Friedewald | Roßnagel | Geminn | Karaboga | Schindler [Hrsg.]

Data Sharing – Datenkapitalismus by Default?

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 4

Michael Friedewald | Alexander Roßnagel
Christian Ludwig Geminn | Murat Karaboga
Stephan Schindler [Hrsg.]

Data Sharing – Datenkapitalismus by Default?

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 2024

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): 978-3-7560-1266-4
ISBN (ePDF): 978-3-7489-4017-3

DOI: https://doi.org/10.5771/9783748940173

Onlineversion
Nomos eLibrary

Vorwort

Das Teilen von Daten (Data Sharing) ist einerseits mit wirtschaftlichen Partikulainteressen verbunden, andererseits soll es Werte für das Gemeinwohl hervorbringen. Zwar gibt es bereits dezentrale Ansätze, die es den Nutzer:innen ermöglichen sollen, ihre Daten selbstbestimmt zu teilen. Derzeit werden jedoch die geteilten Daten zumeist von zentralisierten Plattformen beherrscht. „Sharing" bedeutet in diesem Kontext, dass die großen Branchenakteure exklusiv mit den Daten der Nutzenden arbeiten und diese ausschließlich für ihre Zwecke nutzen können. Um sich diesen Herausforderungen im Rahmen eines über die Wissenschaft hinausweisenden Diskurses zu stellen, veranstaltete die vom Bundesministerium für Bildung und Forschung (BMBF) geförderte „Plattform Privatheit" am 5. und 6. Oktober 2023 in Berlin die Konferenz „Data Sharing - Datenkapitalismus by Default?". 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 eine Plattform 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 Akteur:innen 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

und ausgehend von technischen, juristischen, ökonomischen sowie geistes- und gesellschaftswissenschaftlichen Ansätzen, an einem interdisziplinär fundierten, zeitgemäßen Verständnis von Privatheit und Selbstbestimmung. Hieran anknüpfend hat es Konzepte zur (Neu-) Bestimmung und Gewährleistung informationeller Selbstbestimmung und des Privaten in der digitalen Welt erstellt und öffentlich kommuniziert. Die Plattform Privatheit führt diese Arbeiten auf breiterer Basis mit mehr Projekten fort. In dieser Tradition hat sie auch die Konferenz „Data Sharing - Datenkapitalismus by Default?" 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 waren.

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 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, Frederik Metzger, Sabine Muhr, Gina Ries, Stephanie Peter und Johannes Janik (Fraunhofer ISI) sowie Christian Geminn und Carsten Ochs (Universität Kassel), Marit Hansen und Felix Bieker (ULD), Andreas Baur (Universität Tübingen) sowie Ina Schiering (Ostfalia Hochschule). Darüber hinaus danken wir Barbara Ferrarese (Fraunhofer ISI) für die professionelle Wissenschaftskommunikation, Miriam Janke (Fusionistas) und Barbara Ferrarese für die lebendige Doppel-Moderation sowie Magdalena Vollmer für das Graphic Recording.

Dieser aus der Konferenz hervorgegangene 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. Auch danken wir Jan-Ole Malchow und Florian Patzer, die für den Projektträger VDI/VDE-IT die Forschungsarbeiten der Plattform Privatheit, die Vorbereitung der Konferenz und das Erscheinen des Bandes konstruktiv begleitet haben.

Die Herausgeber und das Team der „Plattform Privatheit“

Karlsruhe und Kassel, im Juni 2024

Inhaltsverzeichnis

3 Regulierung des Datenteilens

4 Der datensouveräne Bürger

Einleitung: Data Sharing – Datenkapitalismus by Default?

Michael Friedewald, Alexander Roßnagel, Christian Geminn, Murat Karaboga und Stephan Schindler

1. Zum Thema dieses Bandes

Das Teilen von Daten ist mittlerweile ein notwendiger und für viele selbstverständlicher Bestandteil gesellschaftlichen Zusammenlebens. Datenteilen bildet die Grundlage gemeinsamer Kommunikation und Aktion. Das Teilen von Daten erhält in einer Gesellschaft, in der die Verarbeitung von Daten in allen Bereichen der Wirtschaft, der Verwaltung, der Bildung, der Forschung, der Gesundheitsversorgung, der Kultur und der Freizeitgestaltung zur Grundlage gesellschaftlichen Handelns geworden ist, eine neue Dimension. Daten sind die Voraussetzungen von Innovationen, von technischen Erfindungen und Entwicklungen, für neue Strategien und Planungen, für neue Geschäftsmodelle, für neue Strukturen und Prozesse, für mehr Effizienz und bessere Effektivität. Insbesondere lernfähige Systeme der Künstlichen Intelligenz sind auf viele Daten angewiesen, um sie zu trainieren, zu verbessern und zu evaluieren. Das Teilen von Daten ist mit wirtschaftlichen Interessen verbunden und soll gleichzeitig Werte für das Gemeinwohl hervorbringen. In einer solchen Gesellschaft wird das Teilen von Daten zu einer Forderung an jedes Mitglied.

Datenteilen

Wer soll welche Daten teilen und wofür? Die Forderung nach Datenteilen ist oft sehr allgemein und soll eine gesellschaftliche Stimmung erzeugen, die sich gegen das Zurückhalten oder das Horten von Daten richtet. Im Interesse des Allgemeinwohls sollen alle die Daten, die sie haben, der Allgemeinheit zur Verfügung stellen, so dass alle die Daten für ihre Zwecke nutzen können. Soweit die Forderung konkreter wird, müsste sie sich gegen diejenigen richten, die die meisten und interessantesten Daten haben. Dies gilt in ersten Linie gegenüber staatlichen Instanzen, die sehr viele für die Mitglieder der Gesellschaft interessante Daten erzeugen, die für politische,

wirtschaftliche und individuelle Interessen von großer Bedeutung sein können. Mindestens ebenso interessant und umfangreich sind die Datensammlungen der großen Digitalkonzerne, die sie bisher zur Steigerung ihrer Marktmacht exklusiv verarbeiten. Über ihre Plattformen werten sie das Verhalten aller Personen aus, die ihre digitalen Infrastrukturen nutzen. Ihre Datensammlungen erlauben tiefe Einblicke in gesellschaftliche Zustände, Strukturen und Entwicklungen. Viele Daten entstehen auch bei denen, die digitale Dienste oder vernetzte Geräte anbieten. Schließlich erzeugen auch alle Individuen Daten, wenn sie in ihrem Alltag digitale Dienste und Geräte nutzen, die sie bisher bei sich behalten.

Zur Förderung des Datenteilens stellt sich die Frage, was diejenigen, die Daten innehaben, bewegen kann, ihre Daten mit anderen oder allen zu teilen. Hierfür sind rechtliche Verpflichtungen denkbar, wie die zu Open Data oder zur Datentransparenz öffentlicher Stellen. Für Unternehmen stellt sich die Frage nach ihrer Sozialpflichtigkeit, die umso drängender ist, je mehr Personen zum Entstehen ihrer Datensammlungen beigetragen haben, je relevanter die Datensammlungen für das Gemeinwohl sind und je mehr wirtschaftliche, soziale und politische Macht sie aus diesen Datensammlungen ziehen. Auch für die Individuen kann es im Einzelfall bei besonderem öffentlichen Interesse Pflichten zur Bereitstellung von Daten geben. Überwiegend wird es jedoch notwendig sein, ein Klima von moralischer Verpflichtung und von Vertrauen in die faire und allgemeinförderliche Verwendung der Daten zu erzeugen.

Datennutzung

Wer soll die Daten nutzen? Wofür sollen sie verwendet werden? Pflichten zum Datenteilen lassen sich nur damit begründen, dass die Daten direkt oder indirekt für das Gemeinwohl verwendet werden. Sie können von staatlichen Instanzen, politischen Parteien, Interessenvertretungen und gesellschaftlichen Initiativen genutzt werden, um Vorhaben zur Verbesserung des Allgemeinwohls informierter, effektiver oder effizienter verfolgen zu können. Sie können für die Forschung genutzt werden, um bessere Erkenntnisse zu gewinnen, und vom Gesundheitssektor, um die allgemeine und die individuelle Gesundheitsversorgung zu verbessern. Wirtschaftliche Akteure können sie nutzen, um Produkte und Dienste zu verbessern sowie Wohlstand und Beschäftigung zu sichern. Individuen können den Zugang

zu Daten nutzen, um Entscheidungen nachzuvollziehen, auf diese Einfluss zu nehmen und ihre Interessen besser zu vertreten.

Folgen des Datenteilens

Welche Folgen entstehen jedoch durch umfassendes Datenteilen? Mit welchen Risiken ist zu rechnen? Noch ist weitgehend unklar, was die angestrebte Nutzbarmachung von Daten tatsächlich für Folgen haben wird, welche Möglichkeiten sie bietet und welche Hindernisse beteiligte Akteure und Sektoren überwinden müssen, um Potenziale zu heben. Daten ermöglichen Wissen – und Wissen ist Macht. Durch das Datenteilen kann sich Macht sowohl im politischen Raum als auch in der Wirtschaft und im sozialen Zusammenleben verschieben. Ob dies zugunsten der ohnehin Mächtigen erfolgt oder ob dies zugunsten der Kontrolle und Beschränkung von Macht genutzt werden kann, hängt von der Gestaltung des Datenteilens ab. Durch das Datenteilen kann auch die Datensouveränität der Einzelnen beeinträchtig werden, wenn sie nicht mehr freiwillig über die Preisgabe ihrer Daten entscheiden können. Ihre informationelle Selbstbestimmung ist auch dann gefährdet, wenn die Verwendung ihrer Daten für sie nicht transparent ist und für die Beeinflussung ihres Handelns benutzt werden kann.

Datenteilen wird nur zum Vorteil aller sein, wenn es so gestaltet wird, dass die erhofften Vorteile erreicht und die befürchteten Folgen vermieden werden – wenn es also fair erfolgt. Dieser Interessenausgleich kann durch rechtliche Regelungen, durch die Gestaltung der Architektur der Infrastruktur des Datenteilens, durch ausreichende Schutzmechanismen für bedrohte Interessen, durch Instrumente zur Selbstbestimmung und durch gesellschaftliche Organisation erreicht werden. Diese Bestimmungsfaktoren für faires Datenteilen sind auch die Voraussetzungen für Vertrauen, ohne das eine große Verbreitung von Datenteilen nicht erwartet werden kann. Sie werden in diesem Buch intensiv untersucht

Rechtlicher Rahmen

Datenteilen erhält seinen rechtlichen Rahmen vor allem durch neue Regelungen des Unionsrechts. Aber auch auf deutscher Ebene soll das Teilen

von Daten gefördert werden – etwa durch ein Forschungsdatengesetz und ein Gesundheitsdatennutzungsgesetz.

Der Data Governance Act (Verordnung (EU) 2022/868) (DGA) vom 30. Mai 2022 soll die Entwicklung eines grenzfreien digitalen Binnenmarktes sowie eine auf den Menschen ausgerichtete, vertrauenswürdige und sichere Datengesellschaft und -wirtschaft vorantreiben. Hierfür sollen öffentliche Stellen, private Unternehmen und betroffene Personen Daten, über die sie verfügen, anderen zur Verwendung preisgeben, weil in diesem Datenraum die Grundrechte betroffener Personen gewahrt werden.

Der DGA enthält für öffentliche Stellen keine Pflicht zum Datenteilen, er soll es ihnen aber erleichtern, weil er die Anforderungen und Möglichkeiten enthält, die Daten vor der Weiterverwendung durch Dritte ausreichend zu schützen. Sie können von interessierten Dritten verlangen, dass sie eine Vertraulichkeitsvereinbarung unterzeichnen, dass sie die Daten vor der Weiterverarbeitung anonymisieren oder pseudonymisieren und vor unbefugten Zugriffen schützen.

Zur Bildung eines Datenmarktes erleichtert der DGA die Arbeit von „Datenmittlern", die den Kontakt zwischen an Datennutzung Interessierten und denjenigen, die zu Datenteilen bereit sind, herstellen und für faire Bedingungen und Preise sorgen. Datenvermittlungsdienste können auch von „Datengenossenschaften" erbracht werden, die diejenigen, die Daten teilen wollen, bei der Wahrnehmung ihrer Rechte unterstützen.

Der DGA soll schließlich auch die freiwillige Spende personenbezogener Daten durch betroffene Personen zum Wohl der Allgemeinheit (Datenaltruismus) erleichtern, indem er „in der Union anerkannten datenaltruistischen Organisationen" ermöglicht, als Treuhänder der Daten ohne Erwerbszweck zwischen Datenspendenden und -nutzenden zu vermitteln. Im Gegensatz zu den Datenmittlern sollen sie keinen Markt für personenbezogene Daten etablieren, sondern die Daten unmittelbar für Zwecke von allgemeinem Interesse sammeln, selbst verarbeiten oder zur Verfügung stellen.

Der Data Act (Verordnung (EU) 2023/2854) (DA) vom 13. Dezember 2023 soll den Zugang zu Daten erleichtern, die von vernetzten Objekten erzeugt werden. Er räumt Einzelpersonen, die solche Objekte nutzen, Unternehmen und Behörden ein Recht ein, solche Daten zu erhalten und an verschiedene Diensteanbieter weiterzugeben. Beispielsweise kann derjenige, der ein Auto oder eine Maschine besitzt, entscheiden, mit dem Auto oder der Maschine erzeugte Daten an sein Versicherungsunternehmen oder

einen Reparaturbetrieb weiterzugeben. Mit Hilfe der Daten können die empfangenden Institutionen neue Dienste für solche Objekte entwickeln.

Die noch im Gesetzgebungsverfahren befindliche Verordnung für einen europäischen Gesundheitsdatenraum soll einen spezifischen Rechtsrahmen bieten, um Gesundheitsdaten zur Verfügung zu stellen und deren Nutzung durch berechtigte Organisationen zu ermöglichen. Die Frage, welche rechtlich organisatorische Gestaltung für welchen Zweck des Datenteilens geeignet ist, wird von Beiträgen in diesem Band aufgegriffen.

Soweit personenbezogene Daten geteilt werden sollen, ist auch die Datenschutz-Grundverordnung (DS-GVO) zu beachten. Verwaltungsbehörden oder Unternehmen haben in der Regel keine Rechtsgrundlage, um personenbezogene Daten für alle Interessierten frei zugänglich zu veröffentlichen. Sie müssen die Daten, bevor sie sie mit anderen teilen, anonymisieren. Das heißt, sie müssen sie so verändern, dass mit ihrer Hilfe dauerhaft kein Personenbezug mehr hergestellt werden kann. Ist die Anonymisierung nicht möglich, ohne dass der Zweck des Datenteilens – wie z.B. Forschung oder Auswertung für Gesundheitszwecke – verfehlt wird, ist eine Einwilligung der betroffenen Person notwendig. Ob hierfür eine gesetzliche Opt-in-Regelung oder eine Opt-out-Lösung ausreichend ist, wird für jeden einzelnen Anwendungsbereich umstritten sein. Wie die Selbstbestimmung beim Datenteilen unterstützt werden kann, ist ebenfalls Thema mehrerer Beiträge.

Fairness

Hinsichtlich der beteiligten Akteure und ihrer Zusammenarbeit stellt sich immer wieder die Frage, wem das Teilen von Daten nützt. Für die Einzelnen muss deutlich werden, worin ihr individueller Nutzen des Teilens von Daten besteht. Als fair wird das Datenteilen nur angesehen werden können, wenn gesellschaftliche Ziele im Mittelpunkt stehen und nicht Partikularinteressen als Gemeinwohlinteresse beworben werden. Zur Bewertung der Fairness wird auch gehören, inwieweit diejenigen, die Daten teilen sollen, auf struktureller Ebene in die Entscheidungen über den Zugang zu den Daten, die Zwecke der Datennutzung und die Verteilung des Mehrwerts der Datenverwendung einbezogen werden. Zur Fairness gehört schließlich auch, dass die Grundrechte aller Beteiligten berücksichtigt werden. Hierzu gehört zum einen, dass die informationelle Selbstbestimmung der betroffenen Personen und die Datensouveränität derjenigen, die Daten teilen

sollen, gewahrt werden. Zum anderen muss aber auch ein fairer Ausgleich mit den Interessen beispielsweise der Forschenden und ihrer Forschungsfreiheit gefunden werden. Diese Fragen verfolgen mehrere Beiträge.

Gestaltung des Datenteilens

Entscheidend für die Voraussetzungen und Folgen des Datenteilens werden auch die Infrastrukturen und die Prozesse sein, die für das Datenteilen genutzt werden. Wie müssten sichere Datenräume konzipiert werden, in denen die Daten sicher aufbewahrt werden, aber zugleich von berechtigten Stellen ausgewertet werden können? Risiken lassen sich besser eingrenzen und vermeiden, wenn die Architektur dezentral und zweckbezogen ist, weil die Prozesse leichter auf die Interessen aller Beteiligten ausgerichtet und Schutzmechanismen zielgerichteter eingerichtet werden können. Anforderungen lassen sich leichter entwickeln und anwenden, wenn die Datenräume sektoral entwickelt werden, wie für spezifische Forschungszwecke in den einzelnen Sektoren der Nationalen Forschungsdaten-Infrastruktur (NFDI) oder für Gesundheitsdaten in den Datenintegrationszentren der Medizininformatik-Initiative. Hier können Schutzmaßnahmen in geeigneter Weise dem spezifischen Schutzbedarf angepasst werden.

Technisch-organisatorische Maßnahmen zum Interessenausgleich zwischen denen, die Daten besitzen, und denen, die Daten nutzen, können auch „Datenmittler" und „Datentreuhänder" bieten. Auf einem Datenmarkt kann ein ehrlicher „Datenmittler" für faire Bedingungen des Datenteilens und für faire Teilhabe am Mehrwert sorgen. Anerkannte „Datentreuhänder" ohne ökonomische Interessen können die Grundlage für altruistische Datenspenden bieten, indem sie die Interessen der Datengeber hinsichtlich des Zwecks, der Empfänger und der Bedingungen der Datenspenden durchsetzen.

2. Die Beiträge

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

Ulrich Kelber (ehemaliger *Bundesbeauftragter für den Datenschutz und die Informationsfreiheit*) thematisiert in seinem einführenden Kapitel „The

winner takes it all? Selbstbestimmung und Fairness beim Teilen von Daten" die komplexen Herausforderungen und Chancen des Datenteilens in der digitalen Welt. Er betont, dass das Teilen von Daten wirtschaftliche, gesellschaftliche und wissenschaftliche Vorteile bietet, jedoch auch erhebliche Risiken für die informationelle Selbstbestimmung birgt. Kelber argumentiert, dass eine übermäßige Machtkonzentration bei großen Tech-Konzernen zu verhindern ist, um das in einem demokratisch-rechtsstaatlichen Gemeinwesen notwendige Maß an Fairness informationeller Selbstbestimmung zu wahren. Er fordert klare Regeln und deren Durchsetzung, um Missbrauch zu verhindern und individuelle Rechte und Freiheiten zu schützen. Er plädiert dafür, dass sich das Maß des Daten-Teilens in Europa am Grad der Allgemeinwohlorientierung und nicht allein an wirtschaftlichen Erwägungen orientieren muss.

Datenintermediäre: Neue Ansätze für das Data Sharing

In einer Zeit, in der die Datenökonomie rapide an Einfluss gewinnt, stehen Datenintermediäre oder -mittler im Zentrum vieler Diskussionen über die Verwaltung und Nutzung von Daten. Diese Intermediäre, die als Vermittler zwischen Datenanbietern und -nutzenden fungieren, spielen eine entscheidende Rolle für die Sicherstellung von Transparenz, Datenschutz und effizienter Datennutzung. Die Beiträge in diesem Abschnitt beleuchten aus verschiedenen Blickwinkeln, wie Datenintermediäre zur Förderung von Innovation und zum Schutz individueller Rechte beitragen können. Gemeinsame Themen der Beiträge sind die Governance von Daten, die Rolle der digitalen Identität im Datenkapitalismus und die Notwendigkeit, eine ausgewogene Datenpolitik zu gestalten, die sowohl ökonomische als auch ethische Aspekte berücksichtigt.

Abel Reiberg, Crispin Niebel und *Anna-Raphaela Schmitz* (Acatech – Deutsche Akademie der Technikwissenschaften) widmen sich in ihrem Kapitel der „Governance von Datenräumen". Der Aufbau von Datenräumen wird aktuell intensiv gefördert, weil damit die Hoffnung auf eine Stärkung der Datenökonomie verbunden ist. Sie betonen die Vorteile von föderierten Strukturen, in denen sich Datensouveränität, Wettbewerb und Innovation in offenen Datenräumen potenziell leichter realisieren lassen als in zentralisierten Infrastrukturen. Dies erfordert allerdings einen nicht unerheblichen Koordinierungsaufwand, um die teilweise konfligierenden Ziele in Einklang zu bringen. Die Autor:innen diskutieren, wie in verschiedenen

Governance-Arrangements praktisch versucht wird, durch ein effizientes und faires Zusammenwirken Datensouveränität, Wettbewerb und Innovation zu fördern, während gleichzeitig die Rechte auf Privatheit, Transparenz und Selbstbestimmung gewahrt bleiben.

Paul C. Johannes und *Maxi Nebel* (Universität Kassel) erörtern in ihrem Beitrag „Wenn die Datengenossenschaft für mich einwilligt" die mögliche praktische Rolle dieses im Data Governance Act (DGA) vorgesehenen speziellen Datenvermittlungsdiensts. Sie beleuchten, wie genossenschaftlich organisierte Datenintermediäre die Verwaltung und Nutzung von Daten durch kollektive Einwilligungsmechanismen verbessern können und diskutieren die rechtlichen Rahmenbedingungen sowie Vor- und Nachteile dieser neuen Form der Datenvermittlung.

Oliver Vettermann (FIZ Karlsruhe) untersucht in seinem Beitrag „Die Infrastruktur, mein digitaler Zwilling und ich: Das Individuum und die digitale Identität im Mittelpunkt des Datenkapitalismus", wie der schwer fassbare Begriff der Datensouveränität in Projekten zum Aufbau von (Forschungs-) Dateninfrastrukturen verwendet wird und welche Rolle er beim Schutz der in digitalen Identitäten dargestellten Personen spielt. Er kritisiert, dass bei der Gestaltung der aktuellen europäischen Datengesetzgebung die ökonomischen Ziele über die Datenschutzinteressen der Individuen gestellt werden. Er führt weiter aus, dass der Fokus auf die Gewinnung und Verwertung von Daten oft die ethischen Aspekte vernachlässigt und das Gemeinwohl hinter den Interessen der Datenkapitalisten zurückbleibt.

Im letzten Beitrag dieses Abschnitts formulieren *Stephanie Fuchsloch, Wolf Zinke* und *York Sure-Vetter* (NFDI e.V.) „Drei Wünsche an die Datenpolitik – aus Sicht einer Dateninfrastruktur". Die Vision der Nationalen Forschungsdateninfrastruktur e.V. (NFDI) ist es, „Daten als gemeinsames Gut für exzellente Forschung … durch die Wissenschaft in Deutschland" selbst zu organisieren. Für die Umsetzung dieser Vision fordern sie erstens eine nachhaltige Finanzierung, nicht nur für den Aufbau einer standardisierten technischen Infrastruktur, sondern auch für die Entwicklung von Prozessen und Methoden zu deren Nutzung. Zweitens argumentieren sie, dass erst die Schaffung standardisierter Prozesse für den sicheren Datenaustausch und die Datenbereitstellung die Sicherheit schafft, die für eine dauerhafte Nutzung und die Hebung der Innovationspotenziale notwendig ist. Drittens braucht es nach Ansicht der Autor:innen eine gerechte Datenpolitik, die Privatsphäre und Zugänglichkeit in einem FAIRen Datenökosystem gewährleistet, damit die Nutzung der Forschungsdateninfrastruktur umfänglich dem Gemeinwohl dienen kann.

Regulierung des Datenteilens

In diesem Abschnitt geht es in drei Beiträgen um Ansätze zur Regulierung von Datenteilen und Datenhandel in Europa. Diskutiert wird dabei, wie Daten verantwortungsvoll und zum Wohl der Gesellschaft genutzt werden können.

In ihrem Beitrag „Europäische KI-Regulierung: Auf der Suche nach verbindlichen Ansätzen für Nachhaltigkeit und Inklusion" setzen sich *Marco Wedel* (TU Berlin), *Antonios Hazim* (Nexus) und *Alexandra Wudel* (FemAI GmbH) mit den aktuellen Entwicklungen und Herausforderungen in der Regulierung künstlicher Intelligenz (KI) in Europa, dem Artificial Intelligence Act (AI-Act) auseinander. Die Autor:innen argumentieren, dass es die ursprüngliche Absicht der Gesetzgeber war, auch ethische, soziale und ökologische Dimensionen zu berücksichtigen. Sie erläutern, wie die von der Hochrangigen Expertengruppe formulierten ethischen Prinzipien und Kernforderungen zwar in den frühen Entwürfen der EU-Institutionen berücksichtigt, jedoch in der endgültigen Fassung des AI-Acts nicht als verbindlich übernommen wurden. Zentral war dabei die „AI Literacy", also die Förderung von Grundkenntnissen über KI in der gesamten Gesellschaft, um eine informierte und demokratische Kontrolle von KI-Systemen zu ermöglichen. Trotz Vorschlägen, die AI Literacy als verpflichtendes Element in die Gesetzgebung einzubinden, bleibt sie in der endgültigen Gesetzgebung unverbindlich. Die Autor:innen schlussfolgern, dass, obwohl der AI-Act als weltweit erster umfassender Regulierungsansatz für KI beeindruckt, er in Bezug auf die konkrete Durchsetzung von Nachhaltigkeit und Inklusion in der KI-Entwicklung zu wünschen übriglässt.

Der Beitrag „Öffentliche Verwaltung als Katalysator für selbstbestimmtes Datenteilen" von *Gunnar Hempel* (HTW Dresden) und *Michael Kubach* (Fraunhofer IAO) beleuchtet auf Grundlage der Ergebnisse zweier Projekte zur Pilotierung einer digitalen Identitätslösung mit einer „kommunalen Datenkarte" die mögliche Rolle der öffentlichen Verwaltung bei der Förderung des selbstbestimmten Datenteilens. Ziel der Projekte war es, ein hohes Sicherheits- und Datenschutzniveau mit einer benutzerfreundlichen Handhabung zu kombinieren. Die Autoren argumentieren, dass die Vernetzung kommunaler Dienstleistungen eine Schlüsselrolle bei der Förderung der digitalen Souveränität der Bürger spielen kann. Neben klassischen Verwaltungsdienstleistungen zählen dazu auch Angebote wie der öffentliche Personennahverkehr, Stadtbibliotheken, Museen und Sporteinrichtungen. Mit der kommunalen Datenkarte können Bürger nun selbst die Kontrolle

über ihre persönlichen Nachweise behalten und diese vertrauensvoll für die Inanspruchnahme kommunaler Dienstleistungen nutzen. Die Autoren betonen, dass eine solche Lösung nicht nur die Effizienz und Benutzerfreundlichkeit kommunaler Dienstleistungen erhöhen, sondern auch das Vertrauen in öffentliche Institutionen stärken kann.

In ihrem Beitrag „Die neue Ära des Datenhandels: Daten als Währung und Gegenleistung" analysieren *Dagmar Gesmann-Nuissl* und *Stefanie Meyer* (TU Chemnitz) die rechtlichen Grundlagen und Herausforderungen des Handels mit personenbezogenen Daten. Die Autorinnen diskutieren die rechtlichen Rahmenbedingungen, insbesondere der europäische Digitale Inhalte-Richtlinie und der Warenkaufrichtlinie sowie deren Umsetzung in deutsches Recht (§§ 327 ff. BGB), die sich auf der Schnittstelle zwischen der Privatautonomie des Vertragsrechts und dem Grundrechtsschutz des Datenschutzrechts bewegt. Als Lösung schlagen die Autorinnen ein „Datenwirtschaftsportal" vor, das den Wert von Daten transparent macht und es Verbrauchern ermöglicht, informierte Entscheidungen zu treffen. Ein solches Portal könnte die Akzeptanz der Datenwirtschaft erhöhen und eine Brücke zwischen Verbraucherschutz und wirtschaftlichen Interessen schlagen.

Datensouveräne Bürger:innen

Im dritten thematischen Abschnitt geht es um die Frage, wie man Bürgerinnen und Bürger mit technischen oder organisatorischen Maßnahmen in die Lage versetzen kann, souverän mit ihren personenbezogenen Daten umzugehen, bzw. mit welchen Verhaltensweisen diese selbst versuchen, die Kontrolle über geteilte Daten zu behalten.

In seinem Beitrag „Dann drück ich aufs Mikro, wenn's hier mal um Dinge geht..." untersucht *Lukas Schmitz* (TU Dresden) den Umgang von Menschen mit Privatheitsfragen bei der Nutzung von Smart Speakern im häuslichen Umfeld. Der Autor argumentiert, dass Menschen trotz des Bewusstseins über potenzielle Datenschutzrisiken oft keine umfassenden Schutzmaßnahmen ergreifen. Er zeigt, dass Menschen das Risiko aber unter Rückgriff auf Formen des Vertrauens sowie Strategien der Analogisierung bearbeiten. Vertrauen manifestiert sich in der Hoffnung auf staatliche Regulierung oder das ethische Verhalten von Unternehmen. Analogisierung bezieht sich auf das Schaffen von kontrollierbaren analogen Räumen. Diese Strategien sind Ausdruck eines individuellen „Attachments", also der

Verhaftung in persönlichen Erfahrungen und Routinen. Der Autor zeigt, dass das vermeintliche „Privacy Paradox" eher eine Folge der ungreifbaren Risiken der digitalen Transformation ist, die es schwer macht, angemessen auf Datenschutzbedrohungen zu reagieren, und plädiert für systemische Lösungen und Aufklärungsarbeit, um den Herausforderungen zu begegnen.

Der Beitrag „Datenautonomie im Smart Home: eine praktische/prototypische Umsetzung" von *Christopher Ruff, Andrea Horch* (Fraunhofer IAO) und *Alexander Orlowski* (Universität Tübingen) thematisiert die Herausforderungen für die Datenautonomie im Smart Home und präsentiert einen „Transparenten Datenautonomie-Meta-Assistenten" (DAMA) als Lösung, um Transparenz über die im Smart Home verarbeiteten Daten zu schaffen und dadurch die informationelle Selbstbestimmung der Nutzenden zu stärken. Der Meta-Assistent reguliert smarte Geräte kontextbasiert, informiert über aktive Sensoren und ermöglicht die automatische Anpassung der Geräte an die Datenschutzpräferenzen der Nutzenden. Die durchgeführten Nutzerstudien zeigten, dass DAMA den Schutz der Privatheit der Nutzenden verbessert und es ihnen ermöglicht, informierte Entscheidungen zu treffen.

Stefanie Brückner, F. Gerrik Verhees, Peter Schwarz, Andrea Pfennig und *Stephen Gilbert* (TU Dresden) untersuchen im Beitrag „Standard Health Consent – Ein partizipativer Einwilligungsmanagement-Ansatz für die Nutzung von Gesundheitsdaten aus Apps und Wearables" die Nutzung von Daten aus digitalen Gesundheits-Apps und Wearables für die Verbesserung der Gesundheitsversorgung und im Rahmen der medizinischen Forschung. Sie beleuchten die Herausforderungen und Chancen, die durch die Erhebung und Nutzung dieser Daten entstehen. Sie kritisieren, dass der bisherige Entwurf für einen Europäischen Gesundheitsdatenraum (EHDS) Kontrollmechanismen für Bürger vernachlässigt. Sie führen aus, dass eine Umfrage unter Ärzten ergab, dass diese die Nutzung von Gesundheitsdaten aus Apps und Wearables als nützlich erachten und befürworten, dass Patienten die Kontrolle über die Weitergabe dieser Daten haben sollten. Die Autor:innen beschreiben einen neuen, standardisierten Ansatz für die Einholung und Verwaltung von Einwilligungen für das Teilen von Gesundheitsdaten aus Apps und Wearables, den Standard Health Consent, der zur Etablierung eines fairen und vertrauenswürdigen Gesundheitsdatenökosystems beitragen könnte.

Der Beitrag „Zur Evaluation der digitalen Kontaktverfolgung" von *Henrik Graßhoff* und *Stefan Schiffner* (Berufliche Hochschule Hamburg) untersucht die digitale Kontaktverfolgung während der Corona-Pandemie

und betrachtet sie als Datenmarkt. Es werden verschiedene Akteure analysiert, darunter Endanwender, die öffentliche Hand, digitale Gatekeeper und private Anbieter. Die Autoren betonen, dass digitale Kontaktverfolgung, insbesondere durch Kontaktverfolgungs-Apps (KVAs), stark von der Akzeptanz der Nutzenden abhängt. Studien zeigen, dass die Bereitschaft zur Nutzung von KVAs durch gesundheitliche Vorteile zwar gefördert, aber durch Datenschutzbedenken gehemmt wird. Die öffentliche Hand spielt eine zentrale Rolle als Regulator und Entwickler von KVAs, während digitale Gatekeeper wie Google und Apple durch die von ihnen zur Verfügung gestellten Schnittstellen maßgeblichen Einfluss ausüben. Die Autoren kritisieren die Dominanz dieser Konzerne und die Abhängigkeit demokratischer Regierungen von ihnen. Schließlich wird die Notwendigkeit einer ständigen Pflege und Weiterentwicklung digitaler Technologien betont, um für zukünftige Pandemien besser gerüstet zu sein.

