoben. Die Gehirnaktivitäten werden dabei als die messbare elektrische Impulse aufgenommen, welche von unseren Neuronen erzeugt werden. Die am meisten verbreitete Methode zur Aufzeichnung ist Elektroenzephalografie (EEG), wobei Elektroden auf der Kopfhaut angebracht werden. Zum heutigen Zeitpunkt ist EEG außerhalb der Forschung und Medizin nicht weit verbreitet, es gibt aber erste kommerzielle AR/VR Geräte, welche begonnen haben EEG zu integrieren[43]. Weitere Methoden[44] zur Aufzeichnung von Gehirnaktivitäten existieren, werden aber außerhalb der Medizin bisher kaum eingesetzt.

Nutzen: In der Medizin wird die Gehirnaktivität für die Diagnose von Krankheiten wie Epilepsie[45] oder Alzheimer[46] verwendet. Auch gibt es Bestrebungen Gehirnaktivitäten zur direkten Mensch-Computer-Interaktion zu nutzen[47]. Eine weitere mögliche Anwendung ist z.B. die Authentifizierung von Personen[48].

Gefahren: In ersten Experimenten konnte gezeigt werden, dass sich Bilder aus EEG-Daten generieren lassen, welche Einblicke in die visuellen Prozesse von Personen zulassen[49]. Auch konnte bereits gezeigt werden,

37 Hess/Polt, in: Science 132, no. 3423, 1960
38 Krejtz u.a., in: PLOS ONE 13, no. 9, 2018
39 Holzman u.a., in: Science 181, no. 4095, 1973
40 Wang u.a., in: Neuron, Volume 88, Issue 3, 2015
41 Ettinger u.a., in: American Journal of Psychiatry 161, 2004
42 Berkovsky u.a., in: Conference on Human Factors in Computing (CHI), 2019
43 https://www.neurospec.com/Products/Details/1077/dsi-vr300
https://mixed-news.com/en/varjo-aero-high-end-vr-headset-gets-brain-interface/
44 Hallinan u.a., in: Surveillance & Society, Vol. 12 No. 1, 2014
45 Subha u.a., in: Journal of Medical Systems 34, 2010
46 Subha u.a., in: Journal of Medical Systems 34, 2010
47 https://neuralink.com/applications/
48 Arias-Cabarcos u.a., in: USENIX Security Symposium, 2021
49 Zeng u.a., in: Biomedical Signal Processing and Control 81, 2023

dass sich aus EEG-Daten Rückschlüsse auf geheime Informationen wie Passwörter ziehen lassen[50]. Darüber hinaus lassen sich aus EEG-Daten auch Informationen über den Konsum von Drogen ableiten[51].

4.5 Menschliche Stimme

Die menschliche Stimme ist vielleicht der bekannteste verhaltensbiometrische Faktor. Durch unterschiedliche Physiologie und erlerntes Verhalten haben Menschen einzigartige Stimmen, die unterschieden werden können. Die Stimme wird im Kehlkopf und im Vokaltrakt des Menschen erzeugt. Aufgenommen wird die Stimme mit Mikrofonen, die heute in den meisten mobilen Endgeräten eingebaut sind. So finden sich Mikrofone auch in den meisten AR/VR-Geräten.

Nutzen: Der Hauptnutzen der menschlichen Stimme liegt in der zwischenmenschlichen Kommunikation. Im AR/VR-Bereich wird Sprache als Eingabemodalität verwendet, z.B. zum Öffnen von Menüs[52].

Gefahren: Neben der Identifikation lassen sich aus aufgezeichneten Stimmen auch die Attribute wie Alter[53], Geschlecht[54], sowie emotionaler Zustand[55] einer Person ableiten. Des Weiteren ist es möglich mit Stimmaufnahmen Personen zu imitieren[56], und so Identitätsdiebstahl zu betreiben.

5. Persönliche Daten besser kontrollieren und schützen

Betrachten wir, wie Daten heute auf Plattformen wie Smartphones und Webbrowsern geteilt werden, so hat sich ein Modell durchgesetzt, bei dem die Nutzer:innen einzelne Sensoren für Anwendungen freigeben. Wir gehen davon aus, dass dieses Modell für MR-Plattformen an seine Grenzen stoßen wird, da es für das Funktionieren von MR-Anwendungen notwendig sein wird, die meisten Sensoren dauerhaft mit der Anwendung zu teilen.

50 Martinovic u.a., in: 21st USENIX Conference on Security Symposium, 2012
51 Matovu/Serwadda, in: IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2016
52 Schwarz, in: IEEE Workshop on Automatic Speech Recognition and Understanding, 2011
53 Jiao u.a., in: Speech Communication 106, 2019
54 Ertam, in: Applied Acoustics 156, 2019
55 Yacoub u.a., in: European Conference on Speech Communication and Technology, *2003*
56 Bendel, in: AI & SOCIETY 34, 2019

Somit werden die Nutzer:innen oftmals keine Entscheidungsmöglichkeit haben.

Wir schlagen daher eine Erweiterung des Modells vor, in der die Nutzer:innen neben der Entscheidung, was geteilt wird, auch eine Entscheidung darüber treffen können, wie diese Daten genutzt werden können. Dafür sehen wir zwei komplementäre Bausteine. Zum einen die rechtliche Zweckbindung nach Einwilligung, wie die Daten genutzt werden dürfen und zum anderen die technische Veränderung der Daten, die bestimmte private Informationen aus den Daten entfernt.

Das Teilen der Daten einzelner Sensoren ist aus drei Gründen problematisch:

1. Zum einen können selbst auf den ersten Blick harmlos erscheinende Daten wie die eines Beschleunigungssensors dazu genutzt werden, Nutzer:innen anhand ihrer verhaltensbiometrischen Faktoren wie Gang und Handbewegungen zu identifizieren. Für Nutzer:innen ist es nur sehr schwer zu verstehen, welche weitreichenden Implikationen die einzelnen Sensordaten mit sich bringen.
2. Für den Einsatz neuer MR-Geräte ist eine permanente gemeinsame Nutzung verschiedenster Sensoren für die Grundfunktionalität der Geräte erforderlich. Bei AR-Geräten muss die Umgebung permanent erfasst werden, damit diese mit Daten angereichert werden kann. Bei VR müssen die Bewegungen des Kopfes und des Controllers permanent erfasst werden, um mit den virtuellen Welten interagieren zu können.
3. Das Teilen von Daten, wie es heute auf mobilen Geräten am weitesten verbreitet ist, erfolgt nach dem Alles-oder-Nichts-Prinzip. Nutzer:innen können nur entscheiden, Daten zu teilen oder dies nicht zu tun. Eine weitere Einflussmöglichkeit, was mit den Daten geschieht, ist nicht vorgesehen.