Der Beitrag „Betroffenenrechte in der digitalen Selbstvermessung" von *Fabiola Böning* (Universität Kassel) und *Uwe Laufs* (Fraunhofer IAO) behandelt die digitale Selbstvermessung und die damit verbundenen Betroffenenrechte gemäß DS-GVO. Mit der zunehmenden Nutzung von Wearables zur Selbstvermessung und der damit einhergehenden Datenverarbeitung durch Anbieter, entstehen zwar ehebliche individuelle Vorteile, es gibt aber auch erhebliche ethische und rechtliche Fragen, u.a. in Bezug auf die effektive und nutzerfreundliche Wahrnehmung von Betroffenenrechten. Die Autor:innen legen dar, wie ein Privacy-Assistent aussehen kann, der Transparenz und Intervenierbarkeit bei der Datenverarbeitung ermöglicht. Dabei erfolgt die Ausübung der Betroffenenrechte bei dem Anbieter eines Selbstvermessungsgerätes selbst direkt über eine Schnittstelle oder mittels eines Anfragengenerators mit vorgefertigten Templates, die individualisiert und an die Bedürfnisse der Nutzenden angepasst werden können.

Im Beitrag von *Daniel Franzen* und *Claudia Müller-Birn* (FU Berlin) wird schließlich erläutert, wie Laien durch ein geeignetes *Privacy Decision User Interface* bei der Nutzung von Differential Privacy (DP) zu informierten Entscheidungen befähigt werden können. DP bietet einen quantifizierbaren Schutz der Privatsphäre und könnte deshalb das Vertrauen und die Bereitschaft zur Datenweitergabe erhöhen, ist aber wegen der technischen Komplexität für Laien schwer verständlich. Die Autor:innen berichten über die Ergebnisse aus zwei empirischen Studien zur Kommunikation von Datenschutzrisiken und Privatheitsschutz durch DP. Dabei zeigt sich, dass eine Kommunikation von Datenschutzrisiken mithilfe grafischer Elemente (Icons) und insbesondere einer Kombination von Text und Grafik zu einer

signifikant besseren Verständlichkeit führt als rein textuelle Informationen und damit informierte Entscheidungen fördert. Sie folgern, dass dieser Ansatz Potenzial besitzt, das Vertrauen in Datensammlungen zu stärken und somit einen wertvollen Beitrag zur Nutzung von Daten für das Gemeinwohl zu leisten. Um Benachteiligungen zu vermeiden, sollten dabei individuelle Kompetenzen berücksichtigt und adaptive Benutzeroberflächen entwickelt werden.

1 Keynote

The winner takes it all? Selbstbestimmung und Fairness beim Teilen von Daten

Ulrich Kelber

Zusammenfassung

Das Teilen von Daten bietet die Chance auf Fortschritt und Wachstum. Es gehört zur Evolution und Vielfalt digitalen Lebens und Wirtschaftens dazu. In einem demokratisch-rechtsstaatlichen Gemeinwesen müssen allerdings Fairness und der unveräußerliche Grad an Selbstbestimmung und Freiheit gewahrt bleiben. Deshalb besteht kein Raum für Monopolisten und Oligopole. Die Verarbeitungskultur anderer Teile der Welt, die individuelle Rechte und Freiheiten ausblendet, kann nicht der Maßstab oder das Ziel unseres Handelns sein. Stattdessen brauchen wir einen Schutz- und Vertrauensraum mit Regeln, Schutzmechanismen und Kontrolle. Das Maß des Daten-Teilens muss sich am Grad der Allgemeinwohlorientierung orientieren, nicht allein an wirtschaftlichen Erwägungen. Eine allgemeine Sozialpflichtigkeit zum Teilen personenbezogener Daten darf es nicht geben. Wir brauchen einen eigenen europäischen Weg, geprägt von unseren gemeinsamen Werten.

Geteiltes Glück, so sagt der Volksmund, ist doppeltes Glück. Und auch für Daten lässt sich zunächst einmal sagen, dass Wissen, Nutzen und Wertschöpfung sich multiplizieren, wenn Informationen geteilt werden. Doch ganz so einfach wie beim Glück ist die Formel beim Data Sharing nicht. Denn hier geht es nicht um mildtätige Freigiebigkeit, sondern um die Verteilung von materiellen Werten und Wertschöpfungsperspektiven in der Gestalt von Daten.

Außerdem haben wir es weniger mit dem heiligen Sankt Martin von Tours zu tun, der seinen Mantel barmherzig mit einem Bettler teilt, sondern mit teils knallharten, interessengeleiteten Akteuren. Zu ihnen gehören eben nicht nur seriöse Forschende und lautere Gewerbetreibende, sondern auch jede Menge Goldgräber, Glücksritter und Global-Player. Und mittendrin steht der digitale Mensch als Verarbeitungssubjekt und bisweilen hilfloser Grundrechtsträger.

Ohne einen wertebasierten und menschenzentrierten Rechtsrahmen mit Selbstbestimmung und Fairness für alle heißt es schnell: „The winner takes it all!" – und wir wissen, wer dies bei einer falscher Chancen-, Risiken- und Rollenverteilung ist. Deshalb ist es notwendig, Aspekte der Datenökonomie und des Datenkosmos nicht allein marktwirtschaftlich, sondern auch sozial-, grundrechts- und demokratieorientiert zu denken.

1. Daten-Teilen als Chance für Innovation und digitales Wirtschaftswachstum

Es gibt wohl niemanden, der ernsthaft bestreitet, dass das multilaterale Teilen von Daten wirtschaftlich, gesellschaftlich und entwicklungszivilisatorisch erhebliche Vorteile bringen kann. Der breite und wechselseitige Zugang zu Daten bietet zunächst einmal Transparenz und schafft Kontrolle in Prozessen und gegenüber Akteuren – etwas, was wir Datenschützer uns immer wieder wünschen.

Der zweite Vorteil im Teilen von Daten besteht in der Effizienz, gleiche Informationen nicht immer wieder neu erheben zu müssen, sondern auf vorhandener Datenbasis aufzubauen. Dies ist in gewisser Weise ein Beitrag zur Datensparsamkeit, jedenfalls unter dem Gesichtspunkt der Vermeidung doppelter Datenerhebung. Man denke hier nur an die Entlastungswirkung für Bürgerinnen und Bürger bei datenschutzfreundlicher Umsetzung des „Once-Only-Prinzips" bei Verwaltungsleistungen.

Unbestreitbar ist auch, dass eine breite Datenbasis mit Zugriff auf umfassende Informationen verschiedener Quellen oft fundiertere Entscheidungen ermöglicht. Intelligent nach Maßstäben der Kritikalität von Inhalten, Nutzern, Nutzungen und Compliance einschließlich der Grundbedingungen des Datenschutzes konzipiert und differenziert können so bereichsspezifische Daten-Fundamente als stetig wachsender Grundstock vorhandener und künftiger Verarbeitungen entstehen.

Ein legitimes Verarbeitungsinteresse besteht dabei allerdings nur an probaten Daten, nicht aber an einer willkürlichen Verarbeitung „ins Blaue". Denn nur bei wissenschaftlicher Herangehensweise steigen Objektivität, Reliabilität und Validität von Daten und den aus ihnen gewonnenen Informationen – etwas, was den Datenschützer freut.

Aber auch Wissenschaft und Forschung, Wirtschafts- und Geschäftsverkehr sowie unser demokratisches Gemeinwesen verlangen in einer digitalen Welt ein zunehmendes Maß an Redlichkeit in der Datenverarbeitung.

Bei diesem Aspekt sehe ich übrigens die Datenverarbeitenden in einer positiven Bringschuld was den transparenten Nachweis der Seriosität ihres Handelns angeht. Es kann jedenfalls nicht sein, dass allein Verarbeitungssubjekte, Mitbewerber, Interessen-Sachwalter oder gar Aufsicht ex post aufgerufen sind, Verarbeitungen jeweils von außen betrachtet zu hinterfragen. Wer Akzeptanz, Mitwirkung und einen echten Aufbruch in der Kultur des Daten-Teilens will, muss jedenfalls eine befriedigende Antwort auf das legitime Verlangen nach Lauterkeit insbesondere in der Form von Transparenz, Kontrolle und Selbstbestimmung geben.

Ein legitimes Verarbeitungsinteresse verlangt in einem Rechtsstaat eine klare mehrdimensionale grundrechtliche Legitimität über die Person und Perspektive des Verarbeiters hinaus – so ist unsere DSGVO und unsere ganze demokratische Freiheitsordnung konzipiert. Das grundrechtliche Austarieren kollidierender Interessen und Rechtsgüter gilt es beim Teilen von Daten genauso, wenn nicht sogar sensibler als in der analogen Welt, zu verwirklichen. Und ich glaube, dass unsere Gesellschaft hier in Anbetracht der Risiken digitaler Verarbeitungen zu Recht besonders aufmerksam und kritisch ist. Deshalb wäre allein das Gefühl „The winner takes it all!" für die weitere Evolution der Digitalisierung fatal!

2. Keine digitale Evolution ohne das Teilen von Daten

Der zentrale Vorteil des Teilens von Daten besteht weiterhin darin, dass das Zusammenführen von Informationen unterschiedlicher Quellen Auswertungen erlaubt, die Grundlage neuer Erkenntnisse und Innovationen sein können. In einer digitalen Gesellschaft ist dies die zentrale Voraussetzung ihrer weiteren Entwicklung. Das Teilen von Daten nimmt hierbei funktional quasi die Rolle einer Synapse ein und ist so ein maßgeblicher Impulsgeber der Digitalisierung. Digitale Evolution ist ohne das Teilen von Daten schlechthin kaum mehr vorstellbar. Froh bin ich, dass sich in der Debatte um das Data Sharing hierbei immer mehr die Einsicht durchsetzt, dass nebulöse geschlossene Datensilos weniger großer globaler Akteure oder das fragliche Credo vom vermeintlichen Sacheigentum an Daten keine gewinnbringenden Perspektiven einer digitalen Gesellschaft sind. Trotzdem begegnet das Teilen von Daten ungeachtet der Rahmenbedingungen schon ganz allgemein zahlreichen Vorbehalten außerhalb von Datenschutzfragen.

Im Mai 2023 hat der Branchenverband Bitkom e.V. eine Unternehmensbefragung vorgestellt, dass hiesige Unternehmen noch wenig aufgeschlossen sind, Daten zu teilen, auch keine nicht-personenbezogenen; zu groß wären Verlustängste.[1] Dies mag damit zu tun haben, dass das Teilen von Daten eben einen grundlegenden Paradigmenwechsel bedeutet und unternehmerisch gefühlt mit der Preisgabe von Betriebsgeheimnissen gleichgesetzt wird.

International betrachtet ist man andernorts bereits weiter im Denken. Gleichwohl haben wir es mit einer Entwicklung zu tun, der sich niemand auf Dauer wird verschließen können, gerade wenn man als Industrie-, Wissenschafts- und Servicestandort Deutschland nicht ins Hintertreffen geraten möchte. Ich warne aber davor bei der Frage der Akzeptanz einer neuen Kultur des Daten-Teilens allein die Wirtschaft und Wissenschaft mit ihren Interessen in den Blick zu nehmen. Denn dort, wo es um personenbezogene Daten geht, müssen wir unsere Gesellschaft als Ganzes abholen. Wer glaubt, die Menschen müssten sich einfach fügen und einem Digitalzwang unterwerfen, hat weder unser demokratisches Gemeinwesen, noch die wirtschaftlichen Erfolgsparameter digitalen Fortschritts verstanden.

3. Die Ambivalenz des Daten-Teilens

Einleuchtende Positivbeispiele für das sinnvolle und gewinnbringende Teilen von Daten gibt es viele. So etwa in Echtzeit geteilte Mobilitätsdaten zur Verkehrslenkung. Dies verhilft allen Verkehrsteilnehmern zu möglichst freier, planbarer Fahrt und spart so uns allen Zeit, Geld und andere Ressourcen. Mit Blick auf die nicht zuletzt aus Klimaschutzschutzgründen notwendige Verkehrswende ein unbestreitbar lohnenswerter Ansatz, solange und soweit dies nicht zur Profilbildung führt und damit auf Kosten der Privatsphäre geht.

Ein weiteres Paradebeispiel für ein sinnvolles allgemeines Verarbeitungsinteresse bietet die medizinische Forschung. Gerade unter Einschluss künstlicher Intelligenz bieten Behandlungsdaten ein wertvolles Reservoir für systematische und vernetzte interdisziplinäre wissenschaftliche Studien. Vom hierdurch möglichen medizinischen Fortschritt profitieren wir alle. Als Patienten von neuen Diagnostik- und Therapiemöglichkeiten, als Ge-

1 https://www.bitkom.org/Presse/Presseinformation/Datenoekonomie-Unternehmen-nutzen-Daten

meinschaft von besseren Erkenntnissen zur Gesundheitsprävention. Und nicht zuletzt können die Daten mittelbar helfen, den Versorgungs- und Finanzbedarf unseres Gesundheitssystems zu optimieren.

Und auch außerhalb der Gesundheitsforschung gibt es gute Gründe für das Teilen von Daten. So helfen beispielsweise landwirtschaftliche Daten aus Tierhaltung, Fischerei, Pflanzenbau und Forstwirtschaft sowie allgemeine Umwelt-, Geo- und statistische Daten bei der Vorhersage und Anpassung an den Klimawandel bis hin zur Vorhersage kurz- und langfristiger Gefahren- und Schadenslagen. Auch dies sichert Wohlstand und die kollektive und individuelle Sicherheit Aller.

Ein weiteres, plastisches Beispiel, das jeder kennt: Die beliebte Wikipedia ist nichts anderes als eine Open-Data-Gemeinschaftsplattform, gespeist aus universellen Quellen; es zeigt, was bei multilateraler Kooperation möglich ist.

Gerade im Bereich von Wissenschaft und Forschung drängen sich also der Nutzen des Teilens von Daten besonders auf. Aber vergessen wir nicht: Daten heißt Wissen, Wissen heißt Macht und Macht heißt Geld. Und genau diese Gleichung verlangt nach einer sensiblen Herangehensweise, denn ein vom Datenteilen bestimmter digitaler Wandel hat Auswirkungen auf uns alle.

Deshalb geht es beim Teilen von Daten nicht ohne einen kritischen Blick auf die Verarbeitungszwecke und die jeweiligen Verarbeiter mit ihren Interessen zu werfen. Denn das Teilen von Daten ist kein selbstloses Spiel nach dem Win-Win-Prinzip. Sollen geteilte Daten beispielsweise dafür genutzt werden, die Nachfrage von Konsumenten oder die für sie gültigen Preise und Konditionen individuell „zu lenken", kann von einem fairen Interessenausgleich gewiss keine Rede mehr sein. Das Teilen von Daten darf weder kollektiv, noch individuell zu strukturellen Ungleichgewichten führen. Hier geht es insbesondere um die gleichberechtigte Teilhabe an der Wertschöpfung sowie die diskriminierungsfreie und selbstbestimmte Teilhabe Aller in der digitalen Welt.

Vor diesem Hintergrund sehe ich insbesondere das Teilen von Daten im Kontext von Social- und Financial-Profiling oder Scoring äußerst kritisch. Wer Kredit, Versicherung oder Job nur noch nach Maßgabe von (Selbst-) Vermessung, Publizität, Prognosefähigkeit und Risikoabsicherung erhält, erntet keine Früchte der Digitalisierung, sondern ist Sklave seiner Daten. Eine Gesellschaft, die sich allein digitaler Entscheidungen und der Reduzierung des Einzelnen auf seine mehr oder minder „guten" Daten unterwirft, ist nicht frei, nicht demokratisch und auch nicht sozial. Sie ist schlicht

unmenschlich. Ein umfassender Datenschutz ist einer der wichtigsten Garanten, dass wir diese Entwicklung nicht gehen. Nicht zuletzt deswegen ist er so manchen Verarbeitern ein großer Dorn im Auge.

4. Aktuelle politische Bestrebungen zum Teilen von Daten

Wo stehen wir derzeit aktuell? Die gesellschaftliche Debatte über das Teilen von Daten ist in vollem Gange. Auch wenn wir uns in Deutschland etwas schwerer mit dem Gedanken des Teilens von Daten anfreunden können, geht es auch bei uns in der gesellschaftlichen Debatte längst nicht mehr um das „Ob" des Teilens von Daten, sondern im Schwerpunkt bereits um das „Wie".

Dabei werden von der Politik schon erste regulatorische Weichen gestellt. So hat das Bundeskabinett im letzten Jahr auf seiner Klausur auf Schloss Meseberg eine neue Digitalstrategie beschlossen, die Orientierung für die Zukunft des Digitalstandorts Deutschland bieten soll.[2] Darin enthalten ist das Bestreben einer sogenannten „neuen Datenkultur", die das möglichst zügige und breite Teilen industrieller wie öffentlicher Daten als Ziel beinhaltet, auch um als Industriestandort mit der globalen Konkurrenz weiter Schritt halten zu können. Und in einzelnen Bereichen laufen längst Normsetzungsprozesse, national, wie auch auf europäischer Ebene. So geht die Bundesregierung mit dem Gesundheitsdatennutzungsgesetz, das die Verfügbarkeit von Gesundheitsdaten für Forschungszwecke verbessern soll, bereits diesen Weg. Auch ein allgemeines Forschungsdatengesetz ist avisiert. Auf europäischer Ebene nimmt die Verordnung zur Schaffung eines europäischen Raums für Gesundheitsdaten Behandlungsdaten ebenso in den Blick. Ferner läuten der Data Governance Act und der Data Act einen Binnenmarkt für Daten ein, dessen Merkmale Fairness und Zukunftsfähigkeit sein sollen.

Ich will gar nicht auf jedes der genannten Vorhaben im Einzelnen eingehen, Kritik im Detail hätte ich durchaus. Aus Datenschutzsicht geht es allerdings am Ende immer um das Gleiche: Wie lassen sich bei personenbezogenen Daten diverse Verarbeitungsinteressen mit dem Schutz des Grundrechts auf informationelle Selbstbestimmung in Einklang bringen?

2 https://www.bundesregierung.de/breg-de/themen/digitalisierung/digitalstrategie-2072884

5. Der Staat nur verbal Vorreiter

Auch für uns Datenschützer sind Datenverarbeitungen kein Teufelszeug oder per se schlecht. Wir verstehen uns allerdings als Grundrechtslotsen der Digitalisierung. Diese Rolle verlangt von uns, digitale Entwicklungen zu begleiten und zu befördern, aber eben auch darauf hinzuwirken, Risiken für den Menschen und sein Grundrecht auf informationelle Selbstbestimmung zu minimieren. Denn wie bei allen grundlegenden Entwicklungen, so warten auch bei der Digitalisierung nicht nur Chancen, Verheißungen und Renditen auf uns, sondern es gibt – wie bereits angedeutet – ebenso fundamentale, grundrechtsbezogene Risiken.

In meiner zweiten Rolle als Bundesbeauftragter für die Informationsfreiheit ist mir qua Amt gleichfalls wichtig, dass jedenfalls die allgemein verwaltungsbezogenen Informationen des Staates getreu dem Prinzip von Open Data umfassend und auf einfache Weise für Alle verfügbar sind. Denn Transparenz als Kennzeichen einer modernen Verwaltung schafft Legitimation, bringt Kontrolle, verhindert Korruption, ermöglicht Beteiligung und erlaubt die Nutzung von Informationen als Wirtschaftsgut. Seit vielen Jahren fordere ich daher in meinen Tätigkeitsberichten, das Informationsfreiheitsgesetz zu einem Transparenzgesetz mit proaktiven Veröffentlichungspflichten weiterzuentwickeln.

Angesichts des Umstandes, dass die Bereitschaft des Staates, Informationen öffentlich zu teilen, allgemein noch nicht sehr hoch ist, sollte er in seiner Datenstrategie nicht nur zum Teilen von Daten aufrufen. Das Bild eines Daten-Ökosystems mit umfassendem Data Sharing zu entwerfen, dann aber selber in der Praxis nicht mit gutem Beispiel voranzugehen, ist ein großer Fehler. Gerade die öffentliche Verwaltung verfügt über ein nahezu unerschöpfliches Maß an Statistiken, Erhebungen, Entscheidungen, Verkehrs- und Umweltdaten, Geo- und Wetterdaten, Haushaltsdaten, Protokollen und Publikationen. Alles ist zwar irgendwie irgendwo vorhanden, aber halt nicht öffentlich erschlossen. Angesichts dieses riesigen ungenutzten Potentials wird der Staat seiner Vorbildfunktion mit Blick auf das Teilen von Daten nicht gerecht. Ich hoffe, dass sich hier bald etwas tut. Aktuell jedenfalls fehlt es staatlicherseits teilweise am Willen und ebenso noch weitgehend an den technischen Voraussetzungen.

6. Gewinner und Verlierer beim Teilen von Daten

Wie bei jedem gesellschaftlichen, wirtschaftlichen und technischen Umbruch gilt auch im Kosmos der Digitalisierung und speziell beim Teilen von Daten: es gibt immer Gewinner und Verlierer. Und hier liegt die Verantwortung der Politik, nämlich nicht allein die bisherigen Daten-Giganten reicher zu machen, sondern auf faire Weise allen Teilen von Wissenschaft, Wirtschaft und Gesellschaft Prosperität zu ermöglichen; alles andere wäre ein blanker Datenkapitalismus, nicht anders als der industrielle Manchester-Kapitalismus.

Dabei ist die Ausgangslage allerdings alles andere als rosig. Faktisch haben wir es längst mit einem Daten-Oligopol von – außerhalb Chinas – im Wesentlichen US-amerikanischer Tech-Giganten und zentralisierten Plattformen zu tun. Deren Lust zum Teilen von Daten ist naturgemäß nicht sonderlich ausgeprägt; sie setzen eher auf eine Daten-Einbahnstraße gegenüber allen anderen Beteiligten. Sie sind schon jetzt die großen Gewinner, denn sie verfügen exklusiv über weite Teile der täglich anfallenden Daten. Diese werden auch beständig mehr, denn allumfassende Services in allen Lebensbereichen und die Lust der Menschen am digitalen Konsum sorgen für eine nie versiegende Datenquelle. Wer dann noch über exklusive Services oder Endgeräte den Markt kontrolliert ist dann in der Poleposition für jede Form des Big Data.

Und selbst, wenn diese Unternehmen dann doch einmal Daten mit anderen teilen müssen, können sie eigentlich nur gewinnen, denn ihr Datenschatz wird dann auch noch von Anderen gespeist. Allein ihre Marktmacht impliziert nämlich, dass sie weit mehr vom Zugriff auf fremde Daten profitieren als die kleine und mittelständische Digitalwirtschaft, die Wissenschaft und Forschung oder gar die Allgemeinheit. Denn allen anderen Akteuren fehlt ein vergleichbares Know-how ebenso wie technische und wirtschaftliche Ressourcen auf Augenhöhe. Das unter anderem auch mit der DSGVO verfolgte Ziel, ein einheitliches Level Playing Field zu schaffen, ist in der Realität leider auch nach fast 6 Jahren noch nicht annähernd erreicht.

Wer also nicht möchte, dass nach der Devise: „The winner takes it all" die Großen als Sieger vom Platze gehen und das breite Teilen von Daten zum sozioökonomischen Bumerang wird, muss handeln und die Datenmacht der großen Datenkonzerne brechen. Deswegen geht es beim Teilen von Daten zwangsläufig um rechtliche und strukturelle Vorkehrungen, sodass ein profitabler Anteil am Datenpool allen verbleibt. Schlagworte sind

hier Chancengleichheit und Fairness. Und an einigen Stellen muss das Datensammeln der US- (und China-)Datenkraken schlicht unterbunden werden. Letztlich dürfte es auch in Kreisen unserer heimischen Wirtschaft kaum vermittelbar sein, zwar Daten mit den amerikanischen Platzhirschen teilen zu müssen, ohne jedoch gleichermaßen eine vergleichbare Perspektive auf eigene prosperierende Verarbeitungen zu haben.

Aus meiner Sicht stellt sich gerade beim Thema Teilen von Daten mehr als an jeder anderen Stelle in der digitalen Welt die Frage nach der Gemeinwohlorientierung, insbesondere wenn das Teilen von Daten teilweise verpflichtend sein soll. Nach alledem: Politisch kann es angesichts der Erfordernisse der Digitalisierung tatsächlich nicht mehr um das „Ob" des Daten-Teilens gehen. Wohl aber müssen wir uns Gedanken über das „Wie" der Entwicklung machen.

7. Das Gefahrenpotential der Datenmonopolisten

An dieser Stelle möchte ich noch etwas mehr auf die großen Tech-Giganten eingehen. Ihr Datenhunger, ihre Lock-in-Effekte und ihre Datenmonopole sind für den Kurs einer digitalen Gesellschaft und insbesondere die Freiheit, Chancengleichheit und Selbstbestimmung ihrer Individuen entscheidend. Die Überdominanz dieser Konzerne steht eigentlich schon sinnbildlich für das Prinzip „The winner takes it all". Dies nicht nur in wirtschaftlicher Hinsicht, sondern auch gegenüber Selbstbestimmung suchenden Grundrechtsträgern.

Diese Unternehmen entscheiden über favorisierte Technologien, gängige Geschäftsmodelle und üben großen Einfluss in wirtschaftlicher und politischer Hinsicht aus. Die These, große Tech-Giganten gehörten möglicherweise zerschlagen, hört sich übrigens weit weniger radikal an, wenn man folgendes bedenkt: Marktbeherrschende Unternehmen verfolgen mit Blick auf Zukunftsentwicklungen gerade keinen allgemeinzivilisatorischen Ansatz, sondern nehmen interessengeleitet allein die eigene Profitmaximierung zum Fortschrittsmaßstab. Auf diese Weise beschränken sie zwangsläufig das Entwicklungspotential der Digitalisierung, indem sie Entwicklungen mittelbar oder unmittelbar einseitig prägen und keinen Raum für konkurrierende Ansätze lassen.

Zudem besteht das Risiko, dass sie qua Machtfaktor die Gesellschaft auch inhaltlich formen und im schlimmsten Fall aktiv Einfluss zu nehmen versuchen. Zu denken wäre hier beispielsweise an einen Kurznachrichten-

dienst unter einer sendungsbewussten neuen Führung. Und selbst eine vermeintlich unabhängige Aufsicht steht – und dies nicht nur auf grünen Inseln – im Risiko, sich marktmächtigen und wirtschaftlich bedeutsamen Giganten anzupassen und nicht umgekehrt, wie es eigentlich sein sollte. Zum Schutz unseres wirtschaftlichen, sozialen und demokratischen Gemeinwesens sollten marktdominante Akteure der digitalen Welt daher aus allen Blickwinkeln kritisch betrachtet werden. Aus ihrer ambivalenten Rolle leiten sich schließlich auch die Bedingungen für das Teilen von Daten ab. Letztlich beginnt die Freiheit des Digitalen erst, wo die Freiheit der Monopolisten endet!

8. Der plurale Datenkosmos als Herz des demokratischen Gemeinwesens

In der digitalen Welt steht der Austausch von Informationen, sprich das Teilen von Daten, sinnbildlich für soziale Interaktion und ist deren unverzichtbare wie logische Voraussetzung. Hierbei gilt: Je vielfältiger und umfassender Informationen und ihr Austausch sind, umso breiter und offener ist der Dialog. Und umgekehrt gilt: Je limitierter Informationen und ihr Kommunikationsraum sind, umso kleiner und einseitiger fallen gesellschaftlicher und politischer Diskurs aus. Anders gesagt: Demokratie lebt vom Teilen von Informationen, speziell vom Teilen von Daten. Es gibt also ein demokratisches Vitalinteresse an einem pluralen Datenkosmos. Wenn wir also über das Teilen von Daten sprechen, stellt sich nicht allein die Frage nach dem zivilisatorischen Mehrwert unter dem Gesichtspunkt wirtschaftlicher, wissenschaftlicher und gesamtgesellschaftlicher Prosperität. Genauso geht es um jene originäre Inhalts- und Angebotsvielfalt sowie Transparenz, die ein demokratisches Gemeinwesen zwingend verlangt, gerade wenn der soziale Interaktionsraum zunehmend digitaler wird.

Pluralität, wie wir sie als Demokraten gewahrt wissen wollen, ist in der digitalen Welt aber keineswegs selbstverständlich – weder technisch, noch wirtschaftlich, noch politisch. Die vordergründig scheinbar grenzenlose Offenheit und Transparenz des vernetzten digitalen Raumes, an die wir alle gerne glauben möchten, wird schnell sehr klein, wenn Algorithmen, Lock-in-Areale sowie fehlende Interoperabilität und fehlende Interaktion inhaltliche Grenzen setzen.

Dahinter muss nicht einmal die böse Absicht dominanter Akteure und der von ihnen geprägten Technik stehen. Es reicht, und ich glaube wir befinden uns auch hier in Deutschland schon an dieser Stelle, wenn wir den

Gedanken des Netzes als offenen wirtschaftlichen, sozialen und demokratischen Gemeinschaftsraums vernachlässigen und geschlossenen Filterblasen insbesondere undemokratischer Kreise untätig überlassen. Deshalb plädiere ich auch aus diesem Blickwinkel für ein „Digital Diversity by default", gelebt durch das Teilen von Daten.

9. Die Fairness-Balance – Bedingungen für einen digitalen Fortschritts- und Vertrauensraum

Wie schon an anderer Stelle angeklungen: Wenn etwas für die Akzeptanz und die Mitwirkung einer zivilisatorischen Entwicklung „tödlich" ist, dann das Gefühl der Ohnmacht des Ausgeliefertseins, gerade gegenüber einzelnen dominanten Playern. Der dahinterliegende Gedanke ist simpel: Die Digitalisierung ist nur dann erfolgreich, wenn sie entwicklungszivilisatorisch Fortschritt und Wohlstand für möglichst Viele bringt. Dies wiederum setzt die Bereitschaft einer Gesellschaft voraus, zielorientiert den hierfür notwendigen technologischen Wandel zu beschreiten und sich digitalen Angeboten in allen Bereich des Lebens zu öffnen.

Dafür brauchen insbesondere natürliche Personen das notwendige Vertrauen in den Nutzen und die Integrität des Wandels. Es geht also gleichermaßen um einen Fortschritts- und Vertrauensraum. Beim Teilen von Daten bedeutet dies letztlich die Einsicht aller, dass Teilen keinen Verlust, sondern einen Gewinn bedeutet.

Hinsichtlich des Teilens von Daten müssen dafür aus meiner Sicht zehn wichtige Bedingungen erfüllt werden, die ich über das allgemeine Datenschutzrecht und Datenschutz-Credo als Parameter einer zwingend ausgewogenen Fairness-Balance bezeichnen möchte:

1. Keine Datenmonopole
2. Keine Datensilos
3. Kein Sacheigentum an Daten
4. Eine umfassende Technologiefreiheit und Interoperabilität
5. Ein fairer, diskriminierungsfreier Datenzugang aller Marktteilnehmenden und Forschenden
6. Ein fairer Wettbewerb auf Augenhöhe, u.a. durch Chancengleichheit gegenüber den Tech-Giganten
7. Eine faire Beteiligung aller, also auch der Datensubjekte, an den Früchten bzw. der Wohlstandsrendite

8. Ein austarierter Schutz von Geschäftsgeheimnissen sowie des geistigen Eigentums
9. Ein verlässlicher Rechtsrahmen, der die genannten Bedingungen sichert, flankiert von einer effektiven Aufsicht mit einem effektiven Sanktionsregime und schließlich
10. Keinerlei Erosion des Grundrechts auf informationelle Selbstbestimmung und keine Einschränkung bei der Datensicherheit.

Zur Schaffung eines solchen Fortschritts- und Vertrauensraums ist aus dem Blickwinkel des Datenschutzes insbesondere der Schutz des Grundrechts auf informationelle Selbstbestimmung entscheidend.

10. Keine Sozialpflichtigkeit, Daten zur eigenen Person zu teilen

Bisher habe ich nicht wirklich durchgehend zwischen personenbezogenen und nicht-personenbezogenen Daten differenziert. Dies ist aber für die notwendige datenschutzrechtliche Einordnung erforderlich. Schließlich ist es rechtlich völlig unbedenklich, nicht-personenbezogene Daten, wie beispielsweise Maschinendaten, Geodaten, Statistiken oder sonst anonyme Daten zu teilen. Und bei ehrlicher Betrachtung haben wir es in der digitalen Welt eigentlich überwiegend mit solchen nicht-personenbezogenen Daten zu tun.

Die Behauptung, es gäbe zukünftig eigentlich keine Daten ohne Personenbezug mehr, ist schlicht falsch und kommt meistens aus dem Kreis jener Stimmen, die alles über einen Kamm scheren wollen, damit der ungeliebte besondere Schutz personenbezogener Daten perspektivisch sein Ende findet. Der wahre, gegenteilige Umstand, dass Big Data in sehr vielen Fällen gar keine Personenbezüge erfordert, liegt dabei eigentlich auf der Hand. Bis auf den Bereich individueller Angebote oder des gezielten werblichen Tracking ist die konkrete Identität einer Person zumeist völlig irrelevant.

An dieser Stelle möchte ich übrigens darauf hinweisen, dass das Anonymisieren personenbezogener Daten der zentrale Schlüssel zur Weiterverarbeitung und auch dem unproblematischen Teilen von Daten ist. Aktuell fehlt es mir aber noch deutlich an der Aufgeschlossenheit, den Weg der Anonymisierung zu beschreiten, obwohl in technischer Hinsicht sehr Vieles auf sehr einfache Weise möglich ist.

Bei klarer Transparenz und absolut freiwilliger Willensentscheidung ist darüber hinaus das Teilen personenbezogener Daten grundsätzlich auch auf Einwilligungsgrundlage möglich. In der Praxis sieht es hier aber zu-

meist nicht sehr gut aus oder, anders gesagt, die Bedingungen, die das Datenschutzrecht hier aus gutem Grunde fordert, werden allenfalls oberflächlich eingehalten.

Ohnehin steht die informierte Einwilligung bei der datenverarbeitenden Ökonomie nicht sehr hoch im Kurs. Zu einfach und schön ist es doch, einen Datenkosmos zu forcieren, der breiteste Verarbeitungen und auch das Teilen von Daten qua bloßer Interessenlage gestattet. Die Vorstellungen gehen hier soweit, dass im Interesse digitaler Wertschöpfung eine weitgehende Verpflichtung zum Teilen auch personenbezogener Daten gefordert wird.

Um es klar zu sagen: Aus meiner Sicht gibt es keine allgemeine, insbesondere voraussetzungslose Sozialpflichtigkeit, Daten zur eigenen Person qua Sonder- bzw. Grundrechtsopfer für Zwecke allgemeiner digitaler Prosperität abseits spezifischer Fragen z.B. im Gesundheitssektor zur Verfügung zu stellen. Andernfalls würden wir den Kern des Grundrechts auf informationelle Selbstbestimmung aufgeben. Dies wäre wiederum reiner Datenkapitalismus – für mich ein Schreckensbild!

11. Von der Freiwilligkeit des Teiles personenbezogener Daten

Dass nicht jede vermeintlich freiwillige Datenpreisgabe personenbezogener Daten den hehren Ansprüchen des Datenschutzes genügt, ist hinlänglich bekannt; ich erwähnte es bereits. Doch auch die Verfechter einer weniger strengen Sicht müssen gelegentlich zugeben, dass es weniger die innere Überzeugung ist, die Menschen „freiwillig" ihre Daten teilen lässt, als vielmehr das alternativlose Geschäftsgebaren der hier schon mehrfach erwähnten großen Marktteilnehmer.

Auf der anderen Seite räume ich unumwunden ein, dass es gelegentlich auch der Reiz von Technik und die Verführung lukrativer Services und Preise ist, die zur Datenpreisgabe bzw. dem Teilen eigener Daten verleiten. So gehört es zu digitaler Interaktion schlicht dazu, dass wir alle breit Dinge posten, liken und teilen. Und dies ist prinzipiell auch gut so. Bliebe es bei der offen erkennbaren bzw. erwartbaren Verarbeitung personenbezogener Daten, die zur Nutzung eines Angebots naturgemäß notwendig ist, wäre dies auch kaum ein Problem.

Die Realität ist aber eine andere. Von der Marktmacht einzelner Anbieter gezwungen oder wegen fehlender Transparenz blenden viele Nutzende weitreichende und teils sehr sensible Annexverarbeitungen aus bzw. sind

sich dieser nicht bewusst. Für uns Datenschützer ist es immer wieder erschreckend, was sich hinter teils sybillinischen Datenschutzerklärungen verbirgt. Deswegen gehört für mich zur „neuen" Kultur des Teilens von Daten unabdingbar dazu, sich von der „alten" Unkultur des „unfreiwilligen" Teilens von Daten zu verabschieden.

12. Den Kern von Freiheit wahren: Selbstbestimmung

Wenn die Zukunft der Digitalisierung im Teilen von Daten besteht, müssen wir also darüber reden, unter welchen Bedingungen und in welchem Umfang für welche Zwecke unter welchen besonderen Vorkehrungen personenbezogene Daten Eingang in die Kultur des Teilens von Daten finden. Und um den Begriff des immer wieder beschworenen risikobasierten Ansatzes gleich vorweg aufzugreifen: Das Wesen der Digitalisierung liegt in ihrer kaum vorausplanbaren Dynamik und der Schwierigkeit, aus den einzelnen Schritten auf das Gesamtbild des Datensammelns und -auswertens zu schließen. Es lässt sich eben heute nicht sagen, was morgen kommt. Das ist der Grund, weshalb allein risikobasierte Ansätze Fehlentwicklungen im Vorfeld nicht sicher ausschließen können und immer die Gefahr besteht, dass bedenkliche Verläufe sich ordnungspolitisch kaum mehr einfangen lassen.

Ich glaube auch, dass unser Verfassungsrecht und auch die Europäische Grundrechtecharta an einer so sensiblen Stelle wie dem gesamtgesellschaftlichen und gesamtwirtschaftlichen Teilen personenbezogener Daten keine Kompromisse außerhalb der bisherigen und bewährten Struktur des Datenschutzrechts zulässt. Eine Erosion des Grundrechts auf informationelle Selbstbestimmung wäre auch inhaltlich kaum zu rechtfertigen, denn wie gesagt, ist Teilen personenbezogener Daten in den allermeisten Fällen überhaupt nicht notwendig.

Zudem stelle man sich vor, dass ausgerechnet im Bereich des universellen Teilens von Daten mindere Schutzstandards als bei übrigen Verarbeitungen gelten sollen. Dies wäre insgesamt der Einstieg in den Ausstieg aus dem Datenschutzrecht und damit aus der Freiheit zur Selbstbestimmung, wie sie Bundesverfassungsgericht und EuGH aus Grundgesetz und Grundrechtecharta abgeleitet haben. Dass ich dies nicht gutheißen kann, ist sicher verständlich.

Wir brauchen stattdessen eine andere Herangehensweise, ausgehend vom bisherigen Recht. Und hier wäre zunächst einmal zu klären, für

welche, dann legitimen Zwecke, sich ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung im Kontext des Teilens von Daten rechtfertigen lässt. Angesichts der besonderen grundrechtlichen Bedeutung der Privatsphäre gerade in der digitalen Welt geht es hier um Fallgruppen hochrangiger Gemeinwohlinteressen. Und dies ist nicht das generelle Bedürfnis der Datenökonomie nach Daten. Vielmehr muss es um gesamtgesellschaftliche Belange wie die Lösung bedeutsamer Probleme, etwa das Überwinden von Krankheiten, Mobilitätsdefiziten oder der Kriminalitätsbekämpfung, gehen.

Auch das zivilisatorische Fortkommen, die Sicherung und der Ausbau des Wohlstandes sowie der gesamtgesellschaftliche Nutzen sind Betrachtungen, die je nach Verarbeitung verhältnismäßig sein können. Am Ende ist zudem aus der Perspektive des Betroffen die abstrakte Frage zu stellen, inwieweit auch ihm das Ergebnis einer Verarbeitung individuell nutzt, die sich aus seinen Daten speist. Denn wer nicht möchte, dass das Phänomen „The winner takes it all" aufgeht, muss die Frage nach fairer Beteiligung auch der Datensubjekte an den Früchten von Verarbeitungen stellen.

Insgesamt lässt sich folgende Gleichung aufstellen: Je mehr es um partikulare und einseitig monetäre Interessen geht, umso weniger verfängt eine Rechtfertigung eines Grundrechtseingriffs. Und umgekehrt: Je überragender der Beitrag zum Allgemein- und individuellen Wohl der Grundrechtsträger, desto legitimer kann eine Verarbeitung sein.

Das Beispiel, an das viele an dieser Stelle denken und das ich in diesem Beitrag bereits aufgegriffen habe, ist die medizinische Forschung. Von ihr profitieren wir alle. Die schon genannten Stichworte sind hier: Medizinischer Fortschritt, Volksgesundheit und Finanzierbarkeit des Gesundheitswesens. Allerdings – und dies möchte ich betonen – geht diese Gleichung nur auf, wenn auch hier das Prinzip Fairness gilt. Pharmakonzerne, die von den Daten der Allgemeinheit profitieren, müssen bei ihren Preisen berücksichtigen, dass die Entwicklung ihres Präparates ganz wesentlich auf Ressourcen der Allgemeinheit beruht. Genau dies drückt beim Teilen von Daten die beschriebene Win-Win-Situation aus, die für eine solche neue Datenkultur und deren Akzeptanz entscheidend ist.

13. Differenzierte Datenräume und weitere Safeguards schaffen!

Angesichts der unterschiedlichen Kontexte des Teilens von Daten und den sich hieraus ergebenden unterschiedlichen Vorgaben ist es gerechtfertigt,

Verarbeitungslagen normativ differenziert aus dem Verbot mit Erlaubnisvorbehalt positiv herauszuarbeiten. So entstehen einzelfallbezogen getrennte Räume zum Teilen von Daten.

Der Begriff des Datenraumes bedeutet – und das macht ihn zum Schutz- und Vertrauensraum – die Abkehr von dem einen großen Datenpool hin zu sektorspezifischen, intelligent vernetzten dezentralen Datenräumen mit klaren Regeln. Eine davon kann übrigens auch darin bestehen, die uns bekannten Monopolisten von der Nutzung auszunehmen. Überhaupt lässt sich, wie es auch das Datenschutzrecht möchte, sehr gut zwischen unterschiedlichen Daten, Akteuren, Zwecken und weiteren Bedingungen differenzieren. Ich weiß, dies bedeutet für Einige zu viel regulatorisches Fahrwasser. Und dies an einer Stelle, wo Forschung und Entwicklung gefühlt eigentlich große Freiräume bräuchten. Zudem ist es eine Herausforderung, vorab möglicher wissenschaftlicher Korrelationen Datenräume sinnvoll ab- und einzugrenzen. Dem kann aber durch eine Flexibilität in der späteren Anpassung und Vernetzung Rechnung getragen werden.

Ein weiterer Vorteil solcher Datenräume besteht darin, dass sie sich mit Treuhändermodellen (z.B. Non-Profit-Akteuren als Intermediären) und Aufsichtsmodulen sehr gut kombinieren lassen und in ihrer überschaubaren Struktur revisionssicher sind. Und natürlich sind dezentrale Datenhaltungen unter Sicherheitsgesichtspunkten von Vorteil. Im Kosmos geteilter Daten braucht es zudem weitere Sicherungsmaßnahmen jedenfalls dann, wenn es um personenbezogene Daten geht. Vieles ist hier vorstellbar. Da wäre zum einen eine Eigenständigkeit oder zumindest binnenorganisatorische Selbstständigkeit der Betreiber der Datenräume. Zum anderen wäre an eine Zertifizierung zu denken. Und auch die Aufsicht spielt eine wichtige Rolle. Hinzu kommen die Instrumente des Wettbewerbsrechts und des wirtschaftlichen Verbraucherschutzes in Gestalt von Unterlassungsklagebefugnissen der Marktbeteiligten.

Wichtig ist mir, dass wir den digitalen Kosmos dabei ganzheitlich betrachten. Denn an den Komplex des Teilens von Daten schließt sich beispielsweise nahtlos das Thema Einsatz künstlicher Intelligenz an – ein nochmals ganz eigenes Problemfeld. Die Komplexität der Digitalisierung zwingt uns also, alle ihre Facetten in drei Dimensionen nebeneinander zu betrachten. Der Datenschutz ist dabei ein zentraler Baustein.

14. Fazit: Europäisch denken!

Wir alle merken zunehmend, dass sich die (politischen) Werteräume in dieser Welt diametral unterscheiden. Und ich befürchte, dass sich dieser Trend noch fortsetzen wird. Die Unterschiede in der Wertekultur, gerade was den Freiheitsbegriff angeht, zwingen aber dazu, sich auch in der Verarbeitungskultur zu unterscheiden, auch auf die Gefahr hin, dass andere Teile der Welt in Einzelfällen davon profitieren, dass sie keine Skrupel haben, ihre Bürgerinnen und Bürger gläsern zu machen und für Zwecke vordergründiger wirtschaftlicher Prosperität auszubeuten.

Ich warne jedenfalls davor, die vermeintlich so tolle Verarbeitungsfreiheit Anderer, die sich in Wahrheit auf Unfreiheit gründet, zum Maßstab unseres digitalen Zusammenlebens zu nehmen. Auf Wettbewerbsverzerrungen im Digitalen müssen wir wie im Analogen reagieren und – wenn wir sie nicht durch andere Instrumente wie angepasste Technologien ausgleichen können – notfalls zu Marktzugangsbeschränkungen greifen. Denn ohne ein einheitliches Level-Playing-Field geht es nicht. Was uns für den Schutz unserer Autowirtschaft recht ist, sollte uns für den Schutz unserer Daten und Digitalmärkte billig sein.

Ich habe manchmal das Gefühl, dass Einige hier in Europa im Angesicht der Tech-Giganten und ihrer Marktmacht in einen gefühlten David-gegen-Goliath-Komplex verfallen. Nach dem Motto „The winner takes it all" faktisch aufzugeben und das Teilen von Daten nur unter dem Aspekt zu forcieren, dass hiermit vielleicht einige Krumen vom Tisch der Herren fallen, wird weder der Bedeutung des Teilens von Daten für die Digitalisierung, noch der Rolle Europas gerecht. Ein Binnenmarkt mit fast 500 Millionen Menschen und einem BIP von 15 Billionen Euro braucht sich nicht zu verstecken und sollte selbstbewusst auf die eigene Kreativität setzen und auf die Einhaltung seiner Marktverhaltensregeln pochen.

Es bringt nichts, mehr schlecht als recht unter Aufgabe von Grundrechtspositionen schrittweise dem vermeintlich erfolgreicheren Verarbeitungshandeln Anderer nachzueifern. Stattdessen sollten wir lieber die Eindimensionalität der Tech-Welt beenden.

Und was heißt dies? Wir brauchen einen europäischen Ansatz, unabhängig und jenseits bisheriger vermeintlicher oder tatsächlicher Gewinner! Dies sage ich im Bewusstsein, dass wir jedenfalls hinsichtlich der Verarbeitung personenbezogener Daten mit der Datenschutz-Grundverordnung bereits einen sehr guten Ordnungsrahmen haben, auf dem wir aufbauen

können. Ich weiß, nicht jeder teilt diese Einschätzung, aber unbestreitbar ist, dass das europäische (Datenschutz-)Recht international Maßstäbe setzt.

In einem gemeinsamen europäischen Binnenmarkt, der eben nicht nur ein Wirtschafts- und Sozialraum, sondern auch eine Wertegemeinschaft ist, müssen wir grundsätzlich gemeinsame Regeln haben, auch was das Teilen von Daten angeht. Der europäische Digitalraum sollte ein datenagiles System mit einem grundrechtsakzentuierten Schutz, widerstandsfähiger und offener Datenkultur und -infrastruktur bei wehrhaften europäischen Werten und Prinzipien sein. So entsteht ein zukunftsträchtiger gemeinwohlorientierter Chancenraum mit Platz für Innovation und Wettbewerbsfähigkeit.

2 Datenintermediäre: Neue Ansätze für das Data Sharing

Governance von Datenräumen: Akteure, Strukturen und Phasen der Datenraum-Governance

Abel Reiberg, Crispin Niebel, Anna-Raphaela Schmitz

Zusammenfassung

Mit Datenräumen wird die Hoffnung verbunden, die Datenökonomie zu stärken und dabei die Rechte auf Privatheit, Transparenz und Selbstbestimmung zu verbessern. Entsprechend wird der Aufbau von Datenräumen aktuell intensiv gefördert. Bei diesem kommt insbesondere der Governance (hier verstanden als die Koordinierung der relevanten Akteure) entscheidende Bedeutung zu. Datenräume sind föderiert aufgebaut und bieten daher einer Vielzahl von Akteuren die Möglichkeit, als Teilnehmende und Betreiber mitzuwirken. Dies ist jedoch Chance und Herausforderung zugleich: Einerseits lassen sich Datensouveränität, Wettbewerb und Innovation in offenen Datenräumen potenziell leichter realisieren als in zentralisierten Infrastrukturen. Andererseits gilt es dafür ein effizientes, effektives und faires Zusammenwirken der Akteure durch entsprechende Governance-Arrangements zu gewährleisten. Zweck dieses Beitrags ist es, eine Einführung in Themen der Datentraum-Governance zu bieten und so die theoretische Auseinandersetzung mit Lösungen sowie die praktische Umsetzung dieser zu fördern. Dazu wird jeweils kurz auf grundlegende Themen, darunter Akteure, Strukturen und Phasen der Datenraum-Governance, eingegangen.

1. Einleitung

Der Aufbau von Datenräumen wird derzeit als ein taugliches Mittel betrachtet, um die Entwicklung der Datenökonomie in Europa zu stärken und gleichzeitig die Rechte der beteiligten Akteure – darunter insbesondere auch das Recht auf Privatheit – zu stärken.

Dies beruht unter anderem auf dem dezentralen Aufbau von Datenräumen. Diese bieten per se einer größeren Anzahl an Akteuren Mitwirkungsmöglichkeiten – nicht nur bei der Nutzung, sondern auch beim Betrieb. Monopolbildung und ein daraus resultierendes Machtgefälle zwischen Anbietenden und Nutzenden, das in der aktuellen Datenökonomie oftmals

anzutreffen ist und vielfach zur Benachteiligung von Nutzenden und insbesondere deren Privatheit geführt hat, soll vermieden werden.

Daher wird der Aufbau von Datenräumen aktuell mit einer Vielzahl von Maßnahmen insbesondere von staatlicher Seite unterstützt. Zu diesen zählen sowohl Regulierungsmaßnahmen wie beispielsweise der Data Governance Act (DGA) als auch Fördermaßnahmen wie jene zu „Europäischen Datenräumen" und Gaia-X.

Der intensiv geförderte Aufbau von Datenräumen bietet wichtige Chancen: Er stärkt die europäische Datenökonomie unter Berücksichtigung von Werten wie Privatheit, Sicherheit und Transparenz. Gleichzeitig stehen dem Aufbau von Datenräumen viele Herausforderungen entgegen: Anders als bei zentralisierten Infrastrukturen sind bei dezentralen Infrastrukturen wie Datenräumen eine Vielzahl unterschiedlicher Akteure in verschiedenen Koordinationsformen dauerhaft einzubeziehen. Dadurch ergeben sich hohe Anforderungen in Bezug auf die zu etablierenden Governance-Arrangements.

Um diese Herausforderungen meistern zu können, braucht es ein grundlegendes Verständnis darüber, was Datenraum-Governance umfasst und welche Gestaltungsoptionen sich bieten. Der vorliegende Beitrag soll diese Fragen adressieren und das neue Feld der Datenraum-Governance beleuchten.

Zu diesem Zweck wird zunächst dargelegt, was unter Datenraum-Governance zu verstehen ist. In den anschließenden Abschnitten werden dann zentrale Themen der Governance von Datenräumen betrachtet, darunter Akteure, Strukturen und Phasen der Datenraum-Governance. Jedes der Themen wird mit Bezug zu zwei konkreten Projekten aus dem Kontext von Gaia-X – dem Mobility Data Space (MDS) und Catena-X – erläutert. Ziel dabei ist es, die jeweiligen Aspekte der Datenraum-Governance zu veranschaulichen und konkrete Umsetzungsoptionen aufzuzeigen.

2. Begriffsbestimmung: Datenraum-Governance

Um zu klären, was Governance von Datenräume umfasst, bietet es sich an, zunächst die beiden Begriffsbestandteile „Datenraum" und „Governance" zu betrachten und anschließend zu klären, was als „Datenraum-Governance" zu verstehen ist.

2.1 Datenraum

Es wurden bereits zahlreiche Definitionen und Beschreibungen des Konzeptes Datenraum vorgelegt. Beim Vergleich der verschiedenen Ansätze, darunter den Definitionsansätzen der Gaia-X-Association, der International Data Spaces Association und der Europäischen Kommission zeigen sich jedoch zahlreiche Gemeinsamkeiten (Reiberg et al. 2022, S. 9-10). So wird die Ermöglichung des Datenteilens (Data Sharing) durchgehend als zentrale Funktion von Datenräumen genannt. Zudem werden als Merkmale von Datenräumen ein föderierter/dezentraler Aufbau, die Nutzung gemeinsamer Regelsysteme, sowie die Sicherstellung von Datensouveränität, Interoperabilität und Offenheit gegenüber Teilnehmern und Betreibern genannt. Auf diese Gemeinsamkeiten gestützt, lässt sich ein Datenraum definieren als „föderierte, offene Infrastruktur für souveränen Datenaustausch, die auf gemeinsamen Vereinbarungen, Regeln und Standards beruht" (Reiberg et al. 2022, S. 11).

Vereinfacht lassen sich die stets dezentral aufgebauten Datenräume als Gegenmodell zu den zentralisierten Plattformen betrachten, die aktuell die Datenökonomie stark prägen. Sie sind offen gestaltet, da sie Teilnehmern offenstehen, die innerhalb der Datenräume Daten anbieten und nachfragen können. Sie sind zudem auch insofern offen gestaltet, als neben der Nutzung auch der Betrieb eines Datenraums für interessierte Akteure offensteht. So, wie beispielsweise bei dem System E-Mail, kann sich prinzipiell jeder, der die entsprechenden grundlegenden Anforderungen erfüllt, an Entwicklung und Betrieb der Infrastruktur — ähnlich wie mit dem Betrieb eines E-Mail-Servers — beteiligen. Dezentralität wird auch erreicht, weil Datenrauminitiativen die Interoperabilität der Datenräume zum Ziel haben. So soll ermöglicht werden, dass beispielsweise ein Datenraum, in dem Wetterdaten ausgetauscht werden, auch interoperabel ist mit einem Datenraum in dem Mobilitätsdaten ausgetauscht werden, um weitere nutzenbringende Anwendungen, beispielsweise Informationen über Gefahrensituationen im Straßenverkehr, zu ermöglichen. Bereits dieser dezentrale Aufbau selbst hilft dabei, Lock-In-Situationen zu vermeiden, in denen einzelne große Anbieter gegenüber Nutzenden Bedingungen durchsetzen können, die für diese unvorteilhaft sind. So beispielsweise Bedingungen, die Nutzende dazu bewegen, mehr Daten preiszugeben als gewollt und somit die Privatheit der Nutzenden gefährden. Ziel der Datenrauminitiativen ist (wie bereits obige Definition nahelegt) vielmehr ein souveräner Datenaustausch, bei dem es den Nutzenden möglich ist, weitgehend selbst zu bestim-

men, mit wem sie in welchem Maße und zu welchen Bedingungen Daten austauschen. Das somit resultierende Mehr an Souveränität soll wiederum einen bewussten Datenaustausch und den damit verbundenen Nutzen ermöglichen. Der dezentrale Aufbau ist jedoch auch mit Herausforderungen verbunden. Die Beteiligung einer Vielzahl von Akteuren erfordert eine effektive und effiziente Koordination, womit der Bereich der Governance angesprochen ist.

2.2 Governance

Das Konzept Governance selbst ist angesichts der Vielzahl der Definitionsansätze schwer zu umreißen. Bis etwa Ende der 1980er Jahre wurde der Begriff selbst im englischen Sprachraum vergleichsweise wenig genutzt und meist zur Beschreibung staatlichen Handelns, also des Handelns von Regierungen (Governments) verwendet (Mayntz 1998). Ab etwa den 1990er Jahren fand der Begriff dann eine weitere Verbreitung auch im deutschen Sprachraum und wurde erweitert, um auch Formen der kollektiven Entscheidungsfindung jenseits des Staates miteinzuschließen (ebd.). Vereinfachend lässt sich Governance als Steuerung oder Koordinierung gesellschaftlicher Akteure betrachten[1] (Benz 2004, S. 25).

Berücksichtigt werden mit der zunehmenden Verwendung des Begriffs unter anderem zwei Dinge:

Zum ersten wird berücksichtigt, dass gesellschaftliche Koordinierung und Regelsetzung entsprechendes Handeln oftmals sowohl von staatlichen als auch privaten Akteuren umfasst beziehungsweise erfordert[2]. So nehmen in Regulierungskontexten neben staatlichen auch private Akteure, beispielsweise Auditierungs- und Standardisierungsorganisationen, wichtige Rollen ein. Und auch privatwirtschaftliche Unternehmen müssen, um ihr Funktionieren sowie das Erreichen weiterer gesellschaftlicher Ziele sicherzustellen, zunehmend mit staatlichen und anderen privaten Organisationen interagieren. So verpflichten sich Unternehmen beispielsweise gegenüber Nicht-Regierungsorganisationen zur Einhaltung bestimmter Ziele des Gemeinwohls.

1 Wie Benz (2004: 25) herausarbeitet, dient diese Koordinierung in der Regel dem Management von Interdependenzen und erfolgt mittels bestimmter Regelsysteme.

2 Beispielsweise haben Arbeiten zur neuen Institutionenökonomik (siehe zum Beispiel: Williamson, 1999) aufgezeigt, dass die erfolgreiche Interaktion privater Akteure oftmals staatliche Regelsetzung erfordert und Arbeiten zur Global Governance (siehe beispielsweise Beisheim et al., 2011) haben aufgezeigt, dass für erfolgreiches staatliches Handeln oftmals die Beteiligung privater Akteure notwendig ist.

Zum zweiten wird mit dem Begriff Governance – in Abgrenzung zu Begriffen wie „Government“ und „Management“ – angezeigt, dass gesellschaftliche Koordinierung und Regelsetzung in vielen Fällen nicht (mehr) allein hierarchische Formen annimmt, sondern auch wettbewerbliche oder kooperative Formen der Interaktion umfasst.

Zusammenfassend lässt sich sagen, dass ein wichtiger Beitrag der Governance-Forschung insbesondere darin liegt, dass sie die Vielfalt der Akteure und die Formen der Koordination und Steuerung in vielen gesellschaftlichen Teilbereichen aufgezeigt und analysiert hat. Das Konzept eignet sich somit besonders zur Analyse der Interaktion und Koordination im weitläufigen Kontext der Datenwirtschaft und insbesondere im vielfältigen Kontext der Datenräume.

2.3 Datenraum-Governance

Führt man die obigen Ansätze der Begriffsbestimmung nun zusammen, lässt sich Datenraum-Governance als Koordinierung jener Akteure betrachten, die am Geschehen in einem Datenraum (also einer föderierten Infrastruktur des Datenaustauschs) beteiligt oder von dieser (potenziell) betroffen sind.

Als Begriffskombination bietet sich „Datenraum-Governance“ gegenüber denkbaren Alternativen wie „Datenraum-Management“ oder “Steuerung von Datenräumen” an.

Am Begriff Datenraum-Management etwa ließe sich kritisieren, dass dieser eher eine Koordination innerhalb von Organisationsgrenzen und bezogen auf ökonomische Prozesse nahelegen würde. Verloren ginge somit das Verständnis, dass Koordinationsprozesse in Datenräumen in der Regel verschiedene Organisationen umfassen – darunter oftmals sowohl staatliche als auch private Organisationen. Weniger deutlich würde zudem, dass Governance sich nicht nur auf ökonomische Werte, sondern darüber hinaus und damit verbunden auch auf weitere gesellschaftliche Werte beziehen kann.

Beide Begriffe („Management“ sowie „Steuerung“) würden außerdem eine hierarchische Form der Koordinierung nahelegen. Mit der Verwendung dieser Begriffe würde daher nicht ausreichend deutlich, dass bei der Gestaltung eines Datenraumes eine Vielzahl von Akteuren zu beteiligen sind, die nicht unbedingt in hierarchischer Beziehung stehen, und dass eine

Koordination in Form von Kooperation oder Wettbewerb oftmals besser geeignet ist als ein Top-Down-Ansatz.

Das Konzept Datenraum-Governance erlaubt also in besonderem Maße, sich der Komplexität von Datenräumen zu stellen und ein Verständnis zu entwickeln, das zur Gestaltung von Datenräumen hilfreich oder notwendig ist. Dabei gilt es, die komplexe Realität schrittweise zu erschließen, etwa indem wie in den folgenden Abschnitten bestimmte Aspekte der Governance von Datenräumen (in diesem Fall Akteure, Strukturen und Phasen) unterschieden und beleuchtet werden.

3. Akteure der Datenraum-Governance

Der föderierte Aufbau von Datenräumen[3] bietet viele Vorteile gegenüber zentralisierten Formen datenökonomischer Aktivität. So wird es durch den dezentralen Aufbau leichter, verschiedene Akteure einzubinden, da nicht alle Rollen von der Gewinnung über die Verarbeitung bis zur Anwendung von Daten von einem zentralen Akteur ausgefüllt werden, sondern diese offen sind für weitere Akteure. Dies wiederum kann hilfreich sein, um Wettbewerb und Kooperation zu fördern, was sich letztlich positiv auf Wertschöpfung, Innovation und Souveränität auswirken kann. So sind Nutzende bei der Teilnahme an einem Datenraum anders als bei der Teilnahme an bestimmten Plattformen nicht gezwungen, für eine Teilnahme unvorteilhafte Nutzungsbedingungen zu akzeptieren. Der Zugang ist vielmehr offen gestaltet. Nutzende können zwischen Anbietern wählen und sich für jene entscheiden, deren Bedingungen am meisten den eigenen Anforderungen entsprechen – beispielsweise in Bezug auf Datensicherheit. Zum Beispiel könnte ein Anbieter von Bildungsangeboten, der eigene Bildungsdaten analysieren lassen möchte, einem Bildungs-Datenraum beitreten und in diesem z.B. KI-Anbieter finden, die den eigenen Anforderungen an Datensicherheit entsprechen – zum Beispiel dank verlässlicher Anonymisierung und zeitlich beschränkter Datenhaltung auf europäischen Servern. Des Weiteren könnten sich Organisationen mit entsprechenden Kapazitäten auch am Betrieb des Datenraums beteiligen. Beispielsweise könnte ein öffentlicher Träger einen Katalog von Angeboten des Datenraumes betreiben, in dem besonders relevante Angebote für staatliche Bildungseinrichtungen gelistet werden.

3 Siehe die hier zugrundeliegende Definition des Begriffs „Datenraum“ in Abschnitt 2.1.

Mit dem beschriebenen dezentralen Aufbau ist jedoch auch die Tatsache verbunden, dass sich eine Vielzahl unterschiedlicher Akteure koordinieren müssen, wobei dies in unterschiedlicher Form und Intensität geschehen kann beziehungsweise geschehen sollte. Datenraum-Governance ist daher von Vielfalt und Komplexität geprägt.

Um diese konzeptuell greifbar zu machen, lohnt es sich, zunächst zwei Gruppen von Akteuren eines Datenraumes zu unterscheiden[4]: Jene der Teilnehmenden des Datenaustauschs und jene der Betreiber eines Datenraumes oder Föderatoren.

3.1 Teilnehmende

Teilnehmende eines Datenraumes sind jene Organisationen und Personen, die die Funktion des Datenraums nutzen und Angebote im Datenraum anbieten oder nachfragen. Im Falle von Gaia-X sind die Anbieter und Nachfrager von Angeboten in einem Gaia-X-Datenraum als solche zu betrachten. Angebote können Daten sowie datenbezogene oder infrastrukturbezogene Dienste sein. Einige Beispiele für Angebote aus dem Kontext von Gaia-X bietet Tab. 1.

Die Rolle der Teilnehmenden kann von unterschiedlichsten Akteuren eingenommen werden. Dies können Organisationen mit oder ohne Gewinnerzielungsabsicht sein, kleine oder große Organisationen, staatliche und nicht-staatliche Organisationen. Darüber hinaus können prinzipiell auch Einzelpersonen Teilnehmende eines Datenraumes sein.

In den meisten aktuellen Initiativen zum Aufbau von Datenräumen liegt der Fokus in größerem Maß auf Organisationen, darunter insbesondere privaten Unternehmen, die kommerziell beziehungsweise für ihre geschäftlichen Zwecke Daten oder datenbezogene Dienste anbieten oder nachfragen. In geringerem Maß werden weitere Akteure adressiert. Die beiden Beispiele Catena-X und Mobility Data Space verdeutlichen dies: Im Falle von Catena-X werden insbesondere Unternehmen aus den Wertschöpfungsketten der Automobilherstellung adressiert, angefangen bei der Rohstoffgewin-

4 Diese Einteilung von Akteursgruppen ist nur eine von vielen denkbaren Einteilungen. Sie bietet sich insbesondere für die Ebene des Datenraums an. Als weitere Ebenen lassen sich die Ebene der Föderation und die Ebene des Orchestrators unterscheiden (siehe Abschnitt vier), für die gegebenenfalls alternative Einteilungen sinnvoll sind. Zum Zweck der Übersicht wird in diesem Abschnitt der Fokus auf die Ebene des Datenraums beschränkt.

Service Offering	Beispiel
Cloud Service	Infrastructure as a Service, Platform as a Service, Software as a Service
Data Set	data sharing in batch, stream and event driven
Software Licence	perpetual or renewable licenses for a product without an associated online service
Interconnection & Networking Service	services that can go beyond the capacities of the regular Internet connection and exhibit special characteristics, such as and not limited to bandwidth, latency, availability or security-related settings

Tabelle 1: Service Offerings in Gaia-X. Quelle: Gaia-X AISBL 2022a, S. 54

nung über die Herstellung von Komponenten, bis zur Fahrzeugherstellung und dem Vertrieb und schließlich der Demontage und dem Recycling. Daneben sind in geringerem Maße auch Unternehmen aus anderen Bereichen (zum Beispiel Softwareentwicklung) sowie Forschungseinrichtungen und Behörden eingebunden.