Aufgrund dieser Probleme sind wir der Meinung, dass das derzeitige Modell des Teilens von Daten bei der Entwicklung künftiger AR/VR-Geräten verbessert werden muss. Daher schlagen wir einen neuen Ansatz für das Problem des Datenaustauschs mit Anwendungen vor. Anstatt nur zu betrachten, was geteilt wird, sollten wir uns darauf konzentrieren, was mit den Daten getan werden kann und was nicht.

Dabei spielen rechtliche und technische Datenschutzmaßnahmen unterschiedliche Rollen. Mit rechtlichen Maßnahmen kann festgelegt werden, zu welchem Zweck die Daten verwendet werden dürfen, indem eine ausdrückliche Einwilligung in die Verarbeitung der Daten zu einem bestimmten

Zweck erteilt wird. Mit technischen Maßnahmen hingegen können Daten verändert werden, um eine bestimmte Datenverarbeitung zu verhindern. Beide Maßnahmen können zusammen genutzt werden, um eine feinere Aufteilung von Daten zu ermöglichen und den Nutzer:innen die Möglichkeit zu geben, gezielte Erlaubnisse und Verbote auszusprechen.

Konkret schlagen wir mit diesen beiden Maßnahmen vor, um eine neue Schnittstelle für den Datenaustausch mit Anwendungen zu realisieren. Anstelle eines einzelnen Sensors wird ein Sensor von einer Anwendung für einen oder mehrere Verarbeitungszwecke angefordert. Ein Beispiel wäre die Anfrage eines Beschleunigungssensors, um Schritte zu zählen, oder die Anfrage einer Kamera, um Social-Media-Filter auf Personen anzuwenden. Neben dieser aktiven Anfrage durch die Anwendung kann der Nutzer über die Schnittstelle auch festlegen, welche Verarbeitungszwecke unterbunden werden sollen. Diese Verbote werden dann durch eine gezielte Verschleierung der Daten umgesetzt. So kann z.B. bei der Weitergabe von Videos die Identifizierung von Personen durch gezielte Anonymisierung von Gesichtern und Körperbewegungen erreicht werden.

Der Vorteil solch einer feineren Datenteilung liegt in der erweiterten Kontrolle, die die Nutzer:innen über ihre (Teil-) Daten ausüben können. Der Nachteil für die Anbieter:innen von Anwendungen liegt darin, dass sie einen Teil ihrer Flexibilität einbüßen. Allerdings ist der Funktionsumfang mobiler Endgeräte heute relativ gut verstanden, so dass Standardfunktionen definiert werden können. Beispiele hierfür sind die Objekterkennung in Bildern oder die Sprachsteuerung von Anwendungen. Ein weiterer Nachteil ist die mögliche Beeinträchtigung der Funktionalität von Anwendungen durch Obfuskation.

Wir erwarten, dass durch die feinere Freigabe von Daten die Anwendungsentwickler genauer überlegen müssen, welche Daten sie für eine konkrete Funktion tatsächlich benötigen, da eine große Menge an Freigabeanfragen den Nutzer:innen negativ auffallen wird. Es entsteht ein potentieller Anreiz zur Datensparsamkeit.

6. Ansätze zur Anonymisierung verhaltensbiometrischer Daten

Für den Schutz von verhaltensbiometrischen Daten gibt es verschiedene Ansätze, die wir in diesem Abschnitt näher beleuchten wollen. Dabei orientieren wir uns an dem Szenario, das wir in Abschnitt 2 vorgestellt haben und betrachten nur Methoden, die anwendbar sind, wenn eine Weitergabe

der verhaltensbiometrischen Daten an Dritte erfolgen soll. Dies schließt Methoden aus, die nur den Schutz der Daten während der Übertragung gewährleisten, wie z.B. Verschlüsselung. Da auch Methoden wie Zugriffskontrolle in einem solchen Szenario nicht anwendbar sind, betrachten wir nur Methoden, die die Daten modifizieren und damit den Schutz der Privatheit realisieren.

Weiterhin ist es wichtig zu beachten, dass die Nutzer:innen mit der Weitergabe die Kontrolle über ihre Daten abgeben, was zur Folge hat, dass jegliche Schutzmaßnahme vorab angewendet werden muss. Es ist nicht möglich, den Schutz der Privatheit zu einem späteren Zeitpunkt zu ändern oder zu verbessern, wenn sich herausstellt, dass er unzureichend ist. Die Angreifer:innen haben somit vollen Zugang zu den geteilten Daten und sind in der Wahl ihrer Methoden, diese zu analysieren, nicht eingeschränkt.

Im Gegensatz zu herkömmlichen personenbezogenen Daten wie Namen, Adressen oder Telefonnummern sind verhaltensbiometrische Daten in ihrer Form wesentlich komplexer. Häufig als Zeitreihen von Sensordaten erfasst, vermischen verhaltensbiometrische Daten personenbezogene und nicht personenbezogene Informationen, und es ist nicht offensichtlich, welcher Anteil oder welche Struktur der Daten personenbezogene Informationen enthält. Die personenbezogenen Informationen sind nicht explizit, was den Schutz der Privatheit erschwert.

Neben diesem Mix aus personenbezogenen und sonstigen Informationen enthalten die Daten eine Reihe von Abhängigkeiten, die den Schutz der Privatheit zusätzlich erschweren und die wir am Beispiel der Gangdaten kurz erläutern wollen. Zum einen gibt es zeitliche Abhängigkeiten, eine einzelne Haltung einer Person in einer Gangsequenz ist immer abhängig von den vorhergehenden Haltungen und hat einen direkten Einfluss auf die nachfolgenden Haltungen. Zum anderen gibt es strukturelle Abhängigkeiten, z.B. hängen die Farben eines Pixels in gewissem Maße auch von den Farben seiner Nachbarn ab. Wird das einzelne Pixel entfernt, kann es durch Interpolation seiner Nachbarn wiederhergestellt werden. Schließlich gibt es physiologische Abhängigkeiten in den Daten. Beispielsweise kann ein Mensch seine Gelenke nicht beliebig weit beugen, oder die Position des Kopfes hängt stark von der Position des Oberkörpers ab.

Diese drei Abhängigkeiten führen dazu, dass verhaltensbiometrische Daten sehr redundant sind und noch viele private Informationen in den Daten enthalten sind, selbst wenn große Teile der Daten entfernt wurden. Deshalb ist die Anonymisierung von verhaltensbiometrischen Daten nicht

trivial. Beispielsweise können einfache Anonymisierungsmethoden wie das Verrauschen einzelner Datenpunkte oder das Entfernen von Datenpunkten scheitern, weil die Redundanz der Daten es ermöglicht, die ursprünglichen Daten wiederherzustellen[57]. Für eine erfolgreiche Anonymisierung der Daten ist es notwendig, die oben genannten Abhängigkeiten in den Daten zu berücksichtigen.

Für die Anonymisierung verhaltensbiometrischer Daten werden im Folgenden zwei allgemeine Ansätze vorgeschlagen, die den in Abschnitt 2 genannten Anforderungen genügen.

6.1 Modellierung

Der erste Ansatz besteht darin, die Abhängigkeiten in den Verhaltensdaten zu modellieren. Die Modellierung ermöglicht es, die Daten als Kombination eines Modells und seiner Parameter auszudrücken. Das Modell kodiert die Abhängigkeiten (z.B. physikalische Bedingungen oder menschliche Physiologie) der Daten und die Modellparameter kodieren die einzelnen Datenpunkte. Da die Datenpunkte in dieser Darstellung unabhängig voneinander sind, können sie leichter anonymisiert werden, z. B. durch die Anwendung von Rauschen. Nach der Anonymisierung können die Datenpunkte in das Modell eingefügt werden, um sie wieder in ihre ursprüngliche Form zu übersetzen. Der Vorteil dieser Methode ist, dass am Ende die Datenpunkte in der gleichen Form wie vor der Anonymisierung vorliegen.

Ein einfaches Beispiel für die Modellierung ist der Bewegungspfad eines VR-Headsets im Raum, wobei die Punkte auf dem Pfad des VR-Headsets voneinander abhängig sind, da sich das VR-Headset kontinuierlich bewegen muss und somit jeder Punkt von seinen Vorgängern abhängt. Anstatt die Daten als einzelne Punkte auf dem Pfad zu betrachten, wird der Pfad des VR-Headsets als Geschwindigkeit und Richtung zu jedem Zeitpunkt ausgedrückt. Die beiden Parameter des Modells, Geschwindigkeit und Fahrtrichtung, sind unabhängig voneinander und können so einfacher anonymisiert werden.

Nun sind die Abhängigkeiten in verhaltensbiometrischen Daten oft sehr komplex und nicht einfach zu modellieren, daher ist unser Ansatz, die für diesen Ansatz benötigten Modelle mit Hilfe von Methoden des maschinellen Lernens zu erstellen. Eine Möglichkeit ist z.B. das Training von varia-

57 Hanisch u.a., in: arXiv, 2022

blen Autoencodern, um eine Repräsentation der Datenpunkte zu erhalten, bei der die einzelnen Datenpunkte unabhängig voneinander sind.

6.2 Transformation

Der zweite Ansatz besteht darin, die personenbezogenen Informationen in den Daten direkt zu entfernen und nur die für die Nutzwert der Daten erforderlichen Informationen zu erhalten. Dies erfordert eine Quantifizierung, wie viele private Informationen und wie viele Informationen für die Nutzwert in den Daten enthalten sind. Wenn beide Werte quantifiziert werden können, kann die Anonymisierung der Daten als Optimierungsproblem ausgedrückt werden, bei dem die enthaltenen privaten Informationen minimiert werden sollen, während die für die Nutzwert erhaltenen Informationen maximiert werden sollen.

Eine Möglichkeit, dieses Optimierungsproblem zu lösen, besteht darin, ein maschinelles Lernmodell (ML-Modell) zu verwenden, das die Daten in eine neue Darstellung transformiert. Beim Training werden der Informationsgehalt für Privatheit und Nutzwert als Verlustfunktionen verwendet, damit das Modell eine Transformation lernt, die das Optimierungsproblem löst. Um zu quantifizieren, wie viel Privat- und Nutzwertinformation noch in den Daten enthalten ist, können biometrische Erkennungssysteme verwendet werden, um eine Schätzung des Informationsgehalts für Privatheit und Nutzwert der Daten zu erhalten.

Ein Beispiel für ein solches System ist eine Gestenerkennung für ein AR-Headset. Ein maschinelles Modell extrahiert aus Videoaufnahmen der Hände die Merkmale, die für die eigentliche Gestenerkennung verwendet werden. Dieses System wird mit einem biometrischen Erkennungssystem zur Bestimmung des Risikos für die Privatheit und einem Gestenerkennungssystem zur Bestimmung des Nutzwerts trainiert.

7. Fazit

Die Erfassung und Verarbeitung von verhaltensbiometrischen Daten rückt mit der Weiterentwicklung des Internets hin zu digitalen Welten auf Basis von AR/VR-Technologien in den Fokus. Verhaltensbiometrische Daten enthalten ein breites Spektrum an sensiblen persönlichen Informationen, die es ermöglichen, Personen zu identifizieren, aber auch Rückschlüsse auf die Eigenschaften von Personen zu ziehen.

Die Art und Weise wie wir heute Daten mit Anwendungen teilen, wird die Privatsphäre der Nutzer:innen bei AR/VR Anwendungen nur unzureichend schützen, weshalb wir neue Möglichkeiten benötigen, um das Teilen von Daten zu kontrollieren.

Eine Möglichkeit besteht darin, die Daten vor der Weitergabe zu anonymisieren. Aufgrund der Komplexität verhaltensbiometrischer Daten ist diese Anonymisierung jedoch nicht trivial. Wichtig für eine effektive Anonymisierung ist die Berücksichtigung aller Abhängigkeiten in den Daten.

Finanzierung

Gefördert durch die Deutsche Forschungsgemeinschaft (DFG) im Rahmen der Exzellenzstrategie des Bundes und der Länder – EXC 2050/1 – Projektnummer 390696704 – als Exzellenzcluster „Centre for Tactile Internet with Human-in-the-Loop“ (CeTI) der Technischen Universität Dresden. Diese Arbeit wurde duch die DFG und dem Forschungsbereich Engineering Secure Systems (46.23.01) der Helmholtz Gemeinschaft (HGF) durch KASTEL Security Research Labs unterstützt.