Im Falle des Mobility Data Space werden insbesondere Unternehmen angesprochen, die direkt oder indirekt im Bereich Verkehr aktiv sind, darunter Unternehmen des Verkehrs auf Straßen, Schienen und Wasserwegen. Dies schließt unter anderem Unternehmen aus Produktion (wie Automobilhersteller), Dienstleistung (wie Logistikunternehmen) und Digitalwirtschaft (wie Softwareentwicklung) ein. Darüber hinaus sind auch Akteure aus anderen Sektoren (wie Versicherungsunternehmen) sowie Forschung und Verwaltung am MDS beteiligt.

Um Teil eines Datenraums zu werden, müssen bestimmte Anforderungen, insbesondere technischer und rechtlicher Art, erfüllt sein. Diese setzen sich meist aus föderations- sowie datenraumweiten Vorgaben zusammen.

Beispielsweise müssen Teilnehmende von Gaia-X bestimmte Selbstbeschreibungen von sich und ihren Diensten erstellen. Zum Beispiel ist für jedes Angebot in einem Gaia-X-Datenraum anzugeben, von welchem Anbieter es stammt und wo die Nutzungsbedingungen einzusehen sind. Für Teilnehmende von MDS und Catena-X sind weitere Selbstbeschreibungen vorgegeben.

Solche Vorgaben für Teilnehmende bestimmter Datenräume sind meist in Verträgen zur Teilnehmerschaft geregelt, die Rechte und Pflichten der Beteiligten, darunter insbesondere Preise für grundlegende Dienste, regeln.

Generell muss darüber hinaus kompatible Software unter anderem für den Datenaustausch verwendet werden. Im Falle von Gaia-X kann beispielsweise der Eclipse Data Space Connector (EDC) genutzt werden, um sich mit dem Datenraum zu verbinden. Sowohl bei Catena-X als auch beim MDS ist es möglich, den Konnektor eigenständig zu installieren oder externe Anbieter im Sinne eines Connector as a Service in Anspruch zu nehmen.

Für die Ausgestaltung der Vorgaben für Teilnehmende ist auch die zweite Gruppe von Akteuren relevant: die Föderatoren von Datenräumen.

3.2 Föderatoren

Aufgabe der Föderatoren ist es, die Dienste zu erbringen, die für den Betrieb eines Datenraum unerlässlich sind. Dazu zählen bei Gaia-X z.B. Föderationsdienste zum Identitätsmanagement, zur sicheren Datenübertragung und zum Labelling. Diese Dienste ermöglichen, dass Daten und datenbezogene Dienste im Datenraum angeboten und nachgefragt werden können.

Je nach Konzeption des jeweiligen Datenraumes variiert die Anzahl der Föderatoren und ihr Aufgabenbereich. Zum Beispiel ist es prinzipiell möglich, dass fast alle basalen Dienste gemeinsam von einer Vielzahl von Föderatoren bereitgestellt werden. In diesem Fall wäre der Betrieb des Datenraumes weitgehend dezentralisiert. In aktuellen Projekten wird hingegen ein Teil der basalen Dienste von einem einzelnen Föderator erbracht. Der Betrieb ist also zu einem gewissen Grad zentralisiert. Für eine graduelle Zentralisierung kann es unterschiedliche Gründe geben. Beispielsweise kann es sinnvoll sein, zwischen eher kritischen und eher unkritischen Diensten zu unterscheiden und für Betreiber ersterer höhere und Betreiber letzterer niedrigere sicherheitsbezogene Anforderungen zu stellen.

So werden kritische Dienste des Catena-X-Datenraums, zum Beispiel für das Identitätsmanagement, allein durch den aktuell für diesen Zweck mandatierten Betreiber Cofinity-X angeboten. Andere Dienste, beispielsweise Dienste zur Listung von Angeboten des Catena-X-Datenraums und zum Matching von Angebot und Nachfrage, können von verschiedenen Anbietern erbracht werden.

Bei der Mandatierung und Aufsicht wichtiger Betreiber und allgemeiner bei der Koordinierung der Akteure des Datenraums nimmt in vielen Projekten eine einzelne Organisation, die speziell für diesen Zweck gegründet wurde, eine zentrale Rolle ein. Diese fungiert im Sinne eines Orchestrators, insofern als sie das harmonische Zusammenspiel der Akteure gewährleistet[5]. Im Falle des MDS agiert als ein solcher Orchestrator die DRM Datenraum Mobilität GmbH, im Falle von Catena-X der sogenannte Catena-X Automotive Network e.V.

Ob ein solcher Orchestrator gegeben ist, wie dieser verfasst ist und wie sein Verhältnis zu den Föderatoren geregelt ist, ist für die Governance des Datenraumes von wesentlicher Bedeutung. Im Falle des MDS und Catena-X werden wichtige Festlegungen zum Aufbau des Orchestrators mittels Gesellschaftsvertrag beziehungsweise Satzung und Einzelheiten des Verhältnisses zwischen Orchestrator und Föderatoren insbesondere mittels Kooperations- und Dienstleistungsverträgen geregelt. Die in solchen Dokumenten festgeschriebenen Regelungen haben großen Einfluss auf die Interessen und Handlungsspielräume der Föderatoren.

Beispielsweise wird es in der Regel als sinnvoll erachtet, dass für den Orchestrator Neutralitätsverpflichtungen gelten. Dies kann etwa bedeuten, dass für diesen eine Gewinnerzielungsabsicht ausgeschlossen wird. Im Falle von Catena-X handelt es sich um einen Verein, der nicht auf einen wirtschaftlichen Geschäftsbetrieb ausgerichtet ist und für den folglich die Gewinnerzielung als Hauptzweck ausgeschlossen ist. Im Falle des MDS, einer GmbH, wurde ebenfalls die Gewinnerzielung als Zweck in der Satzung ausgeschlossen.

Festzuhalten bleibt, dass Grundlage eines jeden Datenraums ein effektives Zusammenwirken der verschiedenen Akteure ist. Die Funktion der Föderatoren in diesem Kontext ist es, die Grundlage der Interaktion der Teilnehmenden bereitzustellen. Die Teilnehmenden nutzen diese Grundlagen, um zu interagieren, indem sie Daten oder datenbezogene Dienste anbieten oder nutzen.

---

5 Orchestrierung wird hier in Anlehnung an (Abbott et al. 2015) als eine Governance-Form verstanden, durch die ein einzelner Akteur weitere relevante Akteure auf freiwilliger Basis zur Verfolgung eines gemeinsamen Ziels zusammenbringt („enlisted"). Die Koordinierung erfolgt dabei vergleichsweise indirekt und in der Regel ohne harte Sanktionen. Es gilt dabei sicherzustellen, dass die Akteure sowohl ihre spezifischen Fähigkeiten nutzen können als auch harmonisch zusammenwirken – ähnlich dem gemeinsamen Spiel eines Orchesters.

Dieses Zusammenwirken der Akteure lässt sich nur sicherzustellen, wenn die Akteure entsprechende Anreize und Handlungsmöglichkeiten haben. Diese werden wesentlich durch entsprechende Governance-Strukturen geprägt.

4. Strukturen der Datenraum-Governance

Je nachdem wie weit der Begriff gefasst wird, kommen als Strukturen eines Datenraums unterschiedliche Aspekte in Betracht, die Regelsystemen gleichkommen, also die Interessen und Handlungsoptionen der Akteure eines Datenraums dauerhaft mitbestimmen. Im Folgenden werden beispielhaft einige der wichtigsten rechtlichen und technischen Regelsysteme von Datenräumen als Strukturen berücksichtigt. Dabei werden drei Ebenen unterschieden: die der Datenraum-Initiative, die des Datenraums und die der Orchestratoren.

4.1 Ebene der Datenraum-Initiativen (hier Gaia-X)

Ein Grundprinzip von Datenräumen ist, dass diese als Föderationen verfasst sind, also ein Mindestmaß an Interoperabilität aufweisen müssen. So soll es beispielsweise möglich sein, dass Teilnehmende eines Datenraums der Luft- und Raumfahrt bei Bedarf Daten mit Teilnehmenden eines Datenraums für den marinen Bereich austauschen können. Derzeit gibt es mehrere Initiativen, die Grundlagen für Interoperabilität in Form von Vereinbarungen, Standards und *Software Stacks* entwickeln und so den Aufbau einer Föderation von Datenräumen vorantreiben. Darunter zu nennen sind insbesondere die Initiative der International Data Spaces Association (IDSA) sowie Gaia-X. Die IDSA dient der Weiterentwicklung und Anwendung des IDS-Referenz-Architekturmodells, dessen Entwicklung 2015 mit einem durch das Bundesministerium für Bildung und Forschung (BMBF) geförderten und von 16 Fraunhofer Instituten umgesetzten Forschungsprojekts begonnen hat und derzeit insbesondere vom International Data Spaces Association e.V. fortgeführt wird. Gaia-X dient wiederum der Weiterentwicklung und Anwendung des Gaia-X-Referenzrahmens und des dazugehörigen Governance-Arrangements und wurde 2019 auf Initiative der deutschen sowie der französischen Regierung mit zahlreichen Industriepartnern ins Leben gerufen. Derzeit wird das Projekt insbesondere durch die Gaia-X

Association vorangetrieben, die mittlerweile über 300 Mitgliedsorganisationen hat, darunter private non-profit und for-profit Organisationen sowie öffentliche Einrichtungen.

Die Initiativen der IDS und die Initiative Gaia-X ergänzen sich im Wesentlichen, wobei IDS insbesondere im Bereich des Datentransfers und Gaia-X insbesondere im Bereich der Vertrauenssicherung Maßstäbe setzt (Otto 2023, S. 19). Mit beiden Initiativen wurden auch umfassende Governance-Strukturen geschaffen, die bestimmen, wie die Interessen zur Weiterentwicklung der Referenzrahmen gebündelt und in Ausgleich gebracht werden. Im Folgenden wird exemplarisch auf die Strukturen von Gaia-X eingegangen.

Als Beispiel für eine wichtige Struktur von Gaia-X ist zunächst die Gaia-X Association zu nennen, deren Aufbau in Abbildung 1 dargestellt ist. Diese wurde als internationale Vereinigung ohne Gewinnerzielungsabsicht nach belgischem Recht geschaffen (*association internationale sans but lucratif* – AISBL). Zu ihren Aufgaben gehören zum einen die Vertretung der Gaia-X-Initiative nach außen – insbesondere gegenüber anderen Datenrauminitiativen – und zum anderen Koordinationsaufgaben nach innen. Zu letzteren zählt insbesondere die Organisation der Gremien, in denen die Weiterentwicklung des Gaia-X-Rahmenwerks vorangetrieben wird. Dies sind insbesondere drei sogenannte Comittees (Policy Rules Committee, Data Spaces Business Committee, Technical Committee) sowie eine Reihe von Arbeitsgruppen, die den Comitees zugeordnet sind. Die Ergebnisse der Arbeit der Comitees, die Bestandteile des Gaia-X-Rahmenwerks, finden sich in zentralen Dokumenten wie dem Architecture Document (Gaia-X AISBL 2022a) wieder.

Eine weitere wichtige Struktur von Gaia-X stellen die nationalen Gaia-X-Hubs dar. Zu den Aufgaben der Hubs zählen insbesondere Koordination und Wissenstransfer auf der nationalen Ebene. Die Hubs führen neue Mitglieder in die Gaia-X-Gemeinschaft ein, vernetzen laufende Projekte zur Anwendung des Gaia-X-Rahmenwerks und kümmern sich um die Dokumentation und Verbreitung grundlegender Erkenntnisse und praktischer Erfahrungen aller Akteure der Gaia-X-Gemeinschaft. Realisiert werden diese Tätigkeiten in sogenannten Domänen, die bestimmte Gesellschaftsbereiche und Branchen widerspiegeln, etwa den öffentlichen Sektor, den Gesundheitsbereich und den Mobilitätsbereich.

Eine handlungsleitende und koordinierende Funktion kommt neben den genannten Institutionen außerdem den technischen Rahmenwerken selbst zu. Beispielsweise ist hier das Trust-Framework von Gaia-X zu nennen.

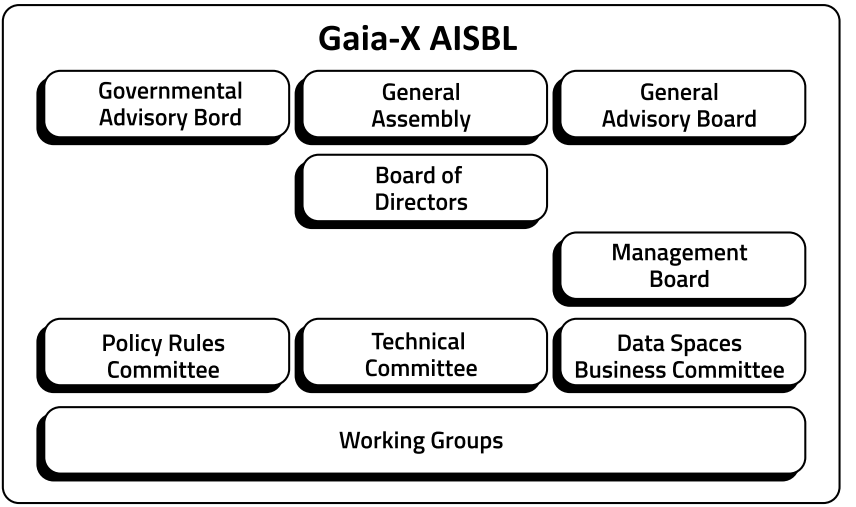

Abbildung 1 Aufbau der Gaia-X AISBL. Quelle: Eigene Darstellung auf Grundlage von (Gaia-X AISBL 2024).

Entsprechend diesem werden Grundlagen zur Erstellung sogenannter Labels definiert, mit denen beispielsweise bestätigt wird, dass einzelne Teilnehmende oder Angebote innerhalb eines Gaia-X-Datenraums bestimmte Anforderungen erfüllen.

Solche Anforderungen können grundlegende Voraussetzungen zur Teilnahme an Gaia-X oder einzelnen Datenräumen sein. Ein Beispiel für erstere sind etwa die drei grundlegenden Labels (Level 1 bis Level 3) die Teilnehmende erhalten können, die bestimmte allgemeine Kriterien in Bezug auf Transparenz, Datenschutz, Datensicherheit, Portabilität und Standort erfüllen. Ein Beispiel für letztere sind die Catena-X-Labels, die Angebote und Anbieter erhalten können, die entsprechende Vorgaben des Catena-X-Datenraums einhalten. So zum Beispiel ein Anbieter, der für Lieferketten in der Automobilbranche Dienste zur Nachverfolgbarkeit einzelner Komponenten von der Produktion bis zum Recycling anbietet und entsprechende Vorgaben zu Datensouveränität und Interoperabilität aus der Catena-X-Domäne „Nachverfolgbarkeit" erfüllt.

Technisch realisiert werden die Labels zusammen mit den Selbstbeschreibungen der Teilnehmenden als *Verifiable Credentials*. Da diese maschinenlesbar sind, ist auch eine Berücksichtigung der Labels bei Abschluss und Umsetzung von Smart Contracts möglich. Beispielsweise lässt sich so

festlegen, dass in bestimmten Bereichen (etwa beim Austausch personenbezogener Daten) oder für eine bestimmte Transaktion (die beispielsweise Geschäftsgeheimnisse beinhaltet) nur Anbieter oder Angebote in Frage kommen, die eine bestimmte Zertifizierung vorweisen oder innerhalb eines bestimmten Staatsgebiets beheimatet sind.

Wer Labels definieren kann und wer Labels, nach einer Überprüfung anhand der entsprechenden Kriterien vergeben darf, wird im Gaia-X Trust Framework (Gaia-X AISBL 2022b) festgelegt. Dabei gilt für einige Labels (insbesondere die grundlegenden Labels zur Gaia-X-Konformität), dass die Definition und Vergabe durch sogenannte Gaia-X Digital Clearing Houses (GXDCH) erfolgt. Weitere Labels können von den Betreibern und Teilnehmern eines Gaia-X-Datenraumes geschaffen werden. Den Teilnehmenden ermöglichen die Labels sowie das Trust-Framework im Ganzen ein hohes Maß an Souveränität, insofern sie festlegen können, unter welchen Bedingungen (bezogen etwa auf Umfang, Dauer, Gegenleistungen etc.) sie mit wem in Austausch treten.

Wie anhand dieser Beispiele deutlich werden dürfte, bestehen bereits bei den Strukturen auf Ebene der Datenraum-Initiativen verschiedene Mitwirkungsmöglichkeiten. Um eine dieser Möglichkeiten zu nutzen, bietet es sich an, zunächst das Onboarding durch den jeweils zuständigen Gaia-X Hub zu durchlaufen. Darüber hinaus kann eine Mitgliedschaft und Mitwirkung im Rahmen der AISBL sinnvoll sein.

4.2 Ebene der Datenräume

Wie im vorangegangenen Abschnitt erläutert, werden viele grundlegende Regeln für Datenräume bereits auf der Ebene der Föderation, also durch die jeweilige Datenrauminitiative gemacht. Dennoch verbleibt ein großer Gestaltungsspielraum auf der Ebene der einzelnen Datenräume. Dies ermöglicht für bestimmte Datenräume – die meist für einen einzelnen Gesellschaftsbereich oder eine Branche bestimmt sind – spezifische Vereinbarungen zu treffen. So können bestimmten Anforderungen, beispielsweise Anforderungen der Teilnehmenden oder Anforderungen externer Regulierer, bereits durch die Gestaltung des Datenraums selbst, also der betreffenden Infrastruktur des Datenökosystems, entsprochen werden. Welche Strukturen die Gestaltung, den Betrieb und die Nutzung des Datenraums ermöglichen, lässt sich mit Bezug zu den Ähnlichkeiten und Unterschieden der Strukturen der Datenräume MDS und Catena-X deutlicher machen.

Ähnlich ist in beiden Projekten zunächst, dass sich die geschaffenen Strukturen grob drei Funktionsbereichen zuordnen lassen: Generelle Koordinationsaufgaben verbleiben bei einer einzelnen Organisation, die als Orchestrator fungiert, während Aufgaben des technischen Betriebs als auch der technischen Entwicklung zu großen Teilen ausgelagert werden. In Bezug auf die technische Entwicklung wird zunächst sichtbar, dass in beiden Initiativen in großem Maße auf Open-Source-Software gesetzt wird. Dies hat den Vorteil, dass die Entwicklung und Überprüfung der grundlegenden Technik offen gestaltet ist und somit Lock-In-Situationen und Sicherheitslücken leichter vermieden werden können.

Um die initiale Softwareentwicklung voranzutreiben, wurde im Falle von Catena-X das Projekt Tractus-X ins Leben gerufen (Eclipse Foundation 2024). Das Projekt wird im Rahmen der Eclipse Foundation von einer Reihe von Unternehmen vorangetrieben, die Mitglieder sowohl der Eclipse Foundation als auch des Catena-X-Vereins sind. Ziel des Projektes ist, Referenzimplementierungen für das Catena-X-Rahmenwerk zu schaffen.

In Zukunft soll die Entwicklungstätigkeit noch weiter geöffnet werden. So soll jedes Mitglied von Catena-X Standards vorschlagen können. Die vorgeschlagenen Standards werden dann vom Catena-X-Verein geprüft. Im Anschluss kann der Standard dann im Betrieb genutzt werden. Das Zusammenspiel dieser Organe wird in Abbildung 2 veranschaulicht.

Im Falle des MDS wird hingegen stärker mit konkreten Aufträgen für Software-Entwicklung gearbeitet. In der Regel werden durch öffentliche Ausschreibungen geeignete Auftragnehmer für die Entwicklung gefunden. Dabei wird viel Augenmerk auf die Unabhängigkeit des Datenraumprojekts von einzelnen Auftragnehmern gelegt.

Im Bereich des technischen Betriebs setzen beide Projekte auf Dezentralisierung, die sich in ihrem Ausmaß von Dienst zu Dienst unterscheidet: Für einzelne Dienste bestehen minimale Anforderungen, beispielsweise die (technische) Anforderung, eine Referenzimplementierung zu nutzen. Solche Dienste können letztlich von fast allen Interessierten angeboten werden und sind daher praktisch gänzlich föderiert.

Für andere, insbesondere sensible Dienste bestehen hingegen hohe Anforderungen, darunter solche, die sich auf technische Systeme, und solche, die sich auf die Organisation beziehen, die das betreffende System betreibt. Diese Dienste werden mitunter nur von einem einzelnen Anbieter angeboten und sind somit weitgehend zentralisiert.

Im Bereich der Weiterentwicklung der Governance kommt in beiden Projekten dem Orchestrator eine zentrale Rolle zu. Dieser wirkt koordinie-

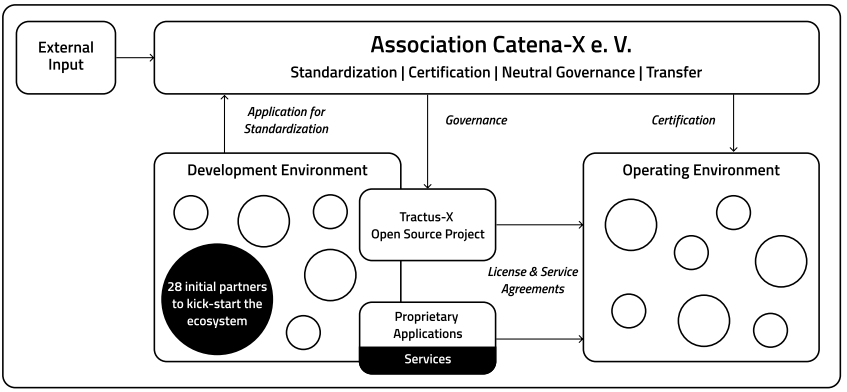

Abbildung 2 Governance-Strukturen des Catena-X-Datenraums. Quelle: (Catena-X Automotive Network e.V. 2022, S. 4)

rend unter anderem auf die technische Entwicklung und den technischen Betrieb ein. Im Falle des MDS erfolgt dies in erster Linie durch entsprechende Ausschreibungen und anschließende Aufträge. Im Falle von Catena-X erfolgt dies insbesondere durch einen Zertifizierungsprozess.

Hintergrund ist eine unterschiedliche Zusammensetzung der beiden Orchestratoren. Im Falle des MDS handelt es sich um eine Gesellschaft, die von der deutschen Akademie der Technikwissenschaften (acatech) als neutraler Instanz gegründet wurde. Bei der Catena-X Association handelt es sich um einen Verein, in dem die Mitgliedsunternehmen stärkeren Einfluss haben. Wie die Betreibergesellschaften aufgebaut sind, wird im nächsten Abschnitt näher erläutert.

Insgesamt lässt sich auch für die Ebene des Datenraumes festhalten, dass Interessierte viele Möglichkeiten haben, an der Regelsetzung zu partizipieren. Organisationen und Einzelpersonen können beispielsweise an der technischen Entwicklung des Datenraums – etwa als Teil der Open-Source-Gemeinschaft oder am technischen Betrieb als Föderator eines Dienstes für den Datenraum – mitwirken. Um den Einstieg zu erleichtern, werden in den Datenräumen in der Regel Onboarding-Dienste durch die Orchestratoren (im Falle MDS und Catena-X) oder unabhängige Dritte (im Falle Catena-X) angeboten, die eine gute erste Anlaufstelle für Interessierte sind.

4.3 Ebene der Orchestratoren

Nach den Strukturen auf Ebene der Föderation von Datenräumen und den Strukturen auf Ebene des einzelnen Datenraumes sollen im Folgenden die Binnenstrukturen der Orchestratoren eines Datenraumes erläutert werden. Als Orchestratoren werden dabei Organisationen betrachtet, die in der Governance eines Datenraumes eine hervorgehobene Bedeutung einnehmen. In vielen Projekten, darunter ~~dem~~ MDS und Catena-X, sind solche Orchestratoren zu finden. Diese sind zwar als eigenständige Organisationen verfasst, ihre Aufgabe liegt jedoch weniger darin, partikulare Interessen zu entwickeln und zu vertreten, sondern mehr darin, die Interessen aller relevanten Akteure eines Datenraumes zu bündeln und in Einklang bringen, um einen effektiven und effizienten Betrieb und Ausbau des Datenraumes zu gewährleisten. Für diesen Zweck ist der Orchestrator entsprechend auszugestalten, wobei die Ausgestaltung durchaus variieren kann.

Beispielsweise kann ein Orchestrator eine Aktiengesellschaft oder auch eine Genossenschaft sein. Besonders häufig ist der Orchestrator wie im Fall des MDS eine Gesellschaft mit beschränkter Haftung (GmbH) oder ein eingetragener Verein (e.V.), wie im Fall von Catena-X.

Betrachtet man die beiden Beispiele MDS und Catena-X genauer, zeigen sich trotz der unterschiedlichen Gesellschaftsformen viele Gemeinsamkeiten: So sind in beiden Fällen ein Leitungs-Organ (Vorstand / Geschäftsführung), eine Versammlung (der Gesellschafter beziehungsweise der Mitglieder), ein oder mehrere Aufsichts- beziehungsweise Beratungsgremien und mehrere Ausschüsse vorhanden. Erkennbar ist dies beispielsweise in Abbildung 3.

Im Falle von Catena-X liegen zentrale Entscheidungskompetenzen beim Vereinsvorstand und der vom Vorstand benannten Geschäftsführung, im Falle des MDS ist hier die Geschäftsführung der GmbH zu nennen. Die Geschäftsführungen sind insbesondere für die Vertretung der Organisation nach außen und das Tagesgeschäft zuständig und damit für die zentralen Entscheidungen zur Ausgestaltung des Datenraums, insbesondere die Abgrenzung der Teilnehmerschaft und die Ermöglichung ihrer Interaktionen.

Im Falle des MDS wird die Geschäftsführung vom Hauptgesellschafter acatech (> 50% Anteil) wahrgenommen, da acatech als neutrale Instanz selbst nicht an Wertschöpfungsprozessen des betreffenden Sektors beteiligt ist. Im Falle von Catena-X wird der Vereinsvorstand nach einem bestimmten Schlüssel aus Vertretern der Mitgliedsunternehmen zusammengesetzt. Dies soll sicherstellen, dass eine angemessene Repräsentation von Bran-

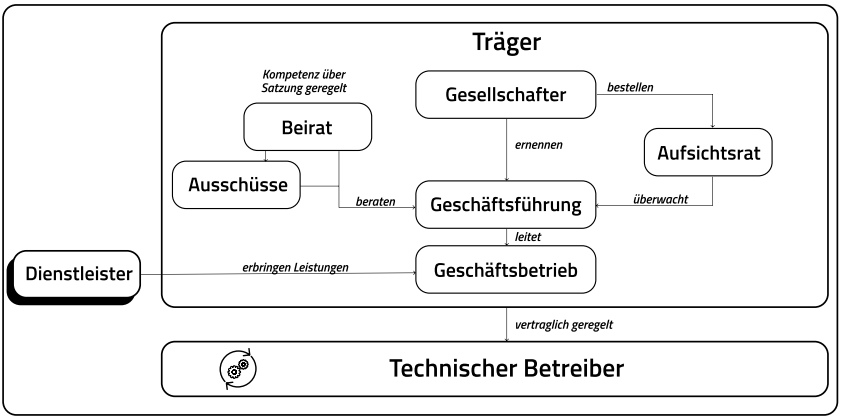

Abb. 3 Aufbau der Betreibergesellschaft des Mobility Data Space. Quelle: Datenraum MDS GmbH.

chen (OEMs, Zulieferer und Ausrüster) und Unternehmenstypen (KMUs sowie multinationale Unternehmen) gegeben ist. Wesentliche Arbeiten des Vorstands übernehmen zudem Arbeitskreise und Fachausschüsse, die der Vorstand einsetzt.

Das am weitesten gefasste Gremium und die basale Instanz zu Legitimierung der Entscheidungen der Gesellschaften stellen in beiden Fällen die Versammlungen dar – beim MDS die Versammlung der Gesellschafter und im Falle von Catena-X die Versammlung der Mitglieder. Sie kommen in regelmäßigen Abständen zusammen, um zentrale Entscheidungen zu treffen oder die Entscheidungen der Leitungsorgane gegebenenfalls zu bestätigen.

Bei Catena-X wählt die Mitgliederversammlung den Vorstand, der wiederum die Geschäftsführung benennt. Im Falle des MDS benennt die Gesellschafterversammlung direkt die Geschäftsführung.

Mitglieder sind im Falle von Catena-X die Mitgliedsorganisationen, wobei sich das Stimmrecht nach dem Typ der Organisation richtet. Stimmberechtigte ordentliche Mitglieder können nur Unternehmen der Automobilbranche sein. Andere Organisationen oder Einzelpersonen können außerordentliche Mitglieder ohne Stimmrecht werden.

Im Falle des MDS ist an dieser Stelle die Versammlung der Gesellschafter zu betrachten. Bei diesen handelt es sich neben acatech um Unternehmen aus dem Mobilitätsbereich (aus dem Bereich des Schienenverkehrs beispielsweise die Deutsche Bahn AG, aus der Logistik zum Beispiel die Deutsche Post DHL Group und aus der Automobilindustrie beispielsweise

die Volkswagen AG), aus anderen Sektoren (zum Beispiel die HUK-Coburg) sowie um die Länder Bayern, Baden-Württemberg und Nordrhein-Westfalen. Die Zahl der Stimmen in der Versammlung entspricht dabei dem Umfang der Gesellschaftsanteile.

Zur Beratung der Leitungsorgane wurde in beiden Fällen ein Beirat geschaffen. Die Mitglieder des Beirates von Catena-X werden je zur Hälfte von der Mitgliederversammlung und dem Vorstand benannt. Die Mitglieder des Beirates des MDS werden hingegen von der Gesellschafterversammlung benannt. In beiden Fällen handelt es sich um Experten des jeweiligen Gesellschaftsbereichs, darunter Mitglieder von Organisationen aus Wissenschaft, Politik und Verwaltung. Zu ihren Aufgaben gehört insbesondere die Unterstützung der Arbeit der Leitungsorgane durch ihre Expertise und die Mitwirkung am Austausch mit externen Organisationen.

Im Falle des MDS existiert der Aufsichtsrat als ein weiteres Organ, das die Leitungsorgane berät und diese zudem überwacht. Wie im Falle des Beirats werden die Mitglieder des Aufsichtsrats von der Gesellschafterversammlung benannt. Zu den Aufgaben des Aufsichtsrats zählt neben der Unterstützung der Arbeit der Geschäftsführung insbesondere die Prüfung der Arbeit der Geschäftsführung im Sinne der Gesellschafter.

Mit Blick auf die kurz dargestellten Gemeinsamkeiten und Unterschiede in der Binnenstruktur der beiden Organisationen lässt sich festhalten, dass ähnliche Ziele in unterschiedlichen Formen erreicht werden können. So wird sowohl beim MDS als auch bei Catena-X das Ziel verfolgt, einerseits eine Repräsentation der Interessen der Datenraum-Teilnehmenden sicherzustellen und zugleich ein Durchsetzen partikularer Interessen zu vermeiden. Beim MDS wird dazu insbesondere auf die Beteiligung der acatech als neutrale Instanz und im Fall von Catena-X auf eine differenzierte Beteiligung verschiedener Mitgliedsunternehmen gesetzt. Gleichzeitig wird das Ziel verfolgt, eine effiziente und sachgerechte Entscheidungsfindung sicherzustellen, indem eine dauerhafte Geschäftsführung eingesetzt und ein unterstützender Beirat beziehungsweise ein Beirat und ein Aufsichtsrat eingesetzt werden.

5 Phasen der Datenraum-Governance

Wie komplex die Governance von Datenräumen ist, zeigt sich bereits deutlich an den erläuterten Akteuren und Strukturen. Diese Komplexität macht auch den Aufbau von Datenräumen zu einem anspruchsvollen und in der

Regel langfristigen Unterfangen. Um die meist mehrjährige Entwicklung eines Datenraumes analytisch handhabbar zu machen, bietet es sich an, Entwicklungsphasen zu unterscheiden.

Im Folgenden werden drei solcher Phasen unterschieden, wobei auf Unterschiede in der Zusammensetzung der Akteure, den dominanten Interaktionsformen und den wichtigsten Ressourcenquellen eingegangen wird. Das denkbare Spektrum reicht dabei von einer mittleren bis zu einer hohen Anzahl von Akteuren, von einer kooperativen, über eine wettbewerbliche bis hin zu einer hierarchischen Interaktion und einer Finanzierung über öffentliche bis hin zu privaten Quellen.

5.1 Initiale Phase

Zur initialen Phase werden hier all jene Aktivitäten gezählt, die sich als Planungsarbeiten für den Datenraum verstehen lassen und noch nicht auf eine konkrete organisatorische oder technische Lösung abzielen.

In der Regel gilt es hier zunächst, eine Evaluation der Potentiale für den angedachten Datenraum vorzunehmen. Dabei sind zumindest die möglichen Teilnehmenden des Datenraums einzugrenzen und mögliche Interaktionen zwischen den Teilnehmenden zu identifizieren.

Beispielsweise war für den MDS und Catena-X zu klären, welche Akteure Interessen an einem Datenraum für Mobilität beziehungsweise einem Datenraum für Automobilproduktion haben und welche Anwendungsfälle sich für den Austausch von Daten und datenbezogenen Diensten entwickeln könnten.

Um dies zu klären, bietet es sich an, in der initialen Phase ein vergleichsweise breites Spektrum von Akteuren zu beteiligen, da so zunächst alle denkbaren Sichtweisen und Anforderungen gesammelt werden können, bevor anschließend eine Konkretisierung der Perspektiven und Anforderungen erfolgt. Als Kooperationsform bieten sich insbesondere niedrigschwellige kooperative Formen an, da so eine möglichst große Anzahl von Perspektiven berücksichtigt werden kann.