Literatur

Abdulhay, Enas; Arunkumar, N.; Narasimhan, Kumaravelu; Vellaiappan, Elamaran und Venkatraman, V. (2018): Gait and Tremor Investigation Using Machine Learning Techniques for the Diagnosis of Parkinson Disease. *Future Generation Computer Systems* 83, S. 366–73. doi: 10.1016/j.future.2018.02.009.

Ali, Mouad. M.H.; Mahale, Vivek H.; Yannawar, Pravin und Gaikwad, A. T. (2016):. Overview of Fingerprint Recognition System. In: *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, S. 1334–38. doi: 10.1109/ICEEOT.2016.7754900.

Arias-Cabarcos, Patricia; Habrich, Thilo und Becker, Karen (2021): Inexpensive Brainwave Authentication: New Techniques and Insights on User Acceptance. 30th USENIX Security Symposium (USENIX Security 21), S. 55–72. isbn: 978-1-939133-24-3.

Wang, Shuo; Jiang, Ming; Duchesne, Xavier Morin; Laugeson, Elizabeth A.; Kennedy, Daniel P.; Adolphs, Ralph und Zhao, Qi (2015): Atypical Visual Saliency in Autism Spectrum Disorder Quantified through Model-Based Eye Tracking. In: *Neuron* 88, S. 604-616. doi: 10.1016/j.neuron.2015.09.042.

Bendel, Oliver (2019): The Synthetization of Human Voices. In: *AI & SOCIETY* 34, no. 1, S. 83–89. doi: 10.1007/s00146-017-0748-x.

Berkovsky, Shlomo; Taib, Ronnie; Koprinska, Irena; Wang, Eileen; Zeng, Yucheng; Li, Jingjie und Kleitman, Sabina (2019): Detecting Personality Traits Using Eye-Tracking Data. In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, S. 1–12. CHI '19. New York, NY, USA: Association for Computing Machinery. doi: 10.1145/3290605.3300451.

Chandolikar, Neelam; Joshi, Chaitanya; Roy, Prateek; Gawas, Abhijeet and Vishwakarma, Mini (2022): Voice Recognition: A Comprehensive Survey. In: *International Mobile and Embedded Technology Conference (MECON)*, S. 45–51. doi: 10.1109/MECON53876.2022.9751903.

Clark, Gradeigh D. und Lindqvist, Janne (2015): Engineering Gesture-Based Authentication Systems. *IEEE Pervasive Computing* 14, no. 1, S. 18–25. doi: 10.1109/MPRV.2015.6.

Deng, Jiankang; Guo, Jia; Xue, Niannan und Zafeiriou, Stefanos (2019): ArcFace: Additive Angular Margin Loss for Deep Face Recognition. In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR),* S. 4690–99.

Ertam, Fatih (2019): An Effective Gender Recognition Approach Using Voice Data via Deeper LSTM Networks. In: *Applied Acoustics* 156, S. 351–58. doi: 10.1016/j.apacoust.2019.07.033.

Ettinger, Ulrich; Kumari, Veena; Chitnis, Xavier A.; Corr, Philip J.; Crawford, Trevor J.; Fannon, Dominic G.; O'Ceallaigh, Séamus; Sumich, Alex L.; Doku, Victor C. und Sharma, Tonmoy (2004):Volumetric Neural Correlates of Antisaccade Eye Movements in First-Episode Psychosis. In: *American Journal of Psychiatry* 161, no. 10, S. 1918–21. doi: 10.1176/ajp.161.10.1918.

Figueiredo, Lucas Silva; Livshits, Benjamin; Molnar, David und Veanes, Margus (2016): Prepose: Privacy, Security, and Reliability for Gesture-Based Programming. In: *IEEE Symposium on Security and Privacy (SP)*, S. 122–37 doi: 10.1109/SP.2016.16.

Gálai, Bence and Benedek, Csaba (2015): Feature Selection for Lidar-Based Gait Recognition. In: *International Workshop on Computational Intelligence for Multimedia Understanding (IWCIM)*, S. 1–5. doi: 10.1109/IWCIM.2015.7347076.

Guzman, Jaybie Agullo de; Thilakarathna, Kanchana und Seneviratne, Aruna (2019): SafeMR: Privacy-Aware Visual Information Protection for Mobile Mixed Reality. In: *IEEE 44th Conference on Local Computer Networks (LCN)*, S. 254–57. doi: 10.1109/LCN44214.2019.8990850.

Hallinan, Dara; Schütz, Philip; Friedewald, Michael und de Hert, Paul (2013): Neurodata and Neuroprivacy: Data Protection Outdated? In: *Surveillance & Society* 12.1, S. 55-72. doi: 10.24908/ss.v12i1.4500.

Halunen, Kimmo und Vallivaara, Visa (2016): Secure, Usable and Privacy-Friendly User Authentication from Keystroke Dynamics. In: *Secure IT Systems*, S. 256–68. doi: 10.1007/978-3-319-47560-8_16.

Hanisch, Simon; Muschter, Evelyn; Hatzipanayioti, Admantini; Li, Shu-Chen und Strufe, Thorsten (2022): Understanding Person Identification through Gait. arXiv. http://arxiv.org/abs/2203.04179.

Harborth, David und Frik, Alisa (2021): Evaluating and Redefining Smartphone Permissions with Contextualized Justifications for Mobile Augmented Reality Apps. In: *Proceedings of the Seventeenth USENIX Conference on Usable Privacy and Security (SOUPS)*, S. 513-533. doi: 10.5555/3563572.3563599.

Harezlak, Katarzynaund Kasprowski, Pawel (2018): Application of Eye Tracking in Medicine: A Survey, Research Issues and Challenges. In: *Computerized Medical Imaging and Graphics*, Advances in Biomedical Image Processing, S. 176–90. doi: 10.1016/j.compmedimag.2017.04.006.

Hess, Eckhard H. und Polt, James M. (1960): Pupil Size as Related to Interest Value of Visual Stimuli. In: *Science* 132, no. 3423, S. 349–50. doi: 10.1126/science.132.3423.349.

Holzman, Philip S.; Proctor, Leonard R. und Hughes, Dominic W. (1973): Eye-Tracking Patterns in Schizophrenia. In: *Science* 181, no. 4095 S. 179–81. doi: 10.1126/science.181.4095.179.

Horst, Fabian; Lapuschkin, Sebastian; Samek, Wojciech; Müller, Klaus-Robert und Schöllhorn, Wolfgang I. (2019): Explaining the Unique Nature of Individual Gait Patterns with Deep Learning. a*rXiv* doi: 10.1038/s41598-019-38748-8.

Jana, S., A. Narayanan und Shmatikov, V. (2013): A Scanner Darkly: Protecting User Privacy from Perceptual Applications. In: *IEEE Symposium on Security and Privacy*, S. 349–63. doi: 10.1109/SP.2013.31.

Jana, Suman; Molnar, David; Moshchuk, Alexander; Dunn, Alan; Livshits, Benjamin; Wang, Helen J und Ofek, Eyal (2013): Enabling Fine-Grained Permissions for Augmented Reality Applications With Recognizers. In: *Proceedings of the 22nd USENIX conference on Security*, S. 415-430. doi: 10.5555/2534766.2534802.

Jankovic, J (2008): Parkinson's Disease: Clinical Features and Diagnosis. In: *Journal of Neurology, Neurosurgery & Psychiatry* 79, no. 4, S. 368–76. doi: 10.1136/jnnp.2007.131045.

Jiao, Dan; Watson, Vicky; Wong, Sidney Gig-Jan; Gnevsheva, Ksenia und Nixon, Jessie S. (2019): Age Estimation in Foreign-Accented Speech by Non-Native Speakers of English. In: *Speech Communication* 106, S. 118–26. doi: 10.1016/j.specom.2018.12.005.

John, Brendan; Jörg, Sophie; Koppal, Sanjeev und Jain, Eakta (2020): The Security-Utility Trade-off for Iris Authentication and Eye Animation for Social Virtual Avatars. In: *IEEE Transactions on Visualization and Computer Graphics* 26, no. 5 , S. 1880–90. doi: 10.1109/TVCG.2020.2973052.

Katsini, Christina; Abdrabou, Yasmeen; Raptis, George E.; Khamis, Mohamed und Alt, Florian (2020): The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. In: *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, S. 1–21. doi: 10.1145/3313831.3376840.

Krejtz, Krzysztof; Duchowski, Andrew T.; Niedzielska, Anna; Biele, Cezary und Krejtz, Izabela (2018): Eye Tracking Cognitive Load Using Pupil Diameter and Microsaccades with Fixed Gaze. In: *PLOS ONE* 13, no. 9. doi: 10.1371/journal.pone.0203629.

Kröger, Jacob Leon; Lutz, Otto Hans-Martin und Müller, Florian (2019): What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking. In: *Privacy and Identity Management Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School.* doi: 10.1007/978-3-030-42504-3_15.

Lebeck, Kiron; Ruth, Kimberly; Kohno, Tadayoshi und Roesner, Franziska (2017): Securing Augmented Reality Output. In: *IEEE Symposium on Security and Privacy (SP)*, S. 320–37. doi: 10.1109/SP.2017.13.

——— (2018): Towards Security and Privacy for Multi-User Augmented Reality: Foundations with End Users. In: *IEEE Symposium on Security and Privacy (SP)*, S. 392–408. doi:10.1109/SP.2018.00051.

Lehman, Sarah M.; Alrumayh, Abrar S.; Kolhe, Kunal; Ling, Haibin und Tan, Chiu C. (2022): Hidden in Plain Sight: Exploring Privacy Risks of Mobile Augmented Reality Applications. In: *ACM Transactions on Privacy and Security* 25, no. 4, S. 26:1-26:35. doi: 10.1145/3524020.

Liebers, Jonathan; Abdelaziz, Mark; Mecke, Lukas; Saad, Alia; Auda, Jonas; Gruenefeld, Uwe; Alt, Florian und Schneegass, Stefan (2021): Understanding User Identification in Virtual Reality Through Behavioral Biometrics and the Effect of Body Normalization. In: *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, S. 1–11. doi: 10.1145/3411764.3445528.

Martinovic, Ivan; Davies, Doug; Frank, Mario; Perito, Daniele; Ros, Tomas und Song, Dawn (2012): On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. In: *Proceedings of the 21st USENIX Conference on Security Symposium*, 34.

Matovu, Richard und Serwadda, Abdul (2016): Your Substance Abuse Disorder Is an Open Secret! Gleaning Sensitive Personal Information from Templates in an EEG-Based Authentication System. In: *IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, S. 1–7. doi: 10.1109/btas.2016.7791210.

Miller, Mark Roman; Herrera, Fernanda; Jun, Hanseul; Landay, James A. und Bailenson, Jeremy N. (2020): Personal Identifiability of User Tracking Data during Observation of 360-Degree VR Video. In: *Scientific Reports* 10, no. 1. doi: 10.1038/s41598-020-74486-y.

Patil, Sandeep; Gudasalamani, Shreya; und Iyer, Nalini C (2016): A Survey on Iris Recognition System. In: *International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, S. 2207–2210. doi: 10.1109/ICEEOT.2016.7755084.

Patney, Anjul; Salvi, Marco; Kim, Joohwan; Kaplanyan, Anton; Wyman, Chris; Benty, Nir; Luebke, David und Lefohn, Aaron (2016): Towards Foveated Rendering for Gaze-Tracked Virtual Reality. *ACM Transactions on Graphics* 35, no. 6, S.179:1-179:12. doi: 10.1145/2980179.2980246.

Petracca, Giuseppe; Reineh, Ahmad-Atamli; Sun, Yuqiong; Grossklags, Jens und Jaeger, Trent (2017). AWare: Preventing Abuse of Privacy-Sensitive Sensors via Operation Bindings. In: *26th USENIX Security Symposium*, S. 379–396.

Pfeuffer, Ken; Geiger, Matthias J.; Prange, Sarah; Mecke, Lukas; Buschek, Daniel; und Alt, Florian (2019): Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In: *Proceedings of the Conference on Human Factors in Computing Systems (CHI)*, S. 1–12. doi: 10.1145/3290605.3300340.

Pollick, Frank E.; Kay, Jim W.; Heim, Katrin und Stringer, Rebecca (2005): Gender Recognition from Point-Light Walkers. In: *Journal of Experimental Psychology: Human Perception and Performance* 31, no. 6, S. 1247–65. doi: 10.1037/0096-1523.31.6.1247.