Im Falle von MDS und Catena-X zeigten sich bestehende Austauschformate wie die „konzertierte Aktion Mobilität“ und die „Plattform Industrie 4.0“ als wichtige Foren. In diesen konnten sich unter anderem Vertreter von Industrie, Forschung und Verwaltung über aktuelle Herausforderungen – beispielsweise Wandlungsprozesse in der Automobilindustrie – austau-

schen und Lösungsansätze, darunter die Realisierung offener und transparenter Datenräume thematisieren.

Zur Finanzierung der Arbeiten kommen wie in den übrigen Phasen private und staatliche Quellen sowie eine öffentlich-private Mischfinanzierung in Frage. Generell ist zu berücksichtigen, dass Datenräume zu einem relativ hohen Grad die Eigenschaften von öffentlichen Gütern aufweisen. So ist eine Ausschließbarkeit in der Nutzung bei Datenräumen insbesondere auch wegen der gesetzlichen Vorgaben, darunter zum Beispiel den Vorgaben des DGA zur Diskriminierungsfreiheit, und Vorgaben von Datenrauminitiativen, zum Beispiel zur Offenheit von Datenräumen in Gaia-X, kaum anzunehmen. Dies legt einen signifikanten Anteil staatlicher Finanzierung nahe. Auch für Zwecke der Sichtbarkeit und Repräsentation bietet sich eine staatliche Beteiligung an. Beides gilt insbesondere in der initialen Phase der Entwicklung eines Datenraums, da hier ein hoher Finanzbedarf besteht, während eine Refinanzierung in relativ weiter Ferne liegt. Zudem ist eine Vermittlung zwischen einer relativ hohen Anzahl von Akteuren notwendig. Derzeit ist die Bereitschaft für Förderung auch vielerorts gegeben, was sich sowohl auf der regionalen, der nationalen wie der europäischen und internationalen Ebene zeigt: so am Engagement von Bundesländern in einzelnen Gaia-X Projekten wie dem Mobility Data Space, am starken Engagement der Bundesregierung im Rahmen des Förderwettbewerbs "Innovative und praxisnahe Anwendungen und Datenräume im digitalen Ökosystem Gaia-X" sowie an Programmen der EU, wie dem „Digital Europe Programme“.

5.2 Aufbauphase

Unter der Aufbauphase versteht man den Zeitraum, der von der Entwicklung konkreter organisatorischer und technischer Lösungen bis zum Start des Regelbetriebs reicht. In dieser Phase gilt es, die vorher erfolgten Festlegungen zu Teilnehmenden des Datenraums und möglichen Interaktionsformen in konkrete technische Systeme und organisatorische Strukturen zu überführen, etwa in Form einer Referenzimplementierung und der Gründung einer Betreibergesellschaft und so weiter. Die Phase schließt auch die notwendigen Tests der Systeme und Strukturen vor Beginn des regulären Betriebs ein.

Im Vergleich zur initialen Phase ist das Akteursnetzwerk in der Aufbauphase in der Regel kleiner, zumindest in Bezug auf ein starkes Engagement.

Der Grund ist, dass in dieser Phase weniger die Einbeziehung einer möglichst großen Anzahl von Perspektiven, sondern eher die effektive Zusammenarbeit einer überschaubaren Anzahl von Beteiligten im Vordergrund steht. Dies legt auch nahe, dass hier neben kooperativen Formen der Interaktion (etwa zwischen Akteuren, die sich ergänzende Arbeitspakete erarbeiten) auch hierarchische Formen der Interaktion (etwa zwischen Akteuren, die die Leitungsaufgaben und Akteuren, die Teilaufgaben übernehmen) zum Tragen kommen. In vielen Projekten erfolgt der Aufbau eines Datenraums im Rahmen eines Konsortiums von Organisationen. Dabei sind häufig private Unternehmen und zugleich öffentliche Forschungseinrichtungen beteiligt.

Auch in dieser Phase ist eine Beteiligung sowohl privater als auch staatlicher Geldgeber oftmals sinnvoll. Privaten Geldgebern eröffnet sich die Möglichkeit, die Entwicklung von Geschäftsmodellen zu beginnen und Kompetenzen für die Realisierung eines Datenraumes aufzubauen, die sich später in Geschäftstätigkeit überführen lassen. Öffentliche Geldgeber können dabei einen Anreiz für eine schnelle Umsetzung setzen und auf diese gestaltend einwirken.

Im Falle des MDS erfolgte eine entsprechende staatliche Unterstützung durch die Bundesregierung im Rahmen des sogenannten MFund zur Entwicklung datenbasierter Geschäftsideen. In drei Forschungsprojekten wurden zunächst grundlegende Fragen zu Aufbau, Betrieb und Nutzung des Mobility Data Space behandelt und schließlich technische und organisatorische Lösungen konzipiert, bevor dann die Gründung der Betreibergesellschaft durch acatech erfolgte. Diese leistete dann die Operationalisierung des MDS bis hin zum Betriebsbeginn.

Catena-X wurde insbesondere im Rahmen des Konjunkturpakets „KoPa35" gefördert, mit dem die Bundesregierung den Transformationsprozess der Fahrzeughersteller und Zulieferindustrie unterstützte. Im Rahmen des Moduls für eine Modernisierung der Produktion erfolgte die Förderung des Konsortiums, aus dem heraus schließlich der Verein Catena-X Automotive Network gegründet und der Aufbau von der Entwicklung der technischen und organisatorischen Grundlagen bis hin zum Betriebsbeginn realisiert wurde.

5.3 Betriebsphase

Als Betriebsphase wird jener Zeitraum betrachtet, in dem Entwicklungsarbeiten soweit abgeschlossen sind, dass der Betrieb des Datenraums mit einer signifikanten Anzahl von Teilnehmenden beginnen kann. In dieser Phase gilt es hauptsächlich sicherzustellen, dass der Betrieb ohne größere Unterbrechungen und Zwischenfälle stattfindet.

Dabei wird die Anzahl der beteiligten Akteure so weit wie möglich erweitert, da dies den Nutzen des Datenraumes im Allgemeinen (auch für bestehende Akteure) erhöhen dürfte. Um dies bestmöglich umzusetzen, ist es sinnvoll, entsprechend einer Wachstumsstrategie vorzugehen. In den meisten Fällen wird es sinnvoll sein, zunächst eine Teilmenge der potenziellen Teilnehmenden und Anwendungen zu fokussieren und die Funktionalität des Datenraumes schrittweise zu erweitern. Sowohl im Falle von Catena-X als auch im Falle des MDS lag beispielsweise der Fokus zunächst auf Unternehmen mit Hauptsitz in Deutschland, während aktuell intensiv an der Internationalisierung, also der Gewinnung von Unternehmen mit Hauptsitz in der EU sowie in Drittstaaten, gelegt wird.

Des Weiteren wird aktuell bei Catena-X noch stärker als in der Anfangsphase Augenmerk auf kleine und mittlere Unternehmen anstelle der oftmals bereits als Teilnehmende gewonnen Großunternehmen und im Falle des MDS auf Unternehmen aus den Bereichen Schienenverkehr und Schiffsverkehr anstelle des weitgehend abgedeckten Bereichs des Individualverkehrs gelegt.

Neben den kooperativen und hierarchischen Interaktionsformen, die beispielsweise insbesondere zwischen und innerhalb von Betreibern des Datenraums bestehen dürften, sollten in dieser Phase des Datenraums zunehmend wettbewerbliche Formen der Interaktion treten. Grund dafür ist, dass hier (in der Regel sowohl bei den Teilnehmenden als auch zum Teil bei den Föderatoren) ein funktionierender Markt für Daten und Dienste entstehen sollte.

Die Finanzierung des Betriebs sollte zunehmend durch Erträge möglich sein, die sich aus dem Wert des etablierten Austauschs von Daten und datenbasierten Diensten ergeben. Eine staatliche Förderung wird hier insofern weniger notwendig sein und private Investitionen sollten zunehmen.

Bei Catena-X und dem MDS erfolgt dies beispielsweise in Form eines schrittweisen Wechsels bei der Finanzierung der Dienste des Datenraumes von einer rein auf Mitgliederbeiträgen (Catena-X) beziehungsweise Gesell-

schafter-Einlagen (MDS) basierenden Finanzierung hin zu einer Bepreisung entsprechend des Nutzungsumfangs.

6 Fazit

Im Rahmen aktueller Projekte erfolgt derzeit bereits die Gestaltung komplexer Governance-Arrangements für die Entwicklung, den Aufbau und den Betrieb von Datenräumen. Einige zentrale Fragen wurden in den vorangegangenen Abschnitten angesprochen: Welche Akteure können sich an Datenräumen beteiligen, welche Strukturen lassen sich für deren Zusammenwirken nutzen und in welchen Phasen kann ein Datenraum schließlich Gestalt annehmen?

Insgesamt sollte die Komplexität des Aufbaus von Datenräumen greifbar geworden sein. Diese Komplexität lässt sich als Fluch und Segen zugleich betrachten: Einerseits lässt sich das Konstrukt Datenraum in unterschiedlichster Form und somit spezifisch und besonders zweckdienlich für den jeweiligen Anwendungsbereich, beispielsweise eine bestimmte Branche, realisieren. Andererseits ist die Entwicklung spezifischer Lösungen, die mit entsprechenden Aufwänden verbunden ist, meist auch erforderlich.

Zwar lassen sich durchaus viele konkrete Projekte als Vorbilder nutzen. Die in diesem Beitrag angesprochenen Beispiele zeigen jedoch exemplarisch auf, dass sich ähnliche Ziele – etwa zur Neutralität von zentralen Akteuren – auf unterschiedlichen Wegen realisieren lassen. Es bleibt festzuhalten, dass für einen spezifischen Fall eine Vielzahl denkbarer Lösungen mit unterschiedlichen Vor- und Nachteilen anwendbar sein wird. So können bestimmte Beteiligungsstrukturen Vorteile hinsichtlich einer weiten Repräsentation, hingegen Nachteile für eine effektive Entscheidungsfindung zeigen. Die Realisierung eines Datenraums wird somit – in jeder Phase – mit schwierigen Entscheidungen verbunden bleiben. Daraus lässt sich schließen, dass eine weitere intensive Beschäftigung mit den verschiedenen Gestaltungsoptionen sowohl für wissenschaftliche Arbeiten zum Konzept Datenräume als auch für die praktische Umsetzung dieses Konzepts dringend geboten ist. Nur so lässt sich der vielfach bereits begonnene Aufbau von Datenräumen erfolgreich gestalten. Dies wiederum ist eine Voraussetzung, um die Vorteile, die dezentrale Datenräume gegenüber zentralisierten Infrastrukturen bieten, darunter ein Mehr an Souveränität, Sicherheit und Transparenz für die Teilnehmenden, zu realisieren.

Literatur

Abbott, Kenneth W., Philipp Genschel, Duncan Snidal, und Bernhard Zangl (Hrsg.) (2015): International Organizations as Orchestrators. Cambridge: Cambridge University Press.

Beisheim, Marianne, Tanja Börzel, Philipp Genschel, und Bernhard Zangl (Hrsg.) (2011): Wozu Staat? Governance in Räumen begrenzter und konsolidierter Staatlichkeit. Baden-Baden: Nomos.

Benz, Arthur (2004): Governance — Modebegriff oder nützliches sozialwissenschaftliches Konzept? In Governance — Regieren in komplexen Regelsystemen: Eine Einführung, Hrsg. Arthur Benz, 11–28. Wiesbaden: VS Verlag für Sozialwissenschaften.

Otto, Boris (2023): Data Sharing in Data Spaces. Konferenz: Data Sharing in Europe. Paris: Paris Dauphine-PSL University.

Catena-X Automotive Network eV. (2022): Catena-X Operating Model Whitepaper V2 abrufbar unter: https://catena-x.net/fileadmin/_online_media_/CX_Operating_Modelv2.1_final.pdf, Zugegriffen: 10.8.2023.

Eclipse Foundation (2024): Eclipse Tractus-X. Eclipse Tractus-X. abrufbar unter: https://projects.eclipse.org/projects/automotive.tractusx/who, Zugegriffen: 16.2.2024.

Gaia-X AISBL (Hrsg.): (2022a): Gaia-X Architecture Document abrufbar unter: https://www.gaiax.es/sites/default/files/2022-01/Gaia-X_Architecture_Document_2112.pdf, Zugegriffen: 19.1.2023.

Gaia-X AISBL (Hrsg.): (2022b): Gaia-X Trust Framework 22.04. abrufbar unter: https://gaia-x.eu/wp-content/uploads/2022/05/Gaia-X-Trust-Framework-22.04.pdf, Zugegriffen: 19.1.2024.

Gaia-X AISBL (2024): Who We Are. Gaia-X.eu. abrufbar unter: https://gaia-x.eu/who-we-are/association/, Zugegriffen: 15.1.2024.

Mayntz, Renate (1998): New Challenges To Governance Theory. Jean Monnet Chair Papers. Nr. 50. Florenz: European University Institute.

Reiberg, Abel, Crispin Niebel, und Peter Kraemer (2022): Was ist ein Datenraum? Definition des Konzeptes Datenraum.

Williamson, Oliver E. (1999): The Mechanisms of Governance. New York: Oxford University Press.

Wenn die Datengenossenschaft für mich einwilligt: Zum speziellen Datenvermittlungsdienst nach DGA

Paul C. Johannes, Maxi Nebel

Zusammenfassung

Der Data Governance Act (DGA) regelt unter anderem die Datengenossenschaften als Unterart der Datenvermittlungsdienste. Die Verordnung lässt offen, welche Rechtsform eine Datengenossenschaft nach DGA haben soll. Bereits vor Erlass des DGA haben sich Unternehmen mit dem Ziel, gemeinsam Daten zu poolen und zu verarbeiten, zu Datengenossenschaften im Sinne des Genossenschaftsgesetzes zusammengeschlossen. Der Beitrag stellt die Idee der Datengenossenschaft vor (1.) und stellt klar, dass diese innerhalb (2.) und außerhalb (3.) des DGA etabliert werden kann, sowohl als eingetragene Genossenschaft als auch in anderer Rechtsform. Dies wird an zwei Beispielen verdeutlicht (4.). Am Beispiel des DGA-Rechtsrahmens wird sodann erörtert, ob und wie eine Datengenossenschaft verbindliche Einwilligungen über die Daten ihrer Mitglieder abgeben kann (5.). Abschließend werden die sich aus den neuen Regeln ergebenden Vor- und Nachteile bewertet und in Bezug zum Risiko des Datenteilens gesetzt (6.).

1. Datengenossenschaft als Idee und im DGA

Die Idee der Genossenschaft beruht auf der Prämisse, dass durch den Zusammenschluss die Interessen der Mitglieder der Genossenschaft besser verwirklicht werden können. Die Mitglieder einer Genossenschaft bringen in der Regel ihre jeweiligen Stärken ein, agieren untereinander auf Augenhöhe und fördern auf diese Weise die Zwecke der Genossenschaft. Datengenossenschaften – als nach genossenschaftlichen Grundsätzen gegründete Zusammenschlüsse von Datenproduzenten oder Datenhaltern – ermöglichen einen selbstbestimmten Umgang mit der Ressource Daten. Eine Da-

tengenossenschaft kann auf unterschiedliche Weise gegründet werden und ist als solche nicht als einheitliches Rechtsmodell geregelt.[1]

1.1 Datenvermittlungsdienste nach DGA

Ein neuerer Bestandteil des europäischen Datenrechts[2] bemüht sich jedoch um die Regulierung von Datengenossenschaften, wenn auch nur rudimentär und mit spezialisierten Hauptzielen.

Der Data Governance Act (DGA) ist am 24. Juni 2022 in Kraft getreten.[3] Die Verordnung gilt vollumfänglich seit dem 24. September 2023. Der DGA zielt darauf ab, das Vertrauen in die gemeinsame Nutzung von Daten zu stärken. Er beinhaltet Regeln für Datenvermittlungsdienste und soll die Wiederverwendung bestimmter Daten im Besitz des öffentlichen Sektors erleichtern. Als Verordnung ist der DGA in den EU-Mitgliedstaaten unmittelbar anwendbar, ohne dass ein Durchführungsrechtsakt erforderlich ist.

Der DGA hat den Begriff „Datenvermittlungsdienste" eingeführt und legt einen Melde- und Aufsichtsrahmen für die Erbringung solcher Dienste fest. Art. 2 Nr. 11 DGA definiert einen Datenvermittlungsdienst als einen Dienst, der darauf abzielt, geschäftliche Beziehungen zum Zwecke der gemeinsamen Nutzung von Daten zwischen einer unbestimmten Zahl von betroffenen Personen und Dateninhabern einerseits und Datennutzern andererseits herzustellen.

Da diese grundsätzliche Definition sehr weit ist, wird sie vom DGA selbst eingeschränkt. Bestimmte Dienste sollen keine Datenvermittlungsdienste im Sinne des DGA sein. Dazu zählen

- Dienste, die Daten für einen Mehrwert und für Lizenzierungszwecke umwandeln oder zusammenfassen, aber keine kommerzielle Beziehung zwischen Dateninhabern und Datennutzern herstellen (Art. 2 Nr. 11 lit. a DGA),
- Dienste, die sich auf die Vermittlung von urheberrechtlich geschützten Inhalten konzentrieren (Art. 2 Nr. 11 lit. b DGA),

1 *Geminn/Johannes/Müller/Nebel* 2023, S. 21.

2 *Johannes*, ZD-Aktuell 2022, 01166; siehe auch *Geminn/Johannes* 2024 (in Vorbereitung).

3 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. L 152 S. 1, 2023 ABl. L 90204 S. 1, Celex-Nr. 3 2022 R 0868.

- Dienste, die ausschließlich von einem Dateninhaber oder einer geschlossenen Gruppe von Dateninhabern genutzt werden (privater Datenaustauschpool) (Art. 2 Nr. 11 lit. c DGA), und
- von öffentlichen Stellen angebotene Dienste zur gemeinsamen Nutzung von Daten, die nicht darauf abzielen, kommerzielle Beziehungen aufzubauen (Art. 2 Nr. 11 lit. d DGA).

Datenmakler, das heißt Unternehmen, die Daten von einer großen Anzahl von Unternehmen oder Personen kaufen, um sie zu verarbeiten und dann an andere Unternehmen zu verkaufen, werden also nicht als Datenvermittlungsdienste reguliert.[4] Ausgenommen sind damit auch Anbieter von Diensten zur gemeinsamen Nutzung von Online-Inhalten, die der Öffentlichkeit Zugang zu einer großen Menge urheberrechtlich geschützter Werke oder anderer geschützter Gegenstände verschaffen, die von ihren Nutzern hochgeladen werden, wie z. B. YouTube.[5] Das Gleiche gilt für geschlossene Datenplattformen, an denen sich nur eine vorher festgelegte Gruppe von Unternehmen beteiligen darf. Auch Plattformen, auf denen nur ein Unternehmen seine Daten mit anderen Unternehmen teilt, fallen nicht in den Geltungsbereich des DGA.[6]

Die gemeinsame Nutzung von Daten durch den Datenvermittlungsdienst kann durch technische, rechtliche oder andere Mittel erleichtert werden, auch zum Zweck der Ausübung der Rechte der betroffenen Personen in Bezug auf personenbezogene Daten. Datenvermittlungsdienste unterliegen im Allgemeinen einem Meldeverfahren nach Art. 11 DGA und bestimmten Bedingungen gemäß Art. 12 lit. a bis lit. o DGA, die erfüllt werden müssen, wie etwa die Einhaltung der Zweckbindung, das Kopplungsverbot oder spezifische Datenumgangsmaßnahmen. Sie werden von den zuständigen Aufsichtsbehörden gemäß Art. 14 DGA überwacht.

Artikel 10 lit. a bis c DGA nennt drei Arten von Datenvermittlungsdiensten, die den Bestimmungen in Kapitel III DGA unterliegen:

- Vermittlungsdienste zwischen Dateninhabern und potenziellen Datennutzern,
- Vermittlungsdienste zwischen betroffenen Personen, die ihre personenbezogenen Daten zur Verfügung stellen wollen, oder natürlichen Perso-

4 *Hennemann/Ditfurth*, NJW 2022, 1905 (1908).
5 Erwägungsgrund 29 DGA.
6 Erwägungsgrund 28 DGA.

nen, die nicht-personenbezogene Daten zur Verfügung stellen wollen, und potenziellen Datennutzern sowie
- Dienste von Datengenossenschaften.

1.2 Dienste von Datengenossenschaften nach DGA

Datengenossenschaften nach DGA sind folglich eine Unterart der Datenvermittlungsdienste. Dienste von Datengenossenschaften sind nach Art. 2 Nr. 15 DGA legaldefiniert als Organisationsstrukturen, „die von betroffenen Personen, Ein-Personen-Unternehmen oder KMU" (kleine und mittelständische Unternehmen) gebildet werden, die Mitglieder dieser Struktur sind. Ihr Hauptziel soll es sein, ihre Mitglieder bei der Ausübung ihrer Rechte in Bezug auf bestimmte Daten zu unterstützen. Dazu gehört nach der Legaldefinition

- die Unterstützung bei der Entscheidung in Kenntnis der Sachlage, bevor sie in die Datenverarbeitung einwilligen,
- der Meinungsaustausch über Datenverarbeitungszwecke und -bedingungen, die die Interessen der Mitglieder in Bezug auf ihre Daten am besten vertreten, und
- die Aushandlung von Bedingungen für die Datenverarbeitung im Namen der Mitglieder, bevor diese ihre Zustimmung zur Verarbeitung nicht personenbezogener Daten erteilen oder bevor sie in die Verarbeitung personenbezogener Daten einwilligen.

Nach Erwägungsgrund 31 DGA sollen Datengenossenschaften bestrebt sein,

- die Position von Einzelpersonen bei der sachkundigen Entscheidung vor der Einwilligung zur Datennutzung zu stärken,
- die Geschäftsbedingungen von Datennutzerorganisationen im Zusammenhang mit der Datennutzung in einer Weise zu beeinflussen, die den einzelnen Mitgliedern der Gruppe bessere Wahlmöglichkeiten bietet, oder
- mögliche Lösungen zu ermitteln, wenn einzelne Mitglieder einer Gruppe unterschiedliche Standpunkte zu der Frage vertreten, wie Daten verwendet werden können, wenn sich diese Daten auf mehrere betroffene Personen innerhalb dieser Gruppe beziehen.

Datengenossenschaften nach dem DGA können also als Organisationen beschrieben werden, die ihre Mitglieder – natürliche Personen oder Unternehmen – bei der Verwendung sowie dem Schutz ihrer Daten unterstützen. Beispiele hierfür sind, wenn einer Datengenossenschaft die Befugnis übertragen wird, die Bedingungen für eine Datenverarbeitung mit Datennutzerorganisationen auszuhandeln oder wenn diese eine Plattform für Austausch und Streitbeilegung unter den Mitgliedern bereitstellt.[7] Sie können auch für kleine und mittelständische Unternehmen nützlich sein, um deren Wissensstand zu verbessern, indem sie Zugang zu Datenbeständen anderer kleiner und mittelständischer Unternehmen erhalten.[8]

1.3 Daten als Vermittlungsgegenstand

Datenvermittlungsdienste und damit Datengenossenschaften sind nicht auf personenbezogene Daten beschränkt. Es können auch Daten ohne Personenbezug (und damit außerhalb des Geltungsbereichs des Datenschutzrechts) Vermittlungsobjekt einer Datengenossenschaft sein. Mögliche Anwendungsbereiche ergeben sich zum Beispiel im produzierenden Gewerbe und im Dienstleistungssektor, etwa im Bankwesen, im Kalibrierwesen, in der Logistik oder im Tourismus. Ein weiteres Beispiel ist die Nutzung von landwirtschaftlichen Daten.

1.4 Ziele von Datengenossenschaften

Dabei bietet die Datengenossenschaft auch Ansätze zur Förderung des Schutzes der Grundfreiheiten und -rechte betroffener Personen, insbesondere des Rechts auf informationelle Selbstbestimmung. Das Hauptziel von Datengenossenschaften besteht darin, ihre Mitglieder bei der Ausübung ihrer Rechte in Bezug auf bestimmte Daten zu unterstützen. Dazu gehören sowohl die Rechte der betroffenen Personen als auch die Rechte der Dateninhaber, zum Beispiel der Datenverarbeiter. Daher können Datengenossenschaften sowohl als Ansätze zur Wahrung der individuellen Rechte betroffener Personen ähnlich einer Art Tarifverhandlung als auch als Ansatz zur Zusammenlegung von Daten durch Dateninhaber zur Wahrung des lauteren Wettbewerbs und von Geschäftsinteressen betrachtet werden.

7 *Beise*, RDi 2021, 597 (602).
8 Erwägungsgrund 31 DGA.

Eine Datengenossenschaft könnte darauf abzielen, die Handlungsfähigkeit der betroffenen Personen und insbesondere die Kontrolle des Einzelnen über die ihn betreffenden Daten zu stärken. Sie könnte Einzelpersonen bei der Ausübung ihrer Rechte gemäß der Datenschutz-Grundverordnung (DSGVO) unterstützen, insbesondere in Bezug auf die Erteilung und den Widerruf ihrer Zustimmung zur Datenverarbeitung, das Recht auf Zugang zu ihren eigenen personenbezogenen Daten, das Recht auf Berichtigung unrichtiger personenbezogener Daten, das Recht auf Löschung oder das Recht „vergessen zu werden", das Recht auf Einschränkung der Verarbeitung und das Recht auf Datenübertragbarkeit, das es den betroffenen Personen ermöglicht, ihre personenbezogenen Daten von einem für die Datenverarbeitung Verantwortlichen zu einem anderen zu übertragen.

2. Datengenossenschaft außerhalb des DGA

Auch schon vor Verabschiedung des DGA haben sich Unternehmen in der Rechtsform der Genossenschaft zum gemeinsamen Verarbeiten und Vermarkten ihrer Daten zusammengeschlossen. Solche Arten von Datengenossenschaften haben den Zweck, Daten zu sammeln, zu verarbeiten und zu nutzen. Sie werden von ihren Mitgliedern gemeinschaftlich selbstverwaltet und demokratisch organisiert. Die Mitglieder sind zugleich Nutzer und Eigentümer der Daten und partizipieren an den Entscheidungen über deren Verwendung. Ziel einer Datengenossenschaft in diesem Sinne ist es, die Vorteile von Datenwirtschaft und Gemeinwohl zu vereinen, indem sie die demokratische Kontrolle und die Beteiligung der Nutzer an der Wertschöpfung gewährleistet.[9]

2.1 Genossenschaftsrecht

Das Genossenschaftsrecht ist ein Bestandteil des Gesellschaftsrechts. Die Idee der Genossenschaft ist der Zusammenschluss von Personen mit einer übereinstimmenden Wirtschaftsgesinnung. Das heißt, dass sich in einer Genossenschaft natürliche und / oder juristische Personen zusammenschließen, die ähnliche wirtschaftliche Ziele verfolgen und eine übereinstimmende wirtschaftliche Haltung haben.

9 Ausführlich *Knapp/Kobler/Richter* 2022, S. 443 ff.

Die eingetragene Genossenschaft ist in § 1 Genossenschaftsgesetz (GenG) definiert. Nach § 1 Abs. 1 GenG ist die eingetragene Genossenschaft eine Gesellschaft von nicht geschlossener Mitgliederzahl, welche die Förderung des Erwerbes oder der Wirtschaft ihrer Mitglieder mittels gemeinschaftlichen Geschäftsbetriebes bezweckt. Demnach werden der Genossenschaft drei Merkmale zugeschrieben: die nicht geschlossene Mitgliederzahl, der Förderzweck und der gemeinschaftliche Geschäftsbetrieb. Besonders an der Genossenschaft ist, dass die wirtschaftliche Förderung der Genossenschaftsmitglieder an erster Stelle steht und nicht das Gewinnstreben. Die Genossenschaft ist zwar nicht selbst der Geschäftsbetrieb, unterhält und betreibt diesen jedoch. Sind die Kriterien des § 1 GenG nicht erfüllt, muss eine andere Rechtsform gewählt werden.

In einer Genossenschaft gibt es Grundprinzipien, die zur Erreichung eines gemeinsamen Zieles beachtet werden müssen. Zum einen gibt es das Prinzip der Selbsthilfe. Die Mitglieder treten freiwillig einer Genossenschaft bei und wollen dadurch ökonomische, soziale und kulturelle Vorteile erhalten. Ein weiteres Prinzip ist das Prinzip der Selbstverantwortung, welches besagt, dass die Mitglieder für die Verbindlichkeiten der Genossenschaft haften. Das dritte Prinzip ist das Prinzip der Selbstverwaltung. Die jeweiligen Organe der Genossenschaft regeln alle wirtschaftlichen Angelegenheiten. Daneben gilt das Demokratieprinzip, welches besagt, dass jedes Mitglied nur eine Stimme hat und wichtige Entscheidungen in der Generalversammlung getroffen werden.

2.2 Datengenossenschaften eG

Datengenossenschaften im Sinne des Genossenschaftsrechts wurden ins Leben gerufen, da Künstliche Intelligenz immer präsenter und Datenanalysen immer relevanter werden. Kleinere und mittelständische Unternehmen haben finanziell nicht dieselben Möglichkeiten wie große Unternehmen. Um dieses Ungleichgewicht auszugleichen, sind Datengenossenschaften eine geeignete Lösung.[10]

Da es sich um die Rechtsform der Genossenschaft handelt, steht auch bei Datengenossenschaften der Förderzweck der Mitglieder und die Selbstverantwortung im Fokus. Das heißt, dass in einer Genossenschaft Personen

10 *Baars*, Was sind Datengenossenschaften? https://www.datengenossenschaft.com/was-sind-datengenossenschaften.

zusammenkommen, die gemeinsam ein Ziel erreichen wollen, was sie allein nicht erreichen könnten. Die Mitglieder von Datengenossenschaften sind gleichzeitig Eigentümer und Kunden ihrer Genossenschaft.

Ziel einer Datengenossenschaft ist es, einen gemeinsamen Datenraum zu erschaffen. Die Rechtsform der Genossenschaft ist dafür geeignet, da die Förderung der Mitglieder gemäß § 1 GenG im Vordergrund steht. Die Datengenossenschaft ermöglicht das Teilen von Informationen und die Datenverarbeitung und erleichtert die Kommunikation der Datengenossenschaftsmitglieder. Es ist allerdings auch möglich, weitere Partner, die nicht der Datengenossenschaft angehören, mit einzubeziehen, um dadurch das Angebot an Services zu erweitern.[11] Eingetragene Datengenossenschaften, die keine Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und Datennutzern andererseits herstellen, sind keine Datenvermittlungsdienste im Sinne von Art. 2 Nr. 11 lit. a DGA. Folglich sind Datengenossenschaften mit dem Ziel, Daten unter ihren Mitgliedern zu poolen oder zu teilen, keine Datengenossenschaften im Sinne des DGA. Dasselbe gilt für Genossenschaften, die einen Weiterverkauf von Daten im eigenen Namen betreiben.

3. Rechtsform von Datengenossenschaften nach DGA

Der DGA schreibt für Datenvermittlungsdienste keine bestimmte Rechtsform vor, verlangt aber, dass dieser Dienst über eine juristische Person bereitgestellt wird, die von den Dateninhabern oder betroffenen Personen getrennt ist. Auch für die Datengenossenschaft macht der DGA keine konkreten Vorgaben zur Rechtsform. Er überlässt dies den Möglichkeiten im Recht der Mitgliedsstaaten. Entscheidend nach DGA ist allein, dass sich die Mitglieder der Genossenschaft in einer Organisationsstruktur zusammenschließen.[12]

---

11 Wirtschaft Digital Baden-Württemberg, Forschungsprojekt Datengenossenschaften, https://www.wirtschaft-digital-bw.de/ki-made-in-bw/forschungsprojekt-datengenossenschaften.

12 Es erscheint daher ausgeschlossen, dass eine einfache Geschäftsbeziehung zwischen der betroffenen Person und der Datengenossenschaft, wie z. B. auch ein Dauerschuldverhältnis zu einer Dienstleistung, den Anforderungen von Art. 2 Nr. 15 DGA genügt; es bedarf einer inneren Verbindung des Mitglieds zur Genossenschaft, das mit organisationstypischen Rechten und Pflichten ausgestattet wird, *Keppler/Poncza*, in Paschke/Rücker 2024, Art. 2 DGA Rn. 74.

Datengenossenschaften nach DGA können in Deutschland als Genossenschaft nach deutschem oder europäischem Recht[13] gegründet werden. Dies liegt bereits begrifflich nahe.

Die idealen Ziele der Datengenossenschaft nach DGA passen auch zu den Zielen der Rechtsform Genossenschaft. Datengenossenschaften nach DGA können so eingerichtet werden, dass jedes einzelne Mitglied der Genossenschaft gleichzeitig Daten bereitstellt und im Gegenzug von den Daten profitiert, die die anderen Mitglieder bereitstellen. Sie können aber auch so betrieben werden, dass es möglich ist, Teil einer Datengenossenschaft zu sein, ohne ein Interesse daran zu haben, Daten von anderen Mitgliedern der Genossenschaft zu erhalten. Die Zwecke der Datennutzung werden innerhalb der Genossenschaft gemeinsam festgelegt, was sich auch entsprechend in der Satzung einer Genossenschaft als Zweck abbilden ließe.[14]

Aber obwohl der Begriff „data cooperative" in der deutschen Fassung des DGA wörtlich mit „Datengenossenschaft" übersetzt wird und das deutsche Recht die Gründung von Genossenschaften als juristische Personen zulässt, sind Datengenossenschaften in Deutschland nicht auf diese Rechtsform beschränkt.[15] Eine Datengenossenschaft könnte auch in einer anderen Gesellschaftsform gegründet werden. In Deutschland kämen sowohl Personengesellschaften wie die Partnerschaftsgesellschaft als auch Kapitalgesellschaften wie eine GmbH in Betracht. Denkbar ist aber auch die Gründung als Gesellschaft bürgerlichen Rechts. Bei all diesen könnten die Dateninhaber Anteile entsprechend ihrer Beteiligung halten. Die Dateninhaber, also betroffene Personen oder Kleinunternehmen, können dann selbst Eigentümer eines solchen Genossenschaft sein.