Raval, Nisarg; Srivastava, Animesh; Razeen, Ali; Lebeck, Kiron; Machanavajjhala, Ashwin und Cox., Lanodn P. (2016): What You Mark Is What Apps See. In: *Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys)*, S. 249–61. doi: 10.1145/2906388.2906405.

Roesner, Franzisk; Molnar, David; Moshchuk, Alexander; Kohno, Tadayoshi und Wang, Helen J. (2014): World-Driven Access Control for Continuous Sensing. In: *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, S. 1169–81. doi: 10.1145/2660267.2660319.

Ruth, Kimberly; Kohno, Tadayoshi und Roesner, Franziska (2019): Secure Multi-User Content Sharing for Augmented Reality Applications. In: *28th USENIX Security Symposium*, S. 141–158. isbn: 978-1-939133-06-9.

Schwarz, Petr (2011): The Kaldi Speech Recognition Toolkit. In: *IEEE Workshop on Automatic Speech Recognition and Understanding*.

Subha, D. Puthankattil; Joseph, Paul K.; Acharya U, Rajendra und Lim, Choo Min (2010): EEG Signal Analysis: A Survey. In: *Journal of Medical Systems* 34, no. 2, S.195–212. doi: 10.1007/s10916-008-9231-z.

Wan, Changsheng; Wang, Li und Phoha, Vir V. (2018): A Survey on Gait Recognition. *ACM Computing Surveys* 51, no. 5, S. 1–35. doi: 10.1145/3230633.

Wang, Wei, Liu, Alex X. und Shahzad, Muhammad (2016): Gait Recognition Using Wifi Signals. In: *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing*, S. 363–73. doi: 10.1145/2971648.2971670.

Yacoub, Sherif; Simske, Steve; Lin, Xiaofan und Burns, John. Recognition of Emotions in Interactive Voice Response Systems. In: *8th European Conference on Speech Communication and Technology (Eurospeech)*, S. 729–32. doi: 10.21437/Eurospeech.2003-307.

Yovel, Galit und O'Toole, Alice J. (2016): Recognizing People in Motion. In: *Trends in Cognitive Sciences* 20, no. 5, S. 383–95. doi: 10.1016/j.tics.2016.02.005.

Zeng, Hong; Xia, Nianzhang; Tao, Ming; Pan, Deng; Zheng, Haohao; Wang, Chu; Xu, Feifan; Zakaria, Wael und Dai, Guojun (2023): DCAE: A Dual Conditional Autoencoder Framework for the Reconstruction from EEG into Image. *Biomedical Signal Processing and Control* 81. doi: 10.1016/j.bspc.2022.104440.

Mitarbeiterinnen und Mitarbeiter dieses Bandes

Dr. Hartmut Aden

ist Jurist und Politikwissenschaftler, seit 2009 Professor für Öffentliches Recht, Europarecht, Politik- und Verwaltungswissenschaft an der HWR Berlin, Fachbereich Polizei und Sicherheitsmanagement/FÖPS Berlin und seit 2020 Vizepräsident für Forschung und Transfer der HWR Berlin.

Dr. Jürgen Anke

ist Professor für Softwaretechnologie und Informationssysteme und Leiter der Arbeitsgruppe Digitale Dienstleistungssysteme an der Hochschule für Technik und Wirtschaft Dresden. E-Mail: juergen.anke@htw-dresden.de

Stefanie Astfalk

ist Human Machine Interaction Expert am Institut für Arbeitswissenschaft und Technologiemanagement IAT der Universität Stuttgart und dem Fraunhofer Institut für Arbeitswirtschaft und Organisation IAO.
E-Mail: stefanie.astfalk@iao.fraunhofer.de

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 interdiszipliären Konsortialprojekts „PERISCOPE", gefödert vom Bundesministerium für Bildung und Forschung. E-Mail: baum@wiwi.uni-frankfurt.de

Dr. Felix Bieker

ist juristischer Mitarbeiter am Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD). E-Mail: fbieker@datenschutzzentrum.de

Fabiola Böning

ist wissenschaftliche Mitarbeiterin am Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht der Universität Kassel (Leiter: Prof. Dr. Gerrit Hornung, LL.M.), sowie am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG). E-Mail: F-Boening@uni-kassel.de

Paulina Bressel

ist wissenschaftliche Mitarbeiterin und Doktorandin am Lehrstuhl für Information Behavior des Instituts für Bibliotheks- und Informationswissenschaft an der Humboldt-Universität zu Berlin und Teil des Verbundprojektes Desive², gefördert vom Bundesministerium für Bildung und Forschung. E-Mail: p.bressel@hu-berlin.de

Fabian Dantscher

ist wissenschaftlicher Mitarbeiter am nexus Institut für interdisziplinäre Forschung und Kooperationsmanagement in Berlin sowie im Projekt „KIDD – KI im Dienste der Diversität", das vom Bundesministerium für Arbeit und Soziales (BMAS) unter dem Dach der Initiative Neue Qualität der Arbeit (INQA) gefördert wird. E-Mail: dantscher@nexusinstitut.de

Leyla Dewitz

ist wissenschaftliche Mitarbeiterin und Doktorandin am Lehrstuhl Information Behavior des Instituts für Bibliotheks- und Informationswissenschaft der Humboldt-Universität zu Berlin und Teil des Verbundprojekts "DESIVE² – Desinformationsverhaltn verstehen", gefördert vom Bundesministerium für Bildung und Forschung. E-Mail: leyla.dewitz@hu-berlin.de

Simon Engert

ist wissenschaftlicher Mitarbeiter und Doktorand am Institut für Digitales Management und Neue Medien (Prof. Thomas Hess) der LMU Munich School of Management und ist Teil des BMBF-Projekts „Faire digitale Dienste: Ko-Valuation in der Gestaltung datenökonomischer Geschäftsmodelle (FAIRDIENSTE)". E-Mail: engert@lmu.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. Marie-Louise Gächter

ist Leiterin der Datenschutz-Aufsichtsbehörde des Fürstentums Liechtenstein und Titularprofessorin an der Universität Fribourg.
E-Mail: marie-louise.gaechter@llv.li

Dr. Armin Gerl

ist Referent des Vizepräsidenten für akademische Infrastruktur/IT der Universität Passau und Postdoc am Lehrstuhl für Verteilte Informationssysteme mit den Forschungsschwerpunkten IT-Governance, Privacy, Green-IT und E-Mobility. E-Mail: armin.gerl@uni-passau.de

Dr. Daniel Guagnin

leitet den Bereich Netze und Gesellschaft am nexus Institut für Kooperationsmanagement und interdisziplinäre Forschung in Berlin und forscht zu Datenschutz, ethischer Technikentwicklung und den gesellschaftlichen Auswirkungen von Technik. E-Mail: guagnin@nexusinstitut.de

Simon Hanisch

ist wissenschaftlicher Mitarbeiter an der Technischen Universität Dresden (Prof. Thorsten Strufe) und arbeitet am Center for Tactile Internet (CeTI). Sein Forschungsschwerpunkt ist die Entwicklung von Anonymisierungsverfahren für menschliche Bewegungen.
E-Mail: simon.hanisch@tu-dresden.de

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 Landesbeauftragte für Datenschutz Schleswig-Holstein.
E-Mail: marit.hansen@datenschutzzentrum.de

Antonios Hazim

ist u.a. studentischer Mitarbeiter des nexus Institut im Projekt „KIDD - Künstliche Intelligenz im Dienste der Diversität", Student der Human Factors an der TU Berlin, Open-source Entwickler im „Neo Collective".

Dr. Gunnar Hempel

ist wissenschaftlicher Mitarbeiter der AG Digitale Dienstleistungssysteme und wissenschaftlicher Leiter Arbeitsgruppe ID-Ideal an der Hochschule für Technik und Wirtschaft Dresden.
E-Mail: gunnar.hempel@htw-dresden.de

Dr. Maria Henkel

ist Postdoc in der Abteilung Web Science des ZBW Leibniz-Informationszentrum Wirtschaft in Kiel. Dort arbeitet sie im vom BMBF geförderten Verbundprojekt DESIVE2 - Desinformationsverhalten verstehen.
E-Mail: m.henkel@zwb-online.eu

Mar Hicks, Ph.D.

is an author, historian, and professor at Illinois Institute of Technology in Chicago doing research on the history of computing, labor, technology, and queer science and technology studies.

Timo Hoffmann

ist ehemaliger wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Europäisches und Internationales Informations- und Datenrecht (Prof. Dr. Moritz Hennemann) sowie im interdisziplinären Konsortialprojekt „Vektoren der Datenpreisgabe", das vom Bayerischen Forschungsinstitut für Digitale Transformation (bidt) gefördert wird.
E-Mail: timo.hoffmann@uni-passau.de

Dr. Gerrit Hornung, LL.M.

ist Professor für Öffentliches Recht, IT-Recht und Umweltrecht und Direktor am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel. E-Mail: gerrit.hornung@uni-kassel.de

Dietmar Jakob

ist wissenschaftlicher Mitarbeiter am Technologie Campus Grafenau der Technischen Hochschule Deggendorf und Doktorand. Er fokussiert seine Forschungsarbeit auf die Themen Mensch-Maschine Interaktion, Privatsphäre und empirischer Sozialforschung. E-Mail: dietmar.jakob@th-deg.de

Paul C. Johannes, LL.M.

ist stellvetretender Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) unter der Leitung von Prof. Dr. Alexander

Roßnagel am Wissenschaftlichen Zentrum für Informations-Technikgestaltung (ITeG) an der Universität Kassel. Er ist Rechtsanwalt mit den Tätigkeitsschwerpunkten IT-Recht und Datenschutzrecht.
E-Mail: paul.johannes@uni-kassel.de

Sebastian J. Kasper, LL.M.

ist wissenschaftlicher Mitarbeiter und am Lehrstuhl für Öffentliches Recht, Medien- und Informationsrecht (Prof. Dr. Kai von Lewinski) der Universität Passau sowie im interdisziplinären Konsortialprojekt „Vektoren der Datenpreisgabe", das vom Bayerischen Forschungsinstitut für Digitale Transformation (bidt) gefördert wird.
E-Mail: sebastian.kasper@uni-passau.de

Dr. Wolfgang Kerber

ist Professor für Wirtschaftspolitik am Fachbereich Wirtschaftswissenschaften der Philipps-Universität Marburg.
E-Mail: kerber@wiwi.uni-marburg.de

Steven Kleemann, LL.M.

ist wissenschaftlicher Mitarbeiter im BMBF geförderten Projekt *VIKING* am Forschungsinstitut für öffentliche und private Sicherheit (FÖPS Berlin) der Hochschule für Wirtschaft und Recht Berlin (HWR Berlin) und Doktorand am MenschenRechtsZentrum der Universität Potsdam.

Marcel Kohpeiß, LL.M. (Glasgow)

ist wissenschaftlicher Mitarbeiter und Doktorand am Fachgebiet für Öffentliches Recht, IT-Recht und Umweltrecht (Leiter: Prof. Dr. Gerrit Hornung, LL.M.), sowie am Wissenchaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel.
E-Mail: marcel.kohpeiss@uni-kassel.de

Dr. Jonathan Kropf

ist wissenschaftlicher Mitarbeiter am Fachgebiet Soziologische Theorie der Universität Kassel (Prof. Dr. Jörn Lamla) und Teil des BMBF-Projekts "Faire digitale Dienste: Ko-Valuation in der Gestaltung datenökonomischer Geschäftsmodelle (FAIRDIENSTE)". E-Mail: kropf@uni-kassel.de

Uwe Laufs

ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO) in Stuttgart im Team Identitätsmanagement.

Florian Müller

ist wissenschaftlicher Mitarbeiter am Fachgebiet Soziologische Theorie an der Universität Kassel (Prof. Dr. Jörn Lamla), sowie Doktorand im DFG-Graduiertenkolleg „Privatheit und Vertrauen für mobile Nutzende".