In Betracht kommt aber auch die Gründung einer Datengenossenschaft als eingetragener gemeinnütziger Verein im Sinne des Bürgerlichen Gesetzbuchs (BGB). Die datengenossenschaftliche Idealvorstellung nach Art. 2 Nr. 15 DGA könnte entsprechend in der Satzung eines gemeinnützigen Vereins als dessen Aufgaben festgelegt sein. Für eine Datengenossenschaft,

13 Mit der Verordnung (EG) Nr. 1435/2003 wurde die Rechtsform der Europäischen Genossenschaft (Societas Cooperativa Europaea - SCE) eingeführt; sie wurde geschaffen, damit die Genossenschaften nicht in jedem Mitgliedstaat der EU eine Tochtergesellschaft gründen müssen; die DGA-Genossenschaft kann, muss aber nicht als SCE gegründet werden; *Specht-Riemenschneider*, in: Specht/Hennemann 2023, Art. 2 DGA Rn. 85.

14 *Schild/Richter/Schmidt-Wudy*, in: BeckOK DatenschutzR 2024, Art. 2 DGA Rn. 84.

15 *Schild/Richter/Schmidt-Wudy*, in: BeckOK DatenschutzR 2024, Art. 2 DGA Rn. 82.

deren Ziel kein kommerzielles Geschäft ist und die möglichst viele Betroffene als Mitglieder gewinnen will, wäre es nach deutschem Recht sinnvoll und sicher, sich als eingetragener Verein zu gründen.[16]

	Datengenossenschaft außerhalb DGA	**Datengenossenschaft nach DGA**
Rechtsform	eingetragene Genossenschaft nach dt. GenG oder SCE nach VO 1435/2003	eingetragene Genossenschaft nach dt. GenG oder SCE nach VO 1435/2003
		Verein nach BGB
		andere Personengesellschaften, z.B. GbR
Mögliche Mitglieder	Dateninhaber und Datennutzer iSd DGA	Dateninhaber und Datennutzer iSd DGA, jedoch nur natürliche Personen und KMU
Vermittlungsdaten	Sowohl personenbezogene Daten als auch nicht personenbezogene Daten	Sowohl personenbezogene Daten als auch nicht personenbezogene Daten
Zwecke	Datenpool unter Mitgliedern	Herstellung geschäftlicher Beziehungen zum Zwecke der gemeinsamen Nutzung zwischen Dateninhabern und Datennutzern
	Datenverkauf durch Genossenschaft	
		Unterstützung ihrer Mitglieder bei der Wahrnehmung von Rechten in Bezug auf bestimmte Daten

Tabelle 1 Gegenüberstellung Datengenossenschaften

Die unterschiedlichen Gesellschaftsformen bieten unterschiedliche Vor- und Nachteile, je nach Betrachtungsweise. Eine eingetragene Genossen-

16 *Geminn/Johannes/Müller/Nebel* 2023, S. 27; *Keppler/Poncza*, in Paschke/Rücker 2024, Art. 2 DGA Rn. 74 beschreiben die vereinsrechtliche Mitgliedschaft als nicht zwingend, aber doch wohl möglich.

schaft bietet den Vorteil der gleichgestellten Entscheidung aller Mitglieder, unabhängig von Anteilen. Dies kann für kapitalstärkere potenzielle Mitglieder jedoch abschreckend sein. Die Gründung als Verein ermöglicht eine einfachere Skalierbarkeit, da betroffene Personen ohne großen Aufwand Mitglied werden können.

4. Beispiele

Viele Anwendungsszenarien von Datengenossenschaften sind denkbar. Im Folgenden sollen zwei davon skizziert werden.

4.1 Abschluss neuer Krankenversicherung (personenbezogene Daten)

Um einen verbindlichen Kostenvoranschlag für eine private Kranken(zusatz)versicherung zu erhalten, muss eine betroffene Person in der Regel ein von der gewählten Versicherungsgesellschaft bereitgestelltes Formular ausfüllen und sehr persönliche und sensible Daten angeben, wie zum Beispiel Daten über Krankheiten (eigene und solche, die in der Familie vorkommen), Körpermaße (Größe, Gewicht), Ernährung und andere (Vor-)Bedingungen, die mit ihrem wahrgenommenen Gesundheitsrisiko zusammenhängen. Um ein persönliches Angebot zu erhalten, müssten auch Name und Adresse angegeben werden. Eine individuelle und angemessene Schätzung kann nur erfolgen, wenn diese Daten zur Verfügung gestellt werden – was die Daten potenziell für zusätzliche Verarbeitung, Datendiebstahl und andere Risiken öffnet.[17]

Eine Datengenossenschaft, die in diesem Szenario die Datensouveränität der Betroffenen stärken will, könnte jedoch den Versicherungsunternehmen neue Kunden auf der Grundlage von anonymen und für die Versicherer verbindlichen Schätzungen anbieten. Ziel wäre es, die bestmöglichen Tarife und Versicherungsbedingungen sowie mehrere Optionen zur Auswahl zu erhalten, ohne dass sensible persönliche Daten an zahlreiche Versicherungsunternehmen übermittelt werden müssen. Zur Erstellung der Kostenvoranschläge würden die Daten der Betroffenen (die über die Mitgliedschaft in der Genossenschaft geteilt werden) in einer sicheren Umgebung verarbeitet werden und die Datenräume der Genossenschaft nie verlassen.

17 Beispiel nach *Geminn/Johannes/Müller/Nebel* 2023, S. 26.

Die Daten einer Person werden erst dann weitergegeben, wenn sie sich für eine Zusammenarbeit mit einer bestimmten Versicherungsgesellschaft entscheidet. Die Daten könnten dann vertraglich so eingeschränkt werden, dass sie nur zum Zweck der Vertragserfüllung verwendet werden.

Audits und andere Mittel zur Kontrolle der Verarbeitung könnten ebenfalls Teil der Anforderungen der Genossenschaft sein, denen ein Nutzer zustimmen müsste, was vielleicht sogar die ausschließliche Verarbeitung im begrenzten Datenraum der Genossenschaft beinhalten könnte. Eine dauerhafte Mitgliedschaft bei der Genossenschaft würde die Möglichkeit bieten, mit relativ geringem Aufwand von einem Versicherungsanbieter zu einem anderen zu wechseln, wenn anderswo bessere Konditionen angeboten werden. Das macht sie zu einem wertvollen Instrument für Menschen, die sowohl Input als auch Output in Sachen Versicherung optimieren wollen. In ähnlicher Weise könnten Genossenschaften auf den Wechsel anderer Vertragsarten (z. B. Mobilfunkverträge oder Strom) ausgerichtet sein.

4.2 Verwaltung von maschinellen Kalibrierinformationen als Vermittlungsdienst (nicht-personenbezogene Daten)

Gerade kleinen und mittelständischen Unternehmen, sogenannten KMU, drohen in einer datengetriebenen Wirtschaft erhebliche Nachteile gegenüber großen Konzernen, da der einzelne Datenbestand eines KMU in der Regel weniger umfangreich und reichhaltig ist wie derjenige großer Konzerne und überdies die Mittel und Möglichkeiten der wirtschaftlichen Nutzung des Datenbestands fehlen. Hier könnte ein Zusammenschluss in Datengenossenschaften sinnvoll sein, um unternehmensübergreifend Objekt- und Industriedaten wie Messdaten, Kalibrierinformationen oder digitale Zwillinge realer Objekte[18] auszutauschen und für einen wirtschaftlichen Mehrwert zu nutzen.

Ein solcher Mehrwert liegt für Unternehmen beispielsweise in der Entwicklung datengetriebener Services und Geschäftsmodelle oder in der Nutzung der Daten für die Überwachung, Steuerung oder Optimierung von Produktionsprozessen.[19]

Denkbar ist in diesem Zusammenhang zum Beispiel die Gründung einer Datengenossenschaft zur Verwaltung von maschinellen Kalibrierinforma-

18 Siehe hierzu z. B. *Müller*, ZD-Aktuell 2021, 05096.
19 *Weber/Werling/Tank/Baars*, HMD (2022) 59:1353–1365.

tionen und digitaler Kalibrierscheine. Kalibrieren umfasst die Tätigkeiten zur Ermittlung des Zusammenhanges zwischen den ausgegebenen Werten eines Messmittels und den bekannten Werten der Messgröße unter bekannten Bedingungen.[20] Solche Kalibrierinformationen werden für jedes kalibrierte Messmittel in Kalibrierzertifikaten dokumentiert. Diese können auch elektronisch ausgestellt werden (Digital Calibration Certificates – DCCs), was erhebliche Vorteile im Produktionsprozess mit sich bringt.[21] Als Mitglied einer Datengenossenschaft können die KMU Kalibrierinformationen und DCCs gemeinsam nutzen, Messprozesse und -qualität überprüfen und gegebenenfalls neue Geschäftsmodelle entwickeln.

5. Stellvertretung durch Datengenossenschaft (?)

Hauptaufgabe der Datengenossenschaft nach DGA ist es, ihre Mitglieder zu unterstützen. Die Legaldefinition nennt dabei beispielhaft Meinungsaustausch, die Sachkundevermittlung und das Aushandeln von Bedingungen.

Fraglich ist aber, ob sich eine solche Unterstützung auch in konkreten Handlungen für den Dateninhaber ausdrücken könnte, insbesondere durch das Abschließen von Verträgen in Vertretung oder die datenschutzrechtliche Einwilligung in Vertretung. Unterstellt wird hier, dass solche konkreten Handlungen für den Dateninhaber arbeitserleichternd wären. Sie würden die Attraktivität der Mitgliedschaft in einer Datengenossenschaft erhöhen können. Denkbar wäre dann, dass die Datengenossenschaft für ihr Mitglied als Stellvertreter handelt und zum Beispiel Datennutzungsverträge abschließen oder Änderungen von Nutzungsbedingungen zustimmen könnte.

5.1 Bei nicht-personenbezogenen Daten

Diese Möglichkeit der Stellvertretung ist hinsichtlich nicht-personenbezogener Daten zu bejahen. Bei nicht-personenbezogenen Daten kann Stellvertretung zusätzliche Aufgabe des Datenvermittlungsdienstes sein. Bei diesen geht es gerade darum, Geschäftsbeziehungen zwischen anderen Parteien, also zwischen Dateninhaber und Datennutzer, herzustellen.

20 *DIN e.V.* 2010.
21 Siehe z. B. *Johannes*, ZD-Aktuell 2020, 07280.

Auch sind die Aufgaben von Datenvermittlungsdiensten und Datengenossenschaften (als deren Unterfall) im DGA nicht abschließend geregelt. Sowohl Art. 2 Nr. 15 DGA als auch Erwägungsgrund 31 geben lediglich Regelbeispiele. Es steht der Datengenossenschaft offen, daneben noch andere Zwecke zu verfolgen.[22] Die Herstellung von Geschäftsbeziehungen erlaubt denklogisch auch die rechtsgeschäftliche Stellvertretung, wenn diese grundsätzlich zulässig ist. Hinsichtlich nicht-personenbezogener Daten ist eine Stellvertretung durch die Datengenossenschaft nach den allgemeinen Regelungen der §§ 164 ff. BGB möglich.[23]

5.2 Bei der Einwilligung zur Verarbeitung personenbezogener Daten

Ob eine Stellvertretung bezüglich personenbezogener Daten möglich ist, ist dagegen schwieriger zu beantworten.

Einerseits sind die Aufgaben von Datengenossenschaften im Rahmen des DGA nicht abschließend geregelt. Es werden lediglich Beispiele genannt, um die Grundlinie der Anwendbarkeit des DGA festzulegen. Eine Stellvertretung als zusätzliche Aufgabe ist daher denkbar. Wenigstens Art. 12 lit. m DGA scheint dies jedoch einzuschränken, indem er vorschreibt, dass Datenverarbeiter im besten Interesse der betroffenen Personen handeln müssen, insbesondere indem sie informieren und beraten, bevor die Einwilligung erteilt wird. Soweit die Stellvertretung jedoch eine zusätzliche Aufgabe außerhalb des DGA darstellt, kann die Aufgabenbeschreibung von Art. 12 lit. m DGA nicht einschränkend wirken.

Die Einwilligung kann eine Rechtfertigung für die Datenverarbeitung gemäß Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO sein. Gerade aber die Frage, ob eine Stellvertretung bei der Abgabe von datenschutzrechtlichen Einwilligungen im Sinne der DSGVO möglich ist, ist umstritten. Die datenschutzrechtliche Einwilligung muss gemäß Art. 4 Nr. 11 und Art. 7 DSGVO freiwillig, für den bestimmten Fall, in informierter Weise und als unmissverständliche Willensbekundung erfolgen. In der DSGVO ist die „Stellvertretung" für Einwilligungen speziell nur für Kinder geregelt. Es wird daher diskutiert, ob die Einwilligung als höchstpersönlich angesehen werden soll.[24] Die

22 *Specht-Riemenschneider*, in: Specht/Hennemann 2023, Art. 2 DGA Rn. 89.
23 *Specht-Riemenschneider*, in: Specht/Hennemann 2023, Art. 2 DGA Rn. 91.
24 *Frhr. v. Ulmenstein*, DuD 2020, 528 (532 f.), der die Einwilligung als höchstpersönliches Rechtsgeschäft einordnet.

herrschende Meinung verfolgt einen vermittelnden Ansatz. Danach ist Stellvertretung auch bei datenschutzrechtlichen Einwilligungen grundsätzlich möglich, aber für die Vollmachtserteilung sollen die gleichen hohen Anforderungen an Informiertheit und Bestimmtheit gelten wie bei einer Einwilligung selber.[25]

Die Praxistauglichkeit dieses Ansatzes ist fraglich und wird entsprechend auch in Diskussionen zu Personenbezogenen Informationsmanagement-Systemen (PIMS) nach § 26 Teledienste-Telemedien-Datenschutzgesetz (TDDDG) behandelt.[26] Wenn keine generalartigen Vollmachten zur Einwilligungserteilung möglich wären, müssten Datengenossenschaften für jeden einzelnen Vertretungsakt spezifisch Rücksprache mit ihrem Mitglied halten und um Vertretungsmacht bitten. Dies würde dem Ziel der Unterstützungsleistung wenigstens hinderlich sein. Oder anders: Wenn ein Vertreter für jeden Vertretungsakt detailliert Rücksprache mit dem Vollmachtgeber halten muss, ist fraglich, welchen Nutzen der Vertreter dem Vollmachtgeber überhaupt bietet.

Es stellt sich hier jedoch die Frage, ob es überhaupt um Einwilligungen geht. Im Kontext von Datenvermittlungsdiensten geht es oft um die Herstellung von Geschäftsbeziehungen, bei denen Daten gegen eine Gegenleistung wie Geld, Rabatte oder Zugang zu Diensten verwendet werden. Gemäß Art. 6 Abs. 1 UAbs. 1 lit. b DSGVO ist die Datenverarbeitung zulässig, wenn sie zur Durchführung eines Vertrags erforderlich ist. Datengenossenschaften können möglicherweise nicht im Namen ihrer Mitglieder „einwilligen", aber sie haben die Möglichkeit, bei entsprechender Bevollmächtigung Verträge über die Datennutzung für ihre Mitglieder abzuschließen. Entscheidend wäre, dass zwischen Einverständnis zur Datenverarbeitung durch den Dateninhaber und Leistung an diesen durch den Datennutzer irgendeine Art Gegenleistungsverhältnis vereinbart würde.

„Daten für Leistung" hat auch der Gesetzgeber als Geschäftsmodell legitimiert. Der zum 1. Januar 2022 neu eingefügte § 312 Abs. 1a BGB bestimmt, dass die §§ 312 ff. BGB auch für Verbraucherverträge gelten, bei denen der Verbraucher personenbezogene Daten bereitstellt oder sich zu deren Bereitstellung verpflichtet. Die Bereitstellung der Daten kann anstelle oder neben der Zahlung eines Preises erfolgen. Daraus resultierte dann auch keine Schlechterstellung des Dateninhabers als Vertragspartner im Vergleich

25 *Kühling*, DuD 2021, 783 (784); *ders.*, ZfDR 2021, 1; *Specht-Riemenschneider/Blankertz/Sierek/Schneider/Knapp/Henne*, MMR-Beil. 2021, 25 (42 f).

26 *Botta*, MMR 2021, 946 (948).

zum Einwilligenden. Einwilligungen können jederzeit widerrufen werden, während Verträge nur unter bestimmten Bedingungen gekündigt werden können. Jedoch stellt § 327q Abs. 1 BGB klar, dass die Ausübung von datenschutzrechtlichen Betroffenenrechten und die Abgabe datenschutzrechtlicher Erklärungen des Verbrauchers nach Vertragsschluss die Wirksamkeit des Vertrags unberührt lassen. Der Unternehmer erhält im Gegenzug ein besonderes Kündigungsrecht nach § 327q Abs. 2 BGB, wenn ihm die Fortführung des Vertrages nach Widerruf der Einwilligung wirtschaftlich nicht mehr zuzumuten ist.[27]

Die Möglichkeit, sich bei Einwilligungen und Verträgen bezüglich personenbezogener Daten wirksam vertreten zu lassen, wäre insgesamt auch eine Chance für die Verwirklichung der Rechte auf informationelle Selbstbestimmung (Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 Grundgesetz (GG)) und Datenschutz (Art. 8 Grundrechtecharta (GrCh)). Sie würden es ermöglichen, dass betroffene Personen kompetente Vertreter auswählen, die Entscheidungen in ihrem Sinne treffen sollen. Dadurch könnten sich die betroffenen Personen zum einen faktisch entlasten und zum anderen absichern. Inhaltlich wären sie durch den Vertreter beraten. Und bei Fehlentscheidungen und Schlechtleistungen wäre unter Umständen ein Rückgriff gegen diesen möglich. Tatsächliche Mängel in der Vertretungsmacht, also dass zum Beispiel ein Datenvermittlungsdienst für jemanden eine Einwilligung abgibt, der ihr gar keine Vollmacht erteilt hat, gingen auf der anderen Seite in der Regel zu Lasten des Verarbeiters. Grundsätzlich trägt nämlich die andere Seite, also diejenige, die sich darauf verlässt, dass der Vertreter mit Vertretungsmacht handelt, das Risiko. Sie kann entscheiden, auf die Anzeige der Vertretungsmacht zu vertrauen oder sich diese, etwa durch Vorlage einer Vollmachtsurkunde, nachweisen zu lassen.

5.3 Bei der Wahrnehmung von Betroffenenrechten nach DSGVO

Wiederum leichter zu beantworten ist die Frage, ob Datengenossenschaften für ihre Mitglieder Betroffenenrechte nach der DSGVO wahrnehmen könnten. Zu den Betroffenenrechten zählen die Rechte auf Auskunft, auf Berichtigung, auf Löschung, auf Einschränkung der Verarbeitung, auf Datenübertragbarkeit und auf Widerspruch.

27 Insgesamt dazu *Metzger/Schweitzer/Wagner*, ZfPW 2023, 227.

Diese Rechte stehen grundsätzlich zur Disposition der betroffenen Personen und können, wie andere Rechte auch, durch einen bevollmächtigten Vertreter wahrgenommen werden; zum Beispiel durch einen Rechtsanwalt oder aber auch durch eine Datengenossenschaft oder einen sonstigen Vertreter.

Unbeachtlich ist, dass Art. 80 DSGVO die außergerichtliche Geltendmachung von Betroffenenrechten nicht erwähnt. Art. 80 DSGVO regelt die kollektive Vertretung in verwaltungsrechtlichen und gerichtlichen Verfahren. Der Titel der Norm „Vertretung von betroffenen Personen" ist insoweit irreführend.[28]

6. Fazit

Es bleibt festzustellen, dass es Datengenossenschaften innerhalb und außerhalb des Anwendungsbereichs des DGA geben kann. Nicht jede Datengenossenschaft im Sinne des DGA muss eine eingetragene Genossenschaft im Sinne des GenG sein. Und nicht jede eingetragene Genossenschaft, die sich auch selbst als Datengenossenschaft bezeichnet, muss auch eine Datengenossenschaft im Sinne des DGA sein. Datengenossenschaften mit dem Ziel, die Daten ihrer Mitglieder in einem gemeinsamen Datenraum zu poolen, sind nämlich nicht per se Datenvermittlungsdienste im Sinne des DGA. Solange sie nicht das Ziel verfolgen, Geschäftsbeziehungen zwischen einer unbestimmten Anzahl von betroffenen Personen oder Dateninhabern einerseits und Datennutzern andererseits herzustellen, sind sie keine Datenvermittlungsdienste im Sinne des DGA.

Zusätzlich zur Datenvermittlung haben Datengenossenschaften die Aufgabe, die Interessen ihrer Mitglieder zu vertreten und können auch als Vereine gegründet werden. Ein bedeutender Aspekt ist die potenzielle Rolle von Datengenossenschaften als Interessenvertreter betroffener Personen. Durch den Zusammenschluss von Mitgliedern könnten Datengenossenschaften ein Gegengewicht zu den marktmächtigen Datenverarbeitern darstellen. Dies könnte insbesondere in Bezug auf personenbezogene Daten von Bedeutung sein. Die Datengenossenschaft könnte dazu dienen, informationelle Selbstbestimmung und Betroffenenrechte in Datenräumen insbesondere dadurch praktisch zu realisieren, dass die betroffenen Personen

28 *Kühling*, DuD 2021, 783 (785).

durch Zusammenschluss auf Augenhöhe mit Datenverarbeitern über die Inhalte von Einwilligungen verhandeln können.[29]

Jedoch wird dies nur dann praxistauglich realisiert werden können, wenn Datengenossenschaften in der Lage sind, in Vertretung der betroffenen Personen Erklärungen wie Einwilligungen oder Vertragserklärungen abzugeben.

Die derzeitige Rechtslage bietet jedoch keine Sicherheit[30] in Bezug auf diese Möglichkeit der Vertretung durch Datengenossenschaften. Es besteht daher Bedarf an weiterer rechtlicher Klärung, um die Rolle von Datengenossenschaften als Vertreter betroffener Personen im Rahmen der Datenverarbeitung zu definieren und zu ermöglichen.

Literatur

Baars, Henning (2022): *Was sind Datengenossenschaften?* https://www.datengenossenschaft.com/was-sind-datengenossenschaften/.

Beise, Clara (2021): Datensouveränität und Datentreuhand. *Recht Digital (RDi)*, 1(12), S. 597-604.

Botta, Jonas (2021): Delegierte Selbstbestimmung? PIMS als Chance und Risiko für einen effektiven Datenschutz. *MultiMedia und Recht (MMR)*, 24(12), S. 946-951.

DIN e.V. (2019): *Internationales Wörterbuch der Metrologie: grundlegende und allgemeine Begriffe und zugeordnete Benennungen* (VIM), 3. Auflage.

Frhr. v. Ulmenstein, Ulrich (2020): Datensouveränität durch repräsentative Rechtswahrnehmung. Begriffliche Prägung und normative Gestaltung sogenannter „Datentreuhänder. *Datenschutz und Datensicherheit (DuD),* 44(8), S. 528-534.

Geminn, Christian; Johannes, Paul; Müller, Johannes und Nebel, Maxi (2023): *Is that even legal? A guide for builders experimenting with data governance in Germany*. Mozilla Foundation. https://foundation.mozilla.org/de/research/library/is-that-even-legal/germany/.

Geminn, Christian und Johannes, Paul (2025): *Europäisches Datenrecht*. Baden-Baden: Nomos (in Vorbereitung).

Hennemann, Moritz und v. Ditfurth, Lukas (2022): Datenintermediäre und Data Governance Act. *Neue Juristische Wochenschrift (NJW)*, 75(27), S. 1905-1910.

Johannes, Paul (2020): GEMIMEG II: Sensoren und digitale Zwillinge – sichere und robuste kalibrierte Messsysteme, *Newsdienst der Zeitschrift für Datenschutz (ZD-Aktuell)*, 07280.

29 Dabei ist *Schild/Richter/Schmidt-Wudy*, in: BeckOK DatenschutzR 2024, Art. 2 DGA Rn. 98 zuzustimmen, dass Datengenossenschaft nur dann eine Waffengleichheit zwischen Datennutzern und Dateninhabern herstellen werden können, wenn sie eine gewisse Größe erreichen.

30 Vgl. auch *Metzger/Schweitzer/Wagner*, ZfPW 2023, 227 (265).

Johannes, Paul (2022): Europäisches Datenrecht – ein Spickzettel. *Newsdienst der Zeitschrift für Datenschutz (ZD-Aktuell)*, 01166.

Knapp, Jakob; Kobler, Jonas; Richter, Phillip (2022): Was der Bauer (nicht) kennt ... Datengenossenschaften. In: Heinze, Christian (Hrsg.): *Daten, Plattformen und KI als Dreiklang unserer Zeit*, OlWIR, S. 443-458.

Kühling, Jürgen (2021): Der datenschutzrechtliche Rahmen für Datentreuhänder. *Datenschutz und Datensicherheit (DuD),* 45(12), S. 783-788.

Kühling, Jürgen (2021): Der Datenschutzrechtliche Rahmen für Datentreuhänder. *Zeitschrift für Digitalisierung und Recht (ZfDR),* 1(1), S. 1 ff.

Metzger, Axel; Schweitzer, Heike und Wagner, Gerhard (2023): Datenschutz und Datenmarkt: Grundzüge einer Marktordnung für die europäische Datenwirtschaft. *Zeitschrift für die gesamte Privatrechtswissenschaft (ZfPW)*, 9(3), S. 227-266.

Müller, Johannes (2021): Der „digitale Zwilling". *Newsdienst der Zeitschrift für Datenschutz (ZD-Aktuell)*, 05096.

Paschke, Anne; Rücker, Daniel (2024): Data Governance Act – Kommentar. München: C.H. Beck (zitiert als Bearbeiter*in, in: Paschke/Rücker).

Specht-Riemenschneider, Louisa; Blankertz, Aline; Sierek, Pascal; Schneider, Ruben; Knapp, Jakob und Henne, Theresa (2021): Die Datentreuhand. *MultiMedia und Recht-Beilage (MMR-Beilage),* 24(6), S. 25-46.

Specht-Riemenschneider, Louisa und Hennemann, Moritz (Hrsg.) (2023): *Data Governance Act*. Baden-Baden: Nomos (zitiert als Bearbeiter*in, in: Specht/Hennemann).

Weber, Patrick; Werling, Maximilian; Tank, Ann und Baars, Henning (2022): Institutionalisierung digitaler Ökosysteme in der Rechtsform einer Genossenschaft: Case Study im produzierenden Kontext. *HMD Praxis der Wirtschaftsinformatik,* 59:1353–1365. https://doi.org/10.1365/s40702-022-00898-1.

Wolff, Heinrich; Brink, Stefan und v. Ungern-Sternberg, Antje (2024): *BeckOK Datenschutzrecht*, München: C.H.Beck, 47. Edition vom 1.2.2024 (zitiert als Bearbeiter*in, in: BeckOK DatenschutzR).

Die Infrastruktur, mein digitaler Zwilling und ich: Das Individuum und die digitale Identität im Mittelpunkt des Datenkapitalismus

Oliver Vettermann

Zusammenfassung

Politisch-strategisch und konzeptionell fokussieren sich Projekte zum Aufbau von Forschungsdateninfrastrukturen auf die Gewinnung und den Erhalt von Daten. Dies lenkt jedoch ab von den darin in Form digitaler Identitäten abgebildeten Individuen. Ein Beleg dafür ist die stetige Referenz auf den nicht greifbaren Begriff der „Datensouveränität". Dieses begriffliche Vakuum füllen die Gesetzesvorhaben auf EU-Ebene nicht in einem datenschutzaffinen Sinne aus, sondern verstehen darunter das ökonomische Ziel der gleichberechtigten Teilnahme an einem Datenbinnenmarkt. Dieses Ergebnis stützt auch die Analyse der nationalen und europäischen Digital- und Datenstrategien. Der status quo honoriert das extraktive Verhalten von Forscher:innen zu Lasten der datengenerierenden Personen in einem kapitalistischen System. Zusätzlich fehlt es den Infrastruktur-Vorhaben in der Konzeption und Umsetzung an ethischem Bewusstsein, um Interessen des Gemeinwohls in den Strukturen zu verankern.

1. Einleitung

2023 war das Jahr der Dateninfrastrukturen: Die Nationale Forschungsdateninfrastruktur (NFDI) weitet mit insgesamt 26 Konsortien ihre Fühler in die verschiedenen Forschungsdisziplinen aus, verknüpft Expertise und bereitet die Verknüpfung bestehender Infrastrukturen mit der European Open Science Cloud (EOSC) vor. In einem ähnlichen Fahrwasser bereitet der European Health Data Space (EHDS) den Boden für Gesundheitsdaten in der Forschung und lässt die fortwährende Diskussion um den Broad Consent in der DSGVO neu aufleben. GAIA-X ergänzt die wissenschaftliche EOSC und will eine europäische Dateninfrastruktur schaffen, die ähnlich wie die NFDI die Datensouveränität durch ein dezentrales Netz aus Datenspeichern in ganz Europa für Unternehmen herstellen will. Neben

dem Plan in NFDI und GAIA-X, anstatt eigener auf bestehende Infrastrukturen zurückzugreifen, fällt ein weiterer gemeinsamer Aspekt auf: Der Nukleus, das datengenerierende Individuum und seine digitale Identität, wird kaum diskutiert.

Basierend auf der im Rahmen der eigenen Doktorarbeit[1] ausgearbeiteten Sicht sämtlicher, von einer Person verursachter Datenbündel als Teil ihrer digitalen Identität sollen in diesem Beitrag nationale und europäische Bestrebungen digitaler Infrastrukturen näher untersucht werden. Damit versucht sich der Beitrag an einer Meta-Analyse, wie die tatsächliche (datenschutzrechtliche) Kontrolle und in der Politik verwendete ethische Konzepte wie Vertrauen, Transparenz und Souveränität umgesetzt werden. In den Blick zu nehmen sind dabei neben der Einwilligung eines „Datensouveräns" auch die Nachvollziehbarkeit eigenen rechtlich relevanten Handelns, technische und organisatorische Maßnahmen und Sanktionsapparate. Resultierend soll dann untersucht werden, ob es einer anderen, ethischen Lesart europäischer Regelungen bedarf, um digitale Identitäten zu schützen und die subjektive bzw. individuumzentrierte Datensouveränität zu stärken. Es ergeben sich folgende, im Beitrag aufzuarbeitende Schlüsselfragen: Auf welche legislativen Grundlagen stützen sich die politischen Bestrebungen nach Transparenz, Souveränität und Vertrauen? Wie lassen sich die verschiedenen Ebenen einer Datensouveränität – nämlich subjektbezogen, geopolitisch und ökonomisch – hier einordnen? Und gelingt es kommenden und jüngeren Regelwerken der EU, den Ausgleich zwischen Infrastruktur und Individuum angemessen umzusetzen?

Mit diesem Thema soll dieser Beitrag ein Gegengewicht zum Überthema der Konferenz – „Data Sharing – Datenkapitalismus by Default?" – bilden, um das datengebende Individuum nicht aus den Augen zu verlieren.

2. Zum Begriff der digitalen Identität

Bevor sich der Untersuchung in der Sache gewidmet wird, ist eine Definition des Begriffs der digitalen Identität[2] für das weitere Verständnis nötig:

Als digitale Identitäten sind in diesem Beitrag miteinander verknüpfte Daten (dann: Teilidentität) oder Datensätze (dann: Gesamtidentität) zu

1 *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, 2022.

2 Hierzu sowie im Folgenden ausführlich *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, 2022 (7ff).

verstehen, die sich durch ihren hohen Aussagegehalt und Identifizierungsgrad in ihrer aggregierten Form auszeichnen. Sie bilden die analoge Identität und damit verschiedenste Wesenszüge, Emotionen und Gedanken des Menschen ab – etwa als „digitaler Zwilling"[3] zum realen Ich. Meistens sind sie mit einem Pseudonym bzw. Identifier versehen, können aber auch selbst als solches fungieren (dann: Quasi-Identifier). Die dadurch mögliche Zusammenführung von Datensätzen bildet Teile und Wesenszüge der analogen Identität ab, bezieht den Begriff des Personenprofils daher ein. Jedoch reicht der Begriff der digitalen Identität weiter, da er nicht das einzelne Profil in den Mittelpunkt stellt, sondern das Bündel aller Datenemissionen des Individuums (z.B. Accounts) selbst. Insofern sind auch anonyme bzw. anonymisierte Datensätze Teil der digitalen Identität, da sie unter gewissen Umständen ein Abbild komplettieren könnten. Ergänzt wird die inhaltliche durch eine zeitliche Abbildungsebene, da mit zunehmender Digitalisierung alltäglicher Vorgänge auch der gesamte menschliche Lebenszyklus mitzudenken ist. Mit zunehmendem Aufhalten in der digitalen Welt bilden Online-Shops, Netzwerke, usw. das analoge Selbst ab. Die Fähigkeit, hierüber aktiv verfügen zu können, wird als digitale Selbstbestimmung bezeichnet.[4] Eine dahingehende (subjektive) Datensouveränität meint also den Gehalt des Grundrechts auf informationelle Selbstbestimmung im Sinne einer eigenverantwortlichen Verfügung über Verbleib und Nutzung der „eigenen" Daten.

3. Thesen

Die einleitenden Fragen werden durch drei Thesen und ihre Analyse beantwortet: Aus dem Blickwinkel des datengebenden bzw. datenden[5] Individuums wird im Folgenden der Begriff der Datensouveränität (These 1), dessen rechtliche Umsetzung in Forschungsdatenräumen (These 2) und ihr rechtlich-ethischer Unterbau (These 3) analysiert.

---

3 Daher nicht gleichzusetzen mit dem Begriff in der Industrie 4.0, siehe *Müller*, ZD-Aktuell 2021, 05096.

4 Exemplarisch *Digital Autonomy Hub*, Policy Brief #4, S. 5; *Denga*, GRUR 2022, 1113 (1113) mwN.

5 Meint „daten" als Verb, stehend für „Daten produzieren/generieren". In Anlehnung an *Lisker*, Masterarbeit: Von der (Un-)Möglichkeit, digital mündig zu sein, 2023.

These 1: Die Datensouveränität ist eine Leerformel für die wirtschaftliche und forschungspolitische Anschlussfähigkeit Deutschlands.

Der Ursprung des Begriffs „Datensouveränität" lässt sich unter anderem[6] im Jahr 2017 auf die Erwähnung von Alexander Dobrindt im Bezug auf ein geplantes Datengesetz zurückführen. Das Gesetz selbst ist Gegenstand des „Strategiepapier Digitale Souveränität", mit dem das Ziel des Gesetzes und das Begriffsverständnis vorwiegend ökonomisch eingeordnet werden. Darin der Satz: „Der Schlüssel dazu ist die Datensouveränität des Einzelnen."[7] Mit „des Einzelnen" referenziert dieser Satz wie auch der Großteil der juristischen Literatur[8] die *subjektive* Lesart im Volkszählungsurteil des BVerfG, in dem die Verfügungsherrschaft über die eigenen Informationen im Mittelpunkt steht: „Im Mittelpunkt [...] stehen Wert und Würde der Person, die in freier Selbstbestimmung als Glied einer freien Gesellschaft wirkt."[9] Die Definition der Datensouveränität erscheint also zunächst als eine subjektivrechtliche, die für das schützende Grundrechtsbündel der digitalen Identität steht. Bündel, weil wegen der zunehmenden Digitalisierung des Alltags der digitale Aspekt des Persönlichkeitsrechts aus Art. 7, 8 GrCh und Art. 2 Abs. 1 iVm 1 Abs. 1 GG in die übrigen, geeigneten Grundrechte hineinstrahlt, sich in diesen verzweigt und sie verselbstständigt. Das subjektive Verständnis erscheint deshalb auch synonym zu den Begriffen „Digitale Souveränität" und „digitale Selbstbestimmung". Eine trennscharfe Definition gibt es insoweit nicht.[10]

Der subjektive Begriff hat in den letzten Jahren eine wiederholte Wandlung und Erweiterung erfahren. Wie die Facetten eines Diamanten hat die Politik die Datensouveränität auch ökonomisch, geopolitisch und nunmehr forschungsbezogen bzw. forschungspolitisch geschliffen:

Ökonomisch steht die Wertschöpfung an und aus Daten im Fokus. Distanziert vom Individuum wird sich allein dem Objekt gewidmet, dessen inhaltlichen Werte möglichst fair und transparent erschlossen werden sol-

6 Vertiefend zur Genese *Pohle/Thüer/Dammann/Winkler*, in: Kersting/Radtke/Baringhorst (Hrsg.), Handbuch Digitalisierung und politische Beteiligung.

7 Siehe https://web.archive.org/web/20171101193849/https://www.bmvi.de/SharedDocs/DE/Artikel/DG/datengesetz.html.

8 *Denga*, GRUR 2022, 1113 (1118f); *Roßnagel*, MMR 2023, 64 (64f); *Krüger*, ZRP 2016, 190 (190f).

9 BVerfGE 65, 1 (41).

10 So auch *Umweltbundesamt*, Digitale Kommune/Digitale Region, Texte 62/2023 (57); *Pohle/Thüer/Dammann/Winkler*, in: Kersting/Radtke/Baringhorst (Hrsg.), Handbuch Digitalisierung und politische Beteiligung.

len. Es handelt sich also in einem kapitalistischen System[11] um „strategische Vermögenswerte“[12], die u. a. als Tauschmittel für die Nutzung von Diensten (also Konsum) genutzt werden – daher auch: Datenkapitalismus. Profiteure sind Staat und Wirtschaft.[13] Regelmäßig werden Nutzer:innen ebenso als Profitierende gesehen, da sie sich durch das Einspeisen von Daten in den Kreislauf einbringen und ihnen je nach Perspektive unmittelbar oder zumindest mittelbar Profit zufließt.[14] Schließlich können Nutzer:innen freiwillig einwilligen („dezentrale Entscheidungsprärogative der Datensubjekte“[15]), zwischen verschiedenen Anreizen – finanziell, moralisch, technisch – wählen und so informiert entscheiden, ob sie mit den Vorzügen übereinstimmen oder nicht – ganz nach dem Vorbild der DSGVO, vgl. Art. 1 Abs. 1. Eine derartige Perspektive gewichtet das Binnenmarkt-Ziel der DSGVO allerdings höher als den grundrechtlichen (Daten-)Schutz der Personen. Schon das Setzen von Anreizen zur Motivation der Wertschöpfung beeinflusst die Freiwilligkeit, weil sie die Wahlmöglichkeit vorgibt und damit begrenzt. Sie ist stets von der Rolle des Subjekts in diesem System abhängig.[16] Die Einwilligung entpuppt sich so als responsibilisierte Form[17] der Souveränität, die systemisch keine echte Souveränität im Sinne einer Entscheidungshoheit aufweist, sondern einem Daten-Extraktivismus im digitalen Raum dient.

Geopolitisch zeigt sich die Datensouveränität dagegen als politische und staatliche Handhabe, und hat dabei die Abhängigkeiten zwischen verschiedenen Staaten und die Sicherheit Europas[18] im Blick. Diese bestehen u. a. in Lieferketten oder durch technische Bedrohungen wie Cyberangriffe. Aufgabe ist es dabei, den Schutz von Daten bzw. Informationen institutionell abzusichern[19] (auch hier: „strategische Vermögenswerte“) und per Gesetz für sicherere Systeme zu sorgen – beispielsweise durch den Cyber Resilien-

11 Hierzu exemplarisch die Beispiele von *Bisges*, MMR 2017, 301 (304ff).
12 So Europäische Kommission, Digitalstrategie, 2022 (5).
13 *Denga*, GRUR 2022, 1113 (1114). Vgl. die Ziele von GAIA-X in *Schütrumpf/Person*, RDi 2022, 281 (283).
14 Zu Datennutzungsverträgen *Rosenkranz/Scheufen*, ZfDR 2022, 159 (170ff). Zum Berufsbild des Dategenerierens unter Art. 12 Abs. 1 GG siehe *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, 2022 (210ff).
15 EuGH C-252/21, Rn. 143, 148f; *Denga*, GRUR 2022, 1113 (1120, 1114).
16 Hierzu *Engeler*, NJW 2022, 3398 (3403).
17 *Lisker*, Masterarbeit: Von der (Un-)Möglichkeit, digital mündig zu sein, 2023 (17ff mwN).
18 Vgl. Europäische Kommission, Digitalstrategie (5).
19 Vgl. *Kelber/Bortnikov*, NJW 2023, 2000 (2001f).

ce Act und die NIS2-Richtlinie. Diese Sicht reiht sich in das allgemeine Monitoring von staatlichen Abhängigkeiten[20] ein, in denen auch das Wissensmanagement als Datenschatz[21] erwähnt wird.

Forschungsbezogen kann die Datensouveränität dagegen als spezielle Form der subjektbezogenen Version verstanden werden. Forscher:innen finden sich in Gesprächen regelmäßig in der Position wieder, eigene Forschungsdaten teilen zu müssen und zugleich nicht aus der Hand geben zu wollen. Dabei kommt der Wunsch auf, dass „ihre" Daten lizenz- und datenschutzrechtlich geschützt werden sollen, auch wenn die gesetzlichen Anwendungsbereiche nicht greifen. Wichtig ist, die Inhalte und Schlussfolgerungen zu beanspruchen und die Lorbeeren – wissenschaftliche Credits – zu ernten. Der damit einhergehende Druck auf Forscher:innen ergibt sich ebenso aus dem Datenkapitalismus und einem stetigen Streben nach Innovation. Hierbei stehen neben Open-Data-Aspekten auch fehlende Anonymisierungsverfahren oder „der böse Datenschutz"[22] im Weg.

Forschungspolitisch dominiert die institutionelle Sicht auf Forschungsdaten, die ebenso das Teilen und Nachnutzen im Fokus hat. Die Begriffe „forschungsbezogen" und „forschungspolitisch" fallen auseinander, weil ersteres die Praxis und Forscher:innen im Fokus hat und zweiteres die übergeordnete Zielrichtung der institutionellen Forschung meint. Im Fokus stehen einzelne Forscher:innen dann nur mittelbar, z. B. wenn ihnen der Zugang zu den Forschungsdatenschätzen ermöglicht und gewährt werden soll. Das setzt jedoch auch voraus, dass sie sich von besagter eigener, subjektiver Souveränität lösen. Abseits davon zeigt sich die forschungspolitische Perspektive in der Datenverarbeitung „um des Antrags Willen", wenn sich Forschungsfragen an gesellschaftlichen Themen und entsprechenden Ausschreibungen orientieren, anstatt sich aus der Sachebene und der wissenschaftlichen Arbeitsweise selbst zu ergeben. Dieser Aspekt ist also ökonomisch, institutions- und strukturbezogen geprägt, um Deutschland international an die Spitze der Forschung „made in Germany" zu führen.

So facettenreich der Begriff damit wirkt, so leer ist er zugleich: Die gezeigten Perspektiven setzen die Erhebung und Verarbeitung von Daten und

20 *BMWi*, Schwerpunktstudie Digitale Souveränität, 2021.

21 Ähnlich *Kelber/Bortnikov*, NJW 2023, 2000 (2001).

22 Exemplarisch die Unsicherheit von Forscher:innen bei Interessenabwägungen skizzierend *Buchner*, DuD 2022, 555 (556f). Ob gemeinwohlorientierte Forschungsinteresse in der datenschutzrechtlichen Interessenabwägung pauschal „unstreitig als hoch" einzuordnen sind, ist vor dem Hintergrund einer einzelfallbezogenen Risikoabwägung streitbar.

damit eine bestehende Rechtsgrundlage voraus. Bei genauem Hinsehen fällt der Wandel von einer subjektivrechtlichen Prägung zu einer struktur- und wirtschaftsbezogenen Neigung der Begriffsverwendung hin auf, die die Interessen der Nutzer:innen als Datensubjekte und -produzent:innen vernachlässigt. Es werden Möglichkeiten zur Teilhabe am Datenmarkt gewährt und positiv herausgestellt, ohne in aktuellen Strategien brauchbare Ansätze und Vorhaben für eine ethische wie grundrechts- bzw. datenschutzkonforme Umsetzung anzureißen[23] – wie noch zu zeigen sein wird. Der Grund dafür liegt auf der Hand: Datenschutz und Datensouveränität sind unter der Einwilligung systemisch nicht vereinbar. Wie *Engeler*[24] und *Samardzic/Becker*[25] herausgearbeitet haben, führt die Einwilligung durch ihre mittlerweile stark ökonomische Prägung zwar zu Anreizen, die aber wiederum nicht zur gesetzlich angelegten Freiwilligkeit führen.[26] Die Einwilligung fungiert damit als Symbol ökonomischer Datensouveränität. Im Forschungskontext spielen forschungspolitische und ökonomische Lesart der Souveränität zusammen: Das Übermaß an Information gegenüber Betroffenen zur Erfüllung der auferlegten Transparenz führt dazu, dass die Einwilligung zunehmend schwieriger für die Forschung umzusetzen ist. Die forschungspolitische Datensouveränität übt hier entsprechend Druck auf Forscher:innen aus, mehr Daten zu verarbeiten und länger nachzunutzen. Die inhärente Dynamik eines Broad Consent, der nur vorübergehend die nicht-detaillierte Information zum Forschungskontext überwinden soll, wird daher selten zutreffend adressiert. Eher wird er glorifiziert, weil sonst keine Möglichkeit besteht, an wertvolle (Gesundheits-)Daten zu kommen.[27] Mit generativen LLM-Modellen und der öffentlichen Diskussion nachgeordneter, sekundärer Verarbeitungsformen liegt das Problem des Kontrollverlustes jedoch offen, da durch eine Einwilligung nur die primäre Verarbeitung betroffen, aber selten die Zwecke der sekundären Verarbeitung vorhergesagt werden könnte. Eine Freiwilligkeit kann sich also nur auf die primäre Verarbeitung beziehen.

Die Einwilligung als Instrument der Datensouveränität ist damit ein leeres Versprechen, im Forschungskontext Handhabe über einen Sachverhalt

23 Beispielsweise *Bundesregierung*, Datenstrategie 2023, S. 32 ohne Einbettung.
24 *Engeler*, NJW 2022, 3398ff.
25 *Becker/Samardzic*, EuZW 2020, 646.
26 Vgl. EuGH C-252/21, Rn. 143, 148f.
27 Vgl. *Spitz/Cornelius*, MedR 2022, 191 (192ff); *Medizininformatik-Initiative AG Consent*, Stellungnahme Dynamic Consent.

zu geben, von dem weder Forscher:innen noch Nutzer:innen vorher wissen können. Werkzeuge wie der Datenmanagementplan oder das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) können hier helfen. Bislang werden sie von Forscher:innen aber nicht als Selbstkontrolle verstanden, sondern häufig als zusätzliche Last der Dokumentation. Vertrauen und Transparenz laufen damit ins Leere. Die Datensouveränität verkommt so zur Worthülse, die den eigentlichen Kern der Privatheit und dem Schutz vor informationellen Kontextverletzungen – zeitlich, kulturell oder publikumsbezogen –[28] nicht gerecht wird. Stattdessen wird sie in wirtschaftlichen und forschungspolitischen Kontexten dazu genutzt, ökonomische Ziele zu verkörpern und Nutzer:innen eine gefühlte Selbstbestimmung zu vermitteln.

These 2: Forschungsdatenräume sind „menschenleer" und datenfreundlich konzipiert.

Die Grundlage eines Zusammenwirkens von Nutzer:innen und der Forschung besteht vor allem darin, dass ein regelmäßiger Datenfluss besteht und die Ergebnisse dieser Preisgabe sich positiv auf die Gesellschaft auswirken. Dies ist mit Blick auf Art. 179 AEUV die Grundvoraussetzung für einen Daten-Binnenmarkt im Sinne eines „free flow of data", vgl. Art. 1 Abs. 1 DSGVO. Forschung, vor allem Gesundheitsforschung, ist damit ein Katalysator für Lösungen, die in Daten-Heuhaufen verborgen sind. Das Gemeinwohl ist diesem Begriffsverständnis schon qua Forschungsfreiheit gem. Art. 13 S. 2 GrCh, Art. 5 Abs. 3 GG in die Wiege gelegt.[29] Dies setzt aber voraus, dass die Datenpreisgabe als Ausnahme und nicht Regel verstanden wird; Privatheit muss respektiert und stets an den Grenzen zu anderen Freiheiten verteidigt werden. Privatheit ist dabei die „Schaffung eines geschützten Raumes als Voraussetzung zur Persönlichkeitsentfaltung, geschützt von den invasiven Kräften einer in die Lebenswelt eindringenden Wirtschaft"[30] in Form des Datenkapitalismus. Dies gesagt, müssen auch Grundlagen wie Governance-Strukturen und Infrastrukturen abbilden, dass die Datenaufnahme und -nutzung stets ein Eindringen ist. Grundsätz-

28 *Heesen/Ammicht Quinn* et al., in: Roßnagel/Friedewald (Hrsg.), Die Zukunft von Privatheit und Selbstbestimmung, 161 (175).

29 Vgl. BVerfGE 35, 79 (114); 111, 333 (354); *Ruffert*, in: Calliess/Ruffert, EUV/AEUV, Art. 13 GrCh Rn. 7.

30 *Heesen/Ammicht Quinn* et al., in: Roßnagel/Friedewald (Hrsg.), Die Zukunft von Privatheit und Selbstbestimmung, 161 (167 mwN). Ausführlich hierzu *Sandfuchs*, Privatheit wider Willen?, 2015 (7ff).

lich kann so ein Eindringen durch das hohe Gut der Volksgesundheit und ähnliche altruistische Ziele gerechtfertigt sein – es kommt für diese Ausnahme aber stets auf den Einzelfall an.

Einen Rahmen für das Verhältnis von Datengebenden und der Forschung als Datenempfängerin sollten die aktuellen[31] europäischen und nationalen Regulierungsvorhaben bieten: Data Act, Data Governance Act, Forschungsdatengesetz sowie Gesundheitsdatennutzungsgesetz, jeweils im Einklang mit der DSGVO. Der Data Act und der Data Governance Act bilden dabei die allgemeine Regulierung von Daten ab; der Data Act bezieht sich auf die aus der Nutzung eines Produkts generierten Daten, der Data Governance Act dagegen auf die Daten in der öffentlichen Hand. Beide EU-Regelungen setzen sich also mit dem Datenzugang auseinander. Für einen ausreichenden Bezug müsste sich der EU-Rahmen aber auch mit den Betroffenenrechten auseinandersetzen. Infrastruktur und Governance-Strukturen müssen die Interessen und Rechte Betroffener sichtbar mitdenken, sei es durch Beteiligungsmöglichkeiten als Kontrolle oder menschliche Werte (z. B. Ethik, siehe hierzu These 3).

Der *Data Act*[32] adressiert vor allem Hersteller von Produkten und Bereitstellung von verbundenen Diensten (also Hard- und Software von smarten Datenanwendungen wie IoT), ihre Nutzer:innen, Dateninhaber:innen und Datenempfänger:innen. Der Begriff der Dateninhaber:in meint gem. Art. 2 Nr. 13 DA im Hinblick auf nicht-personenbezogene Daten eine damit einhergehende Handhabe über die Daten durch die produktherstellenden Unternehmen selbst. Die datengenerierende Person wird in den Erwägungsgründen (zB ErwGr 5 und 18 DA) und via Einschub in Art. 2 Nr. 5 DA als Nutzer:in beschrieben. Wenngleich es sich nicht um personenbezogene Daten handelt, stehen der Person Zugangs-, Weitergabe- und Nutzungsrechte des Kapitel II zu. Nutzer:innen werden so maßgebliche Rechte eingeräumt, allerdings zur Effektuierung des Daten-Binnenmarktes.[33] Sobald es sich um personenbezogene Daten handelt, kommen gem. ErwGr 34 DA die Rechtsgrundlagen der DSGVO hinzu, sodass es für das Datengenerieren bei Personenbezug der Daten einer Einwilligung nach Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO bedarf. Während mit Geltung der DSGVO das Risiko für personenbezogene Daten beim Verantwortlichen liegt, liegt es

31 Der Beitrag bezieht sich auf den letzten Stand im April 2024.

32 Siehe https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L_202302854

33 Vgl. *Funk*, CR 2023, 421 (425f).

nach dem Data Act bei den Nutzer:innen selbst: „Der Nutzer trägt die Risiken und genießt die Vorteile der Nutzung des vernetzten Produkts und sollte auch Zugang zu den von ihm generierten Daten haben. Er sollte daher berechtigt sein, aus den von diesem vernetzten Produkt und allen verbundenen Diensten generierten Daten Nutzen zu ziehen."[34] Über den Umfang an Daten und Risiken werden Nutzer:innen gem. Art. 3 Abs. 2 DA informiert. Eine Gegenleistung für eine Datenweitergabe enthält nicht die Nutzer:in, sondern die Dateninhaber:in (also das Unternehmen) als Kompensation für die technische Infrastruktur und Dienstleistung (Art. 9 DA).[35] Im Gegenzug erhält die Nutzer:in Zugriff auf die selbst generierten Daten (Art. 4 Abs. 1 DA). Nutzer:innen erhalten damit zumindest auch die Nutzung des Geräts und damit verbundener Dienste im Tausch gegen ihre Daten, was dem jüngeren Bild einer datenökonomischen Position der Verbraucher:in entspricht.[36] Dezent lässt sich der Charakter von Leistung (Daten) und Gegenleistung auch in der „Gegenseitigkeit geschlossener Verträge" über nicht-personenbezogene Daten erkennen (vgl. Art. 4 Abs. 13, Art. 1 Abs. 10 DA). Insofern widersprechen sich die Erwägungsgründe leicht im Abschnitt zur Prüfung relevanter Grundrechte, worin wegen der marktorientierten Ausrichtung der Datennutzung für Nutzer:innen durchaus ökonomische Interessen (Art. 15, 16 GrCh als Spiegelbild der Art. 12, 14 GG) benannt werden könnten.[37] Insgesamt lässt der Data Act aber neben erwähnten Möglichkeiten für Information und Teilhabe an dem generierten, nicht-personenbezogenen Datenschatz wenig Spielraum für Widerspruch/Widerruf und Abwägungen von rechtsethischen Interessen. Höchstens über den offenen Begriff der Fairness über die Nutzung wegen außergewöhnlicher Notwendigkeit (Art. 14 ff DA) lassen sich Mechanismen erkennen. Die Schwäche auf der Betroffenenseite könnte darin begründet liegen, dass mit Aktivierung des Personenbezuges dynamisch das Datenschutzrecht zur Anwendung kommt und für nicht-personenbezogene Daten primär keine grundrechtlichen Interessen aufkommen.[38]

Der *Data Governance Act* widmet sich der Weiterverwendung von Daten bestimmter Datenkategorien, die sich im Besitz der öffentlichen Hand in-

34 ErwGr 18 DA.
35 Jeden Ausgleich aufseiten der Nutzer:innen ablehnend *Funk*, CR 2023, 421 (424ff).
36 Vgl. EuGH C-252/21, Rn. 102, 143, 148ff. Auch *Gesmann-Nuissl/Meyer*, Die neue Ära des Datenhandels – in diesem Band.
37 Vgl. *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, 2022 (210ff).
38 Ähnlich *Funk*, CR 2023, 421 (426).

nerhalb der Union befinden (Art. 1 Abs. 1 DGA) und installiert mit dem Datenaltrusimus und Diensten zur Datenvermittlung bei Preisgabe der Daten durch Betroffene Konzepte zur Daten-Governance. Alle Konzepte enthalten Ansätze, die Individuen in die Prozesse einzubeziehen. Einige Beispiele: Für die personenbezogenen Daten im Besitz öffentlicher Stellen sind Schutzmaßnahmen vorgesehen wie die vorherige Anonymisierung und entweder digitale oder physische Zugangsschranken (Art. 5 Abs. 3 DGA). Da die Einwilligungsmöglichkeit hier entfällt, wenn die personenbezogenen Daten per Anonymisierung aus dem Geltungsbereich des Datenschutzrechts entfernt werden, wird sie durch das Erlaubnisverfahren (Art. 5 Abs. 2, 4 und Art. 9 DGA) ersetzt. Datenvermittlungsdienste referenzieren in Art. 12 DGA auf die traditionellen Mechanismen des Datenschutzes und der informationellen Selbstbestimmung, also technische und organisatorische Maßnahmen für Daten- und IT-Sicherheit (lit. c und j), Zweckbegrenzung (lit. a), das Angebot spezifischer technischer Werkzeuge zur Erhöhung der subjektiven Datensouveränität (lit. e) sowie einen fairen, transparenten und nicht-diskriminierenden Zugriff (lit. f). Der Datenaltruismus basiert auf der freiwilligen Datenweitergabe für Zwecke, die eine datenaltruistische Organisation anbietet. Sie fußt damit auf Einwilligung und subjektiver Datensouveränität, wenngleich die nationalen Regeln zur Einrichtung einer Aufsichtsbehörde und der Verfahren (siehe Art. 16 DGA) sowie Empfehlungen zur Einwilligung (Art. 25 DGA) bis dato fehlen. Insoweit dürfte sich nicht nur hierin an der DSGVO orientiert werden, sondern auch bei der Erfüllung der Transparenzanforderungen nach Art. 20 DGA und den Vorgaben zum Schutz subjektiver Interessen der Dateninhaber:innen nach Art. 21 DGA. Informiertheit und Transparenz gepaart mit Freiwilligkeit sollen jedoch ebenso das stark ökonomisch geprägte Ziel des DGA stützen: „Daten stehen im Mittelpunkt dieses Wandels: Die von Daten vorangetriebene Innovation wird sowohl den Bürgerinnen und Bürgern der Union als auch der Wirtschaft enorme Vorteile bringen."[39] Die Governance der Bürger:innen dient damit in erster Linie der „Gestaltung, Schaffung und Aufrechterhaltung gleicher Wettbewerbsbedingungen in der Datenwirtschaft", also dem gleichberechtigten Zugang zu einem Daten-Binnenmarkt. Wie bei These 1 zeigt sich hier erneut, dass subjektive und

39 ErwGr 2 DGA.

ökonomische Datensouveränität eng miteinander verzahnt sind. Ein Indiz dafür ist das Ziel der Innovation.[40]

Der *European Health Data Space* (kurz EHDS) soll laut Entwurf einen Forschungsdatenraum speziell für Gesundheitsdaten schaffen, bestehend aus Vorschriften auf EU-Ebene, Standards und Verfahren sowie Infrastrukturen und einem Governance-Rahmen.[41] Relevante Akteure sind hier Dateninhaber:innen, Zugangsstellen für Gesundheitsdaten und Datennutzer:innen. Nach Art. 2 Abs. 2 lit. y EHDS-VO[42] lässt sich die Dateninhaber:in als natürliche oder juristische Person verstehen, die im Gesundheits- oder Pflegesektor aktiv ist oder die Forschungstätigkeiten hinsichtlich dieser Sektoren durchführt. Dennoch zielt die VO auf den Schutz natürlicher Personen, indem Rechte über Verfügbarkeit und Kontrolle gestärkt werden sollen. Konkret soll diese Stärkung durch Zugriffsrechte (zB Art. 8a EHDS-VO) oder vorgegebene Zwecke der Nutzung (Art. 33, 34 EHDS-VO) als neue Rechtsgrundlagen im Zusammenspiel mit der DSGVO gelingen. Soweit es für den EHDS nicht weiter vorgegeben ist, sind bei personenbezogenen Daten aber die Informationspflichten der Art. 13, 14 DSGVO zu erfüllen – auch bei der Sekundärnutzung. Dadurch wird das Verständnis der Forscher:innen für die eigene Verantwortung verkompliziert. Weitere Unsicherheiten produzieren die fehlende Legaldefinition der Anonymisierung und ihrer relativen bzw. volatilen Wirkung, fehlende interoperable Formate und ein Abgleich der Weiterverarbeitung nach DSGVO mit dem Konzept der Sekundärnutzung nach EHDS-VO.[43] Hevorgehoben sei zuletzt der Ausschluss des Patientenwillens: Soweit in der Trilog-Fassung ersichtlich ist gem. Art. 8h (Primärzweck) und Art. 35f EHDS-VO (Sekundärzweck) keine Einwilligung vorgesehen; alle Patient:innen werden ohne Ausweichmöglichkeit in die elektronischen Register aufgenommen. Der Gesetzgeber nimmt damit eine Abwägung vorweg, die im Einzelfall trotz Anonymisierung und Pseudonymisierung weiterhin eine Identifizierbarkeit ermöglicht.[44]

Doch wie wirkt sich all dies auf die Infrastrukturvorhaben wie GAIA-X oder NFDI aus? Konzeptionell sollten die erwähnten Infrastrukturen unter

40 Kritisch *Buccafusco/Weinstein*, Antisocial Innovation, 2023 (630ff, 623f).
41 Art. 1 Abs. 1 EHDS-VO; *Roos/Maddaloni*, RDi 2023, 225 (226).
42 Der Beitrag bezieht sich auf die vorläufige Fassung aus dem Kompromiss des Trilog, siehe https://www.consilium.europa.eu/media/70909/st07553-en24.pdf.
43 *DSK*, Stellungnahme vom 27.3.2023 – auch DuD 2023, 325; im Einzelnen *Denga*, EuZW 2023, 25 (30 f, 32 ff).
44 So *Denga*, EuZW 2023, 25 (30).

dem fragmentierten Verständnis von Privatheit, Datenschutz und Security (nach NIS2-RL und CRA) by Design bzw. Default entsprechende technische Mechanismen zum Schutz der Betroffenen vorsehen. Das wäre je nach Ansatz der Datenweitergabe vor allem mit Blick auf die European Open Science Cloud (EOSC) eine am Einzelfall ausgerichtete Silo-Lösung, in der Datensätze modular und zweckspezifisch freigegeben würden. Wegen der unterschiedlichen Ausrichtung sollten EOSC und GAIA-X unterschiedlich erreichbar sein, also z. B. nicht auf gleichen Servern liegen. Dies betrifft auch anonymisierte Identitäten aufgrund einer möglichen Auflösbarkeit. In der Realität ist GAIA-X vorwiegend als dezentrale Infrastruktur bestehender Partner konzipiert.[45] Der Fokus liegt dabei auf einer Kooperation von Privatwirtschaft, industrienaher Forschung und öffentlicher Hand.[46] Das Konzept des Datenraums von Datenraum Kultur[47] und des Datenraum Mobilität[48] setzt mit einem ähnlichen B2B-Fokus auf die Triebfedern Wertschöpfung, Innovation, Transparenz, Effizienz und Souveränität – und ist damit auf die ökonomische Datensouveränität ausgerichtet. Ergänzend wirkt insoweit die NFDI als Konstrukt, das community-driven aus der Forschung für die Forschung wächst. Im Fokus steht dabei, dass sich die Anforderungen an die Infrastruktur im Sinne einer forschungsbezogenen Datensouveränität aus der Forschung selbst ergeben. Die Umsetzung der aufgezeigten Ansätze geschieht daher stets in einem Spannungsverhältnis zwischen Recht und Bedarf.

Im Hinblick auf die Konzeption von Regulierung und Forschungsdatenräumen lässt sich also die Tendenz erkennen, dass die Infrastrukturen auf die Datenerhebung und -sammlung ausgerichtet sind und von ihr abhängen. Sowohl Forschung als auch der datenbasierte Binnenmarkt können – glaubt man den Rechtsakten – nur erfolgreich sein, wenn Individuen ihre Daten freiwillig und vertrauensvoll teilen oder ihre Daten anonymisiert

45 Im Beitrag von *Lang/Kneuper*, DuD 2022, 778 ist die dezentrale Architektur nur indirekt als „föderaler Dienst […] der Cloud-Dienste kommerzieller Anbieter auf Basis eines einheitlichen Frameworks zu einem komplexen Ökosystem zusammenschließt" beschrieben. In der Konzeption als Datenraum wird die dezentrale Struktur dagegen als Merkmal für Souveränität benannt, siehe *Reiberg/Niebel/Kraemer*, GAIA-X Hub Whitepaper 1/2022: Definition Datenraum, 5.

46 Vgl. *Reiberg/Niebel/Kraemer*, GAIA-X Hub Whitepaper 1/2022: Definition Datenraum, 5f; *Kraemer/Niebel/Reiberg*, GAIA-X Hub Whitepaper 1/2023: Geschäftsmodelle, 9ff.

47 So *Datenraum Kultur*, Projektsteckbrief; Kurzinformation; Factsheet.

48 *Pretzsch* et al., Mobility Data Space – Whitepaper, 2021 (3).

geteilt werden. Damit bewegen sich die Rechtsakte hin zu einer ökonomischen Datensouveränität, ohne die subjektive Datensouveränität merklich zu stärken. Stattdessen wird der Daten-Extraktivismus in Gesetzen und Vorgaben verstetigt. Vor dem aufgezeigten Hintergrund ist ein Recht auf Vergessenwerden und die Rückzugsmöglichkeit als negative Schutzrichtung von informationeller Selbstbestimmung[49] und europäischem Datenschutzgrundrecht (Art. 7, 8 GrCh) nicht mehr zu erkennen, obwohl sie Teil „europäischer Werte" sind. Forschungsdatenräume und Infrastrukturvorhaben müssen sich an den gezeigten Regelungen orientieren, haben aber auf Ebene der Ethik bzw. Forschungsethik noch Spielraum. Die traditionellen Vorgaben sind gewohnt offen formuliert, sodass die Forschung hier eigenhändig das Individuum in den Fokus rücken könnte. Die Forschung bzw. Forscher:innen selbst benötigen hierbei allerdings Unterstützung, um rechtliche Vorgaben zum Schutz der Interessen der Datengebenden auch umsetzen und wahrnehmen zu können. Hieran fehlt es aufgrund der rechtlich wie forschungspolitisch stark ökonomischen Prägung. Infrastrukturen und Forschungsdatenräume sind also bislang datenfreundlich und forschungsorientiert ausgerichtet, aber nicht menschenzentriert bzw. „menschenleer" angelegt.

These 3: Deutsche und europäische Gesetzesvorhaben fangen die Menschenleere nicht auf. Es fehlt an ethischem Bewusstsein.

Wenn die Infrastruktur Nutzer:innen und ihre digitalen Identitäten nicht ausreichend menschengerecht auffängt, liegt der Grund möglicherweise nicht nur in mäßig guten Governance-Strukturen mit geringen Einwirkungsmöglichkeiten. Es ist zu überprüfen, ob die jeweiligen subjektiven Interessen der Datensubjekte durch das Berücksichtigen (forschungs-)ethischer Grundsätze einbezogen werden. Menschenleere Infrastrukturen könnten so doch noch mit menschlichen Werten angefüllt werden.

Die Ansätze dafür sind zahlreich: National benennen diverse Hochschulgesetze die Verantwortung der Forscher:innen, im Rahmen einer Folgenabschätzung „die Anwendung wissenschaftlicher Erkenntnisse in der Praxis" zu berücksichtigen, „die sich aus der Anwendung wissenschaftlicher Erkenntnisse ergeben können."[50] In einigen Bundesländern wie in Berlin und Schleswig-Holstein wird dieses Vorgehen durch das Einbinden einer Ethik-

49 *Vettermann*, Der grundrechtliche Schutz der digitalen Identität, S. 109 mwN.
50 Exempl. § 40 LHG BW.

kommission gestützt.[51] Ethische Prinzipien-Bündel wie CARE[52], OCAP[53] oder FACT[54] sind darin aber nicht explizit erwähnt, sondern dienen höchstens als Leitlinie für die eigene wissenschaftliche Arbeit.[55] Ergänzt wird die Auseinandersetzung mit den Interessen der Beforschten durch die Einbeziehung der DFG-Praxisregeln in das Arbeitsverhältnis per schriftlicher Vereinbarung, um zukünftige Fördergelder aus DFG-Ausschreibungen zu erhalten.[56] Das verfassungsrechtliche Selbstverständnis der Forschung des Art. 5 Abs. 3 GG, der Gesellschaft per Publikation stets zur Erkenntniserweiterung zu verhelfen[57], wird so mittelbar gesetzlich abgesichert.

Politisch wird die Notwendigkeit, sich mit den Folgen der Forschung auseinanderzusetzen, recht lose eingebunden. In der aktuellen *Datenstrategie der Bundesregierung* sollen für die Nutzung pseudonymisierter Daten „angemessene Haftungsregeln und […] faire Ausgleichsregeln" gefunden werden.[58] Zu ethischen Fragen im Rahmen des kommenden Forschungsdatengesetzes äußert sich die Strategie nicht ausdrücklich. Höchstens lässt sich die Abwägung ethischer Interessen in die „verfassungsrechtlichen und unionsrechtlichen Spielräume"[59] hineinlesen. Ethische Aspekte berücksichtigt die Strategie explizit nur für Künstliche Intelligenz.[60] Die Datenstrategie aus dem Jahr 2021 gibt sich da nur minimal genauer, indem sie unter einer verantwortungsvollen Datennutzung „auch die Orientierung an zentralen ethischen Grundsätzen und Prinzipien" versteht. „Bei der Nutzung von Daten ist nicht alles, was technisch möglich ist, auch ethisch vertretbar und politisch wünschenswert. […] Datenrecht und ethische Grundsätze sind keine Bremse, sondern wichtig für den Schutz der Grundrechte und eine verantwortungsvolle Datennutzung."[61] Damit referenziert der Wortlaut das im Jahr 2019 veröffentlichte Gutachten der Datenethikkommission und die

51 *Vettermann/Petri*, RuZ 2023, 5 (19 ff; zur Übersicht aller Länderklauseln S. 21 – Stand April 2023).
52 Für ethische Aspekte indigener Gruppen, siehe https://www.gida-global.org/care.
53 Die Interessen von First Nations adressierende Interessen, siehe https://fnigc.ca/ocap-training/.
54 Für die Data Science, siehe https://redasci.org/.
55 *Vettermann/Petri*, RuZ 2023, 5 (22, 26).
56 *Vettermann/Petri*, RuZ 2023, 5 (12 mwN): faktisch bindende Wirkung.
57 Zum drittnützigen Grundrecht siehe *Vettermann/Petri*, RuZ 2023, 5 (11).
58 *Bundesregierung*, Datenstrategie, 2023 (17).
59 Ebd.
60 *Bundesregierung*, Datenstrategie, 2023 (32).
61 *Bundesregierung*, Datenstrategie, 2021 (7).

darin erläuterten rechtlich-ethisch geprägten Grundsätze.[62] In der jüngsten Datenstrategie fehlen sie allerdings gänzlich.

Die im Frühjahr 2024 veröffentlichte *Strategie für die Internationale Digitalpolitik* der Bundesregierung setzt diesen Zwiespalt aus Fokus auf Individuen und fehlender Konkretheit fort: Unter anderem widmet sich die Strategie der Förderung „menschenzentrierter und innovationsfreundlicher Regeln für den digitalen Raum". Dies soll auch durch „internationale Regeln […] zu ethischen Herausforderungen der Technologienutzung"[63] gelingen, worunter wohl der Fokus auf eine „menschenzentrierte […] Künstliche Intelligenz"[64] zu verstehen ist. Wie bereits im Zusammenhang mit These 1 erwähnt wurde, schließen sich ökonomische Datensouveränität in Form des Datenkapitalismus und eine ethische, menschenzentrierte Perspektive aus. Anders ausgedrückt: In einem innovationgetriebenen Modell findet nur das Individuum Halt, das in einem Datenmarkt über Daten als kapitalisierte Anteile verfügt und diese einbringen kann. Ein Bewusstsein, weitreichende ethische Fragen als Aushandlungs- und Gesprächsraum beispielsweise auch auf den globalen Süden auszurichten, fehlt.[65]

Eine mögliche Erklärung für dieses Ethik-Defizit wäre die Überformung durch europäische Vorgaben, sofern sie Angaben zur Datenethik enthalten und dadurch Lücken auffüllen. Ein erster Anlaufpunkt sind die Strategievorhaben der EU: Die *EU-Datenstrategie (2020)* beabsichtigt, „den Austausch und die breite Nutzung von Daten kanalisieren und gleichzeitig hohe Datenschutz-, Sicherheits-, und Ethik-Standards [zu] wahren."[66] Gemeint sind damit aber die in der Strategie stets genannten „europäischen Werte"[67], gegebenenfalls auch die Stärkung der Selbstbestimmtheit im Umgang mit Daten.[68] Eine konkrete ethische Einbettung fehlt. Die *Digitalstrategie der Europäischen Kommission (2022)* plant grundlegend einen menschenzentrierten Ansatz zur Konzeption des digitalen Europas. Abgesehen von einer „ethischen Nutzung innovativer Technik"[69] gibt es auch hier keine Anzeichen, wie sich die Ethik in der Strategie niederschlägt – weder

62 Gutachten der Datenethikkommission, 2019 (43 ff).
63 *Bundesregierung*, Internationale Digitalpolitik, 2024 (9).
64 Ebd.
65 Vgl. hierzu die Zusammenarbeit mit westlich orientierten Ländern, *Bundesregierung*, Internationale Digitalpolitik, 2024 (8).
66 EU-Datenstrategie, 2020 (4).
67 EU-Datenstrategie, 2020 (1, 5).
68 EU-Datenstrategie, 2022 (11f).
69 Europäische Kommission, Digitalstrategie, 2022 (2).

unter dem Punkt „Digitale Führung" noch in der „Kommissionsweiten Architektur" von Infrastruktur und Governance.[70] Im Gegenteil lässt die *Pressemitteilung zur Errichtung virtueller Welten*[71] erkennen, dass weniger der Mensch in der virtuellen Welt im Mittelpunkt steht als das damit verknüpfte ökonomische Potenzial der Daten. Oder wie die Kommission selbst in der Mitteilung „Virtuelle Welten, die für Menschen geeignet sind"[72] hervorhebt: „Mit einem geschätzten weltweiten Wachstum von 800 Mrd. Euro bis 2030 und potenziellen 860,000 neuen Arbeitsplätzen bis 2025 werden virtuelle Welten den Wirtschafts- und Beschäftigungssektor in der EU verändern."[73] Die in der damit verbundenen Studie herausgearbeiteten Risiken für digitale Identitäten erwähnt die Kommission nicht.[74]

Die EU-Regelungen DGA, DA und der EHDS-VO sind konkrete Umsetzungen dieser Strategien, in denen sich dann Indizien für erwähnte ethische Aspekte und europäische Grundwerte finden müssten. Der DGA enthält hierzu aber kaum Anhaltspunkte. Einzig im Hinblick auf die „Datenspende" bzw. den Datenaltruismus auf Basis einer Einwilligung werden ethische Aspekte angesprochen. Gemäß ErwGr 46 Abs. 2 DGA kann im Kontext von Aufsichtsmechanismen wie einem Ethikrat eine entsprechende Prüfung erfolgen, ob ein datenaltruistisches Modell also „hohe wissenschaftliche Ethikstandards und den Schutz der Grundrechte einhält". Ähnlich enthält der DA keine eigenständigen Hinweise zu ethischen Vorgaben. Wiederholt weist er formelhaft auf die Absicherung „fairer, angemessener und nichtdiskriminierender Bedingungen für die Bereitstellung von Daten"[75] hin. Gemeint ist damit allerdings nicht der Hinweis, Grundrechte natürlicher Personen und Diskriminierungen marginalisierter Gruppen aus ethischen Gründen abzubauen. Verortet ist die Formulierung vielmehr in der Ungleichbehandlung von Marktteilnehmer:innen im B2B-Kontext, hat damit also einen starken wettbewerbsrechtlichen bzw. ökonomischen Bezug.[76] Die EHDS-VO baut auf beiden EU-Gesetzesvorhaben auf und formuliert im Vergleich dazu konkret ethische Maßstäbe. Beispielsweise

70 Europäische Kommission, Digitalstrategie, 2022 (16).
71 EU-Kommission, Pressemitteilung vom 11.6.2023.
72 Siehe https://digital-strategy.ec.europa.eu/de/policies/virtual-worlds.
73 Ebd.
74 EU-Kommission, Extended Reality: Opportunities, success stories and challenges (Health, Education) – Final Report, S. 58f.
75 Beispielsweise Art. 8 Abs. 1, Art. 10 Abs. 1 DA.
76 Vgl. hierzu *Bornkamm/Feddersen*, in: Köhler/Bornkamm/Feddersen, UWG, § 5 Rn. 3.95-97 sowie ErwGr 42 DA.

legen Art. 45 Abs. 2 lit. ha EHDS-VO sowie ErwGr 50 EHDS-VO nahe, im Genehmigungsverfahren zur Sekundärnutzung von Gesundheitsdaten auch Informationen über die Bewertung ethischer Aspekte der Verarbeitung gemäß nationalem Recht einzuholen. Sie referenziert damit das Gesundheitsdatennutzungsgesetz (GDNG). Letztlich ergeben sich hieraus aber auch nur geringe und disziplinspezifische Leitlinien für Forscher:innen selbst, die eigentlich als Bürger:innen von den Gesetzen und Verordnungen betroffen sind.

Die in These 2 aufgezeigte Menschenleere wird folglich auch nicht dadurch gefüllt, dass in politischen Strategien oder nunmehr umgesetzten Gesetzgebungsvorhaben ethische Maßstäbe klarer eingebunden wären. Stattdessen wird sich üblicher legislativer Instrumente zur Stärkung der informationellen Selbstbestimmung und des Datenschutzes bedient: Transparenz durch Information und Berichte, Verantwortlichkeitsketten und Zuständigkeiten oder die Rechtsgrundlage der Einwilligung als bewusstes Entscheidungsinstrument. Die damit verbundenen „europäischen Werte" regeln damit am Menschen vorbei, sowohl an Bürger:innen als Verwalter:innen ihrer digitalen Identitäten als auch an verunsicherten Forscher:innen.

Damit einher geht eine zunehmende Unsicherheit der Forscher:innen im Umgang mit gesellschaftlichen Anforderungen an ihre Arbeit, die aus ethischen Vorgaben erwachsen: Zum einen benennt die Digitalstrategie der Kommission die „digitale Inklusion"[77], die in der Strategie neben der Barrierefreiheit auch die Data Literacy und Zugänglichkeit meinen kann. Inklusion kann insoweit auch bedeuten, entsprechend niedrigschwellig verschiedene Nationalitäten und marginalisierte Gruppen einzubeziehen. Für die CARE-Prinzipien ist die Verständlichkeit und Zugänglichkeit grundlegend, da indigenen Gruppen der Zugang zu westlich-europäischen Datensätzen in öffentlichen Forschungsrepositorien fremd ist. Insofern kann die Darstellung ihrer digitalen Souveränität schaden, wenn ihre Geschichte durch westlich geprägte Metadatenfelder dargestellt und ggf. verkürzt oder entstellt wird. Inklusion und Souveränität gehen also ineinander auf, wenn durch die Zugänglichkeit auch eine Handhabe über die Darstellung der eigenen (kulturellen) Informationen (vgl. Art. 5 lit. d DSGVO – Richtigkeit) geschaffen wird. Durch die bislang geringe Einordnung – strategisch, (forschungs-)politisch und gesetzlich – sind Forscher:innen regelmäßig überfordert und auf niedrigschwellige Gesprächsformate wie den Legal Helpdesk im DFG-geförderten Forschungsprojekt NFDI4Culture angewie-

77 Europäische Kommission, Digitalstrategie, 2022 (2).

sen. Das Benennen und Einbinden ethischer Grundsätze erfordert jedoch das Gegenteil, also die langfristige und nachhaltige Sensibilisierung für ihre Perspektive. Zum anderen werden sensible Themen wie das Loslösen von Sexualität und Gender als ethische und identitätsstiftende Frage kaum adressiert, obwohl dies für Metadaten und Infrastrukturen in bestimmten Bereichen relevant sein kann. Schon die Aufarbeitung von Frauenrollen in den letzten 50 bis 100 Jahren zeigt, dass in bestehenden Datensätzen – auch in öffentlich auffindbaren – ein gender bias vorliegen kann. Verweise auf „hohe Ethik-Standards" greifen da zu kurz, wo das Bewusstsein schon für bestehende ethische Regelungen fehlt. Forscher:innen und Forschungsprojekten ist bislang selten bekannt, wie angemessen und richtig bei Einwilligungen zu informieren ist oder wie Fotografien von Personen persönlichkeitsrechtlich und datenschutzrechtlich zu behandeln sind – trotz zahlreicher öffentlich verfügbarer Handreichungen, Assistenzsysteme und Entscheidungsbäume. Wenn der Mensch im Mittelpunkt der Daten- und Digitalstrategien stehen soll, braucht es auch eine Orientierung und Unterstützung der Forschung bei der Umsetzung ihrer ethischen Verantwortung. In diesem Punkt fehlt es den Umsetzungen politisch und infrastrukturell in der Breite an einem ethischen Bewusstsein.

4. Conclusio

Insgesamt gelingt es den Regelwerken der EU also nicht, die Perspektive von Individuen aktiv und gestärkt einzubinden. Der Beitrag konnte lediglich folgende strukturellen Defizite offenlegen:

Zunächst konnte gezeigt werden, dass das Politikum der Datensouveränität sich nicht als greifbarer Begriff eignet, den grundrechtlichen Datenschutz zu reflektieren. Er dient vielmehr als flexibler Terminus, der eine von Beginn durch ökonomisch-kapitalistische Werte geprägt war. Der Terminus an sich ist damit kein Ansatzpunkt, der die Betroffenenperspektive und grundrechtlichen Datenschutz in Infrastruktur-Vorhaben hineinbringt.

Diese Perspektive schlägt sich in der untersuchten EU-Regulierung nieder: Data Act, Data Governance Act und EHDS-Verordnung enthalten zwar traditionelle Instrumente des Datenschutzes wie Informationspflichten, Meldeprozesse und Zugangsansprüche. Sie sind jedoch eher symbolischer Natur, da sich sowohl die übergeordneten EU-Strategien als auch die Präambeln der Regelungen für eine Wertschöpfung an Daten in der Breite aussprechen. Infrastruktur-Vorhaben wie der EHDS animieren daher

zum Datenteilen und zur Nachnutzung durch die Forschung in jeder Form. Das Individuum bleibt dabei mangels Opt-In – da ein Opt-Out lt. EHDS-Verordnung vorgesehen ist – und einer unbeeinflussten Entscheidung mit eigenen Interessen außen vor.

Die Interessen der betroffenen Personen in Bezug auf ihre digitale Identität werden auch nicht durch ethische Vorgaben aufgefangen. Weder die Strategien noch EU-Regelungen enthalten konkrete Vorgaben für Forscher:innen sowie für Infrastrukturen an sich. An Konzepten zur (langfristigen) Unterstützung von Forscher:innen bei einer ethischen und rechtskonformen Forschung fehlt es ebenso.

Danksagung

Der Verfasser dankt Malte Engeler, Mareike Lisker und Aline Blankertz für den umfänglichen Austausch anlässlich des Redebeitrags auf dem Forum Privatheit 2023.

Literatur

Bisges, Marcel (2017): Personendaten, Wertzuordnung und Ökonomie. *Multimedia und Recht (MMR)*, S. 301-306.

Buccafusco, Christopher J.; Weinstein, Samuel N. (2023): Antisocial Innovation. Georgia Law Review, Duke Law School Public Law & Legal Theory Series No. 2023-42, Cardozo Legal Studies Research Paper No. 723, S. 573-661. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4520979 (besucht am 8.2.2024).

Buchner, Benedikt (2022): Forschungsdaten effektiver nutzen. *Datenschutz und Datensicherheit (DuD)*, 46(9), S. 555-560.

Bundesregierung (2021): Datenstrategie. Berlin: Deutscher Bundestag. URL: https://www.bundesregierung.de/resource/blob/992814/1845634/f073096a398e59573c7526feaadd43c4/datenstrategie-der-bundesregierung-download-bpa-data.pdf?download=1 (besucht am 8.2.2024).

Bundesregierung (2023): Fortschritt durch Datennutzung. Strategie für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung. Berlin: Bundesministerium für Digitales und Verkehr u.a. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2023/datenstrategie.pdf;jsessionid=DC18FD49F90D19C686236DA5A65B0B3C.1_cid505?__blob=publicationFile&v=3 (besucht am 8.2.2024).

Bundesregierung (2024): Strategie für die Internationale Digitalpolitik. Berlin: Bundesministerium für Digitales und Verkehr. URL: https://bmdv.bund.de/SharedDocs/DE/Artikel/K/strategie-internationale-digitalpolitik.html (besucht am 8.2.2024).

Calliess, Christian; Ruffert, Matthias (Hrsg.) (2022): *EUV/AEUV Kommentar*, 6. Auflage. München: C.H. Beck.

Datenethikkommission der Bundesregierung (Oktober 2019): Gutachten der Datenethikkommission. Berlin: Bundesministerium des Innern, für Bau und Heimat. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6 (besucht am 8.2.2024).

Datenraum Kultur (Jan. 2023): Factsheet. URL: https://www.acatech.de/wp-content/uploads/2023/01/Factsheet_Datenraeume_de.pdf (besucht am 8.2.2024).

Datenraum Kultur (Jan. 2023): Kurzinformation. URL: https://www.acatech.de/wp-content/uploads/2023/01/Kurzinformation_Datenraum-Kultur.pdf (besucht am 8.2.2024).

Datenraum Kultur (Jan. 2023): Projektsteckbrief. URL: https://www.acatech.de/wp-content/uploads/2023/01/Projektsteckbrief_Datenraum-Kultur.pdf (besucht am 8.2.2024).

Datenschutzkonferenz des Bundes und der Länder (2023): Stellungnahme vom 27.3.2023 = DuD 2023, 325. URL: https://www.datenschutzkonferenz-online.de/media/st/2023-03-27_DSK-Stellungnahme_EHDS.pdf (besucht am 8.2.2024).

Denga, Michael (2022): Digitale Souveränität durch Datenprivatrecht? *Gewerblicher Rechtsschutz und Urheberrecht (GRUR)*, 124, S. 1113-1120.

Denga, Michael (2023): Die Nutzungsgovernance im European Health Data Space als Problem eines Immaterialgütermarkts. *Europäische Zeitschrift für Wirtschaftsrecht (EuZW)*, S. 25-33.

Digital Autonomy Hub (2021): Policy Brief #4: Digitale Selbstbestimmung. URL: https://digitalautonomy.net/fileadmin/PR/Digitalautonomy/PDF/DAH_Policy_Brief__4_Digitale_Selbstbestimmung.pdf.

Engeler, Malte (2022): Der Konflikt zwischen Datenmarkt und Datenschutz. *Neue Juristische Wochenschrift (NJW)*, 47/2022, S. 3398-3405.

Europäische Kommission (12. Feb. 2020): Datenstrategie. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066 (besucht am 8.2.2024).

Europäische Kommission (30. Juni 2022): Digitalstrategie. URL: https://commission.europa.eu/publications/european-commission-digital-strategy_de (besucht am 8.2.2024).

Europäische Kommission (2023): Extended Reality: Opportunities, success stories and challenges (Health, Education). Final Report. URL: https://op.europa.eu/en/publication-detail/-/publication/f242f605-a82e-11ed-b508-01aa75ed71a1 (besucht am 8.2.2024).

Europäische Kommission (11. Juni 2023): Web 4.0 und virtuelle Welten: Kommission stellt EU-Strategie vor. Pressemitteilung. URL: https://germany.representation.ec.europa.eu/news/web-40-und-virtuelle-welten-kommission-stellt-eu-strategie-vor-2023-07-11_de (besucht am 8.2.2024).

Funk, Axel (2023): Das Prinzip der Nutzerzentriertheit des Data Act – ein gravierender Strukturfehler. *Computer und Recht (CR)*, 7/2023, S. 421-427.

Heesen, Jessica; Ammicht Quinn, Regina; Baur, Andreas; Hagendorff, Thilo; Stapf, Ingrid (2022): Privatheit, Ethik und demokratische Selbstregulierung in einer digitalen Gesellschaft. In: Roßnagel/Friedewald (Hrsg.), *Die Zukunft von Privatheit und Selbstbestimmung*, Wiesbaden: Springer Vieweg, S. 161-188.

Kelber, Ulrich; Bortnikov, Vyacheslav (2023): Digitale Souveränität von Sicherheitsbehörden und Nachrichtendiensten. *Neue Juristische Wochenschrift (NJW)*, 28/2023, S. 2000-2006.

Kraemer, Peter; Niebel, Crispin; Reiberg, Abel (2023): GAIA-X Hub Whitepaper 1/2023: Geschäftsmodelle. URL: https://gaia-x-hub.de/wp-content/uploads/2023/02/Whitepaper-Gaia-X-Geschaeftsmodelle.pdf (besucht am 8.2.2024).

Krüger, Philipp-L. (2016): Datensouveränität und Digitalisierung. *Zeitschrift für Rechtspolitik (ZRP)*, 7/2016, S. 190-192.

Lang, Simon; Kneuper, Ralf (2022): Datenschutz und Informationssicherheit in Gaia-X. *Datenschutz und Datensicherheit (DuD)*, 46(12) S. 778-781.

Lisker, Mareike (2023): Von der (Un-)Möglichkeit, digital mündig zu sein. Masterarbeit, TU Berlin. URL: https://depositonce.tu-berlin.de/items/ab50df77-b748-4ea3-8dbc-b5afc1ef9574 (besucht am 8.2.2024).

Medizininformatik-Initiative AG Consent (2019): Stellungnahme zu patientenindividueller Datennutzungstransparenz und Dynamic Consent. URL: https://www.medizininformatik-initiative.de/sites/default/files/2019-09/MII_AG-Consent_Stellungnahme-Consent-Modelle_v05.pdf.

Müller, Johannes (2021): Der „digitale Zwilling". *ZD-Aktuell*, Nr. 05096.

Pretzsch, Sebastian; Drees, Holger; Rittershaus, Lutz; Schlueter Langdon, Christoph; Lange, Christoph, Weiers, Christian (2021): Mobility Data Space – Whitepaper. URL: https://www.mobility-data-space.de/content/dam/ivi/mobility-data-space/documents/Mobility_Data_Space_DE_20220603_web.pdf besucht am 8.2.2024).

Pohle, Julia; Thüer, Leo; Dammann, Finn; Winkler, Jan (2020): Das Subjekt im politischen Diskurs zu „digitaler Souveränität". In: Kersting, Norbert; Radtke, Jörg; Baringhorst, Sigrid (Hrsg.): *Handbuch Digitalisierung und politische Beteiligung*. Wiesbaden: Springer VS, S. 1-23.

Reiberg, Abel; Niebel, Crispin; Kraemer, Peter (2022): GAIA-X Hub Whitepaper 1/2022: Definition Datenraum. URL: https://gaia-x-hub.de/wp-content/uploads/2022/10/20220914_White_Paper_22.1_Definition_Datenraum_final.pdf (besucht am 8.2.2024).

Roos, Philipp; Maddaloni, John-Markus (2023): Regulierter Datenaustausch zur Gesundheitsforschung. *Recht Digital (RDi)*, S. 225-232.

Rosenkranz, Frank; Scheufen, Marc (2022): Die Lizenzierung von nicht-personenbezogenen Daten: Eine rechtliche und rechtsökonomische Analyse. *Zeitschrift für Digitalisierung und Recht (ZfDR)*, 2(2), S. 159-198.

Roßnagel, Alexander (2023): Digitale Souveränität im Datenschutzrecht. *Multimedia und Recht (MMR)*, 26(1), S. 64-68.

Samardzic, Darko; Becker, Thomas (2020): Die Grenzen des Datenschutzes – Der beschränkte Schutz durch Freiwilligkeit und Einwilligung bei Corona-Apps. *Europäische Zeitschrift für Wirtschaftsrecht (EuZW)*, 15/2020, S. 646-654.

Schütrumpf, Moritz; Person, Christian (2022): Gaia-X: Vernetzte Infrastrukturen für eine europäisch geprägte Datenwirtschaft. *Recht Digital (RDi)*, S. 281-288.

Spitz, Markus; Cornelius, Kai (2022) Einwilligung und gesetzliche Forschungsklausel als Rechtsgrundlagen für die Sekundärnutzung klinischer Daten zu Forschungszwecken. *Medizinrecht (MedR)*, 40(3), S. 191–198. URL: https://doi.org/10.1007/s00350-022-6136-7.

Umweltbundesamt (2023): Digitale Kommune/Digitale Region, Texte 62/2023. URL: https://www.umweltbundesamt.de/publikationen/digitale-kommunedigitale-region (besucht am 8.2.2024).

Vettermann, Oliver (2022): Der grundrechtliche Schutz der digitalen Identität. Dissertation, Universität Leipzig. URL: 10.5445/KSP/1000148103 (besucht am 8.2.2024).

Vettermann, Oliver; Petri, Grischka (2023): Should I CARE about FAIR? – Ein rechtlicher Blick auf die Prinzipien des Forschungsdatenmanagements, *Recht und Zugang (RuZ)*, 4(1), S. 5–29. DOI: 10.5771/2699-1284-2023-1-5 (besucht am 8.2.2024).

Drei Wünsche an die Datenpolitik – aus Sicht einer Dateninfrastruktur

Stefanie Fuchsloch, Wolf Zinke, York Sure-Vetter

Zusammenfassung

Die Nationale Forschungsdateninfrastruktur (NFDI) e.V. hat die Vision: „Daten als gemeinsames Gut für exzellente Forschung, organisiert durch die Wissenschaft in Deutschland".[1] Um diese Vision zu verwirklichen, richtet NFDI folgende drei Wünsche an die Datenpolitik: Erstens benötigt der Aufbau neuer Infrastrukturen Vertrauen und eine langfristige Finanzierung, da es nicht nur um technische Dienste und Angebote geht, sondern um sämtliche organisatorische Prozesse und forschungsrelevante Methoden (RfII 2016, S. 12). Für den Austausch und die Vernetzung ist die Standardisierung in einer Infrastruktur „zwingende Voraussetzung", weswegen neben der Hardware auch die „Menschen, Praktiken und Software" zentral sind (Strecker et al. 2023, S. 41f.). Zweitens, da der sichere Datenaustausch weitere Innovationschancen für die verschiedenen Datenakteure wie Wissenschaft, Wirtschaft oder Zivilgesellschaft bietet, braucht es standardisierte Prozesse gerade in der Datenbereitstellung und dem Datenzugang. Dadurch mindern sich die Risiken für die verschiedenen Beteiligten durch klare rechtliche Rahmenbedingungen, z. B. hinsichtlich des Zugangs zu den Daten, ihrer Sicherung und Weitergabe (NFDI 2022). Aufgrund standardisierter Datenformate und Authentifizierungssysteme können Daten, Analyseverfahren und entsprechende Software ausgetauscht und ggf. verknüpft werden. Drittens sollen gemeinsame Werte wie Privatsphäre, Selbstbestimmung und Informationen zur Datennutzung durch ein FAIRes Datenökosystem auch durch die Datenpolitik wirksam geschützt werden. Dazu bedarf es einer Aufgabenvielfalt für verschiedene Datenakteure in Wissenschaft, Wirtschaft und Zivilgesellschaft, um so Datenmonopole zu verhindern und eine allgemeine Zugänglichkeit zu gewährleisten. Daher sind die Gesetzgeber aufgefordert, für Forschende erfüllbare Rahmenbedingungen zu schaffen, so dass vertrauensvolle Dateninfrastrukturen eta-

1 https://www.nfdi.de

bliert werden können, z.B. das Recht auf Forschungsgeheimnis (RatSWD 2022).

1. Notwendigkeit der drei Wünsche an die Datenpolitik

Die Anforderungen an die Datenpolitik für das 21. Jahrhundert sind vielseitig und dringlich. Daten werden heute als Rohstoff für vielfältige technische und soziale Innovationen und letztlich für immer mehr wertschöpfende Prozesse gesehen. Mit dem Aufbau der Nationalen Forschungsdateninfrastruktur (NFDI) soll dazu in Deutschland der Zugang zu Forschungsdaten über alle Wissenschaftsbereiche verbessert werden. Intuitiv klar ist, dass der Aufbau einer neuen Infrastruktur von Beginn an ein langfristiges Commitment erfordert, um schrittweise das Vertrauen in die Infrastruktur zu etablieren. Gerechte Möglichkeiten des Datenaustauschs sind dabei ein unerlässlicher Bestandteil für die Innovationschancen in Wissenschaft, Wirtschaft oder Zivilgesellschaft. Für einen effizienten Datenaustausch ist es essentiell, dass die Daten nachhaltig auffindbar (*findable*), zugänglich (*accessible*), interoperabel (*interoperable*) und wiederverwendbar (*reusable*) ausgestaltet sind, was das Ziel der FAIR-Prinzipien ist (Wilkinson et al. 2016). Mit der allgemeinen Verfügbarkeit von Daten zunehmend verknüpft ist zudem, dass gemeinsame Werte und Grundrechte, wie Privatsphäre und Schutz von personenbezogenen Daten, wirksam geschützt werden.

Die Verbesserung der Nachnutzung von Daten hat für wissenschaftliche Entdeckungen und Innovationen ein enormes Potential, da zunehmend neue Erkenntnisse in der Forschung durch die Verwendung von bereits bestehenden Daten gewonnen werden. Auch unter ökonomischen Aspekten ist dies bedeutend: Die EU-Kommission schätzt die jährlichen Kosten dafür, dass bei der Bereitstellung von Forschungsdaten die FAIR-Prinzipien nicht umgesetzt werden, auf ca. 26 Milliarden Euro (EU-Kommission 2018, S. 4). Eines der größten Hindernisse ist dabei noch immer, die richtigen Daten-sätze zu finden, zu verstehen und für die eigene Zwecke nutzbar zu machen. Um dies zu lösen, wurde der NFDI-Verein[2] mit dem Ziel gegründet, einen Wissensspeicher aufzubauen, mit dem wertvolle Datenbestände aus der Forschung systematisch erschlossen und vernetzt werden. Dies

2 Aus diesem Grund empfahl der Rat für Informationsinfrastrukturen (RfII 2016, S. 2) im Bericht „Leistung aus Vielfalt" den Gesetzgebern, eine „netzwerkförmige, dynamische Struktur" mit verschiedenen Service- und Kompetenzzentren der diversen Wissenschaften aufzubauen. Abrufbar hier: https://rfii.de/?p=1998 [26.05.2023].

schafft eine weitere und unverzichtbare Grundlage für ein erfolgreiches und effizientes deutsches Wissenschaftssystem (Sure-Vetter et al. 2021). Die Aufgabe wird durch ein dezentrales NFDI-Netzwerk disziplinübergreifend wahrgenommen, in das die existierenden Einrichtungen eingebunden werden (RfII, S. 40f.).

Mit dieser neuen Forschungsdateninfrastruktur werden für unsere Gesellschaft immense Möglichkeiten eröffnet, was sich z. B. in der Genomforschung zeigt: Gerade seltene genetische Erkrankungen lassen sich nur schwer erforschen, weil ein Zusammenschluss der wenigen vorhandenen Datensätze fehlt - moderne (KI-gestützte) Methoden benötigen aber eine hinreichend große Datengrundlage für das Identifizieren von Zusammenhängen und somit auch die Entwicklung von Therapiemöglichkeiten (siehe GHGA[3]).

Um diesem und weiteren Spannungsfeldern zu begegnen, arbeiten im NFDI-Netzwerk aktuell 26 Fach- und Methodenkonsortien[4] daran, die Expertisen der unterschiedlichen Wissenschaftsdisziplinen zu