Dr. Maxi Nebel

ist wissenschaftliche Mitarbeiterin in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) unter der Leitung von Prof. Dr. Alexander Roßnagel am Wissenschaftlichen Zentrum für Informations-Technikgestaltung (ITeG) an der Universität Kassel. E-Mail: m.nebel@uni-kassel.de

Dr. Rahild Neuburger

leitet die Forschungsstelle Information, Organisation und Management an der LMU Munich School of Management in München.
E-Mail: neuburger@lmu.de

Tahireh Panahi

ist wissenschaftliche Mitarbeiterin am Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht (Prof. Dr. Gerrit Hornung, LL.M.) an der Universität Kassel. E-Mail: t.setz@uni-kassel.de

Dr. Isabella Peters

ist Professorin für Web Science an der ZBW - Leibniz-Informationszentrum Wirtschaft und am Institut für Informatik der Christian-Albrechts-Universität zu Kiel. E-Mail: ipe@informatik.uni-kiel.de

Lars Pfeiffer, LL.M.

ist wissenschaftlicher Mitarbeiter am Fachgebiet für Öffentliches Recht, IT-Recht und Umweltrecht (Leiter: Prof. Dr. Gerrit Hornung, LL.M.) sowie am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel. E-Mail: lars.pfeiffer@uni-kassel.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

Sascha Schiegg

ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Verteilte Informationssysteme an der Universität Passau und Doktorand. Er beschäftigt sich mit den Forschungsschwerpunkten Privatsphäre, Datenhaltung, Datenbanksysteme im Anwendungsbereich von Energiesystemen.
E-Mail: sascha.schiegg@uni-passau.de

Tom Schmidt

ist studentische Hilfskraft am Lehrstuhl für Öffentliches Recht, Informationsrecht, Umweltrecht und Verwaltungswissenschaft (Prof. Dr. Indra Spiecker genannt Döhmann, LL.M.) an der Goethe-Universität Frankfurt am Main.

Dr. Sabrina Schönrock

ist Juristin, seit 2013 Professorin für Öffentliches Recht, insb. Grund- und Menschenrechte sowie Besonderes Verwaltungsrecht an der HWR Berlin, Fachbereich Polizei und Sicherheitsmanagement/FÖPS Berlin und seit 2014 Richterin des Verfassungsgerichtshofes des Landes Berlin.

Dr. Christian Schunck

ist wissenschaftlicher Mitarbeiter im Team Identitätsmanagement am Fraunhofer Institut für Arbeitswirtschaft und Organisation IAO.
E-Mail: christian.schunck@iao.fraunhofer.de

Rachelle Sellung

ist wissenschaftliche Mitarbeiterin im Identity Management Competence Team am Fraunhofer IAO in Stuttgart, Deutschland. Sie erforscht sozioökonomische Aspekte und User-Experience zu einer Vielzahl von neuen Technologien im Bereich Identitätsmanagement und IT-Sicherheit.
E-Mail: rachelle.sellung@iao.fraunhofer.de

Dr. Louisa Specht-Riemenschneider

ist Professorin für Bürgerliches Recht, Recht der Datenwirtschaft, des Datenschutzes, der Digitalisierung und der Künstlichen Intelligenz an der Universtität Bonn. E-Mail: louisa.specht@forschungsstelle-datenrecht.de

Dr. Martin Steinebach

ist Leiter der Abteilung „Multimedia Sicherheit und IT-Forensik" am Fraunhofer SIT und Honorarprofessor zu den gleichen Themen an der TU Darmstadt. Er promovierte zu digitalen Audiowasserzeichen und forscht heute in verschiedenen Themen der Mediensicherheit, der Sicherheit von maschinellem Lernen, der IT-Forensik und OSINT.

Juliane Stiller

ist Vorstandsvorsitzende von Grenzenlos Digital e. V. und Teilprojektleiterin im Projekt DESIVE² - Desinformationsverhalten verstehen. Ihre Forschungsschwerpunkte liegen im Bereich Digitale Kompetenzen, Desinformationsverhalten und Information Retrieval.
E-Mail: juliane@grenzenlos-digital.org

Dr. Thorsten Strufe

ist Professor für praktische IT-Sicherheit am KIT, Honorarprofessor für Privacy und Netzsicherheit an der TU Dresden, stellvertretender Sprecher des Exzellenzclusters CeTI (Centre for Tactile Internet, with Human-in-the-Loop), sowie PI der KASTEL Security Research Labs.
E-Mail: thorsten.strufe@kit.edu

Milan Tahraoui

ist Völkerrechtler und wissenschaftlicher Mitarbeiter im Forschungsinstitut für öffentliche und private Sicherheit (FÖPS Berlin) der Hochschule für Wirtschaft und Recht Berlin.

Julian Todt

ist wissenschaftlicher Mitarbeiter und Doktorand im Bereich Praktische IT-Sicherheit der KASTEL Security Research Labs am Karlsuher Institut für Technologie. Er forscht an Anonymisierungsmethoden für biometrische Daten in Videos. E-Mail: julian.todt@kit.edu

Dr. Violeta Trkulja

ist stellvertretende Vorstandsvorsitzende von Grenzenlos Digital e.V. und wissenschaftliche Mitarbeiterin im vom BMBF geförderten Projekt "DESI-VE² - Desinformationsverhalten verstehen". Sie forscht zu den Themenbereichen Digitale Komptenzen, Desinformationsverhalten und Wissensorganisation. E-Mail: violeta@grenzenlos-digital.org

Dr. Markus Uhlmann

ist wissenschaftlicher Mitarbeiter am Fachgebiet Soziologische Theorie der Universität Kassel (Prof. Dr. Jörn Lamla) und Teil des BMBF-Projekts "Faire digitale Dienste: Ko-Valuation in der Gestaltung datenökonomischer Geschäftsmodelle (FAIRDIENSTE)". E-Mail: markus.uhlmann@uni-kassel.de

Inna Vogel

ist wissenschaftliche Mitarbeiterin in der von Prof. Dr.-Ing. Martin Steinebach geleiteten Abteilung „Multimedia Sicherheit und IT-Forensik“ am Fraunhofer SIT. Sie promoviert zu der Frage wie Fake News mithilfe von maschinellen Lernverfahren automatisiert erkannt werden können. E-Mail: inna.vogel@sit.fraunhofer.de

Dr. Melanie Volkamer

ist Professorin am KIT in der Fakultät für Wirtschaftswissenschaften und Management. Sie leitet die Forschungsgruppe SECUSO und ist PI der KASTEL Security Research Labs. E-Mail: melanie.volkamer@kit.edu

Sebastian Wilhelm

ist wissenschaftlicher Mitarbeiter am Technologie Campus Grafenau und promoviert in Kooperation mit der Universität Passau. Er beschäftigt sich mit Fragestellungen zu Datenschutz, Anonymisierung und Aktivitätserkennung im Smart Home Bereich. E-Mail: sebastian.wilhelm@th-deg.de

Matthias Winterstetter

ist wissenschaftlicher Mitarbeiter an der Universität Stuttgart im Team Identitätsmanagement. Er beschäftigt sich mit Themen im Bereich der Cybersicherheit und IT/OT Security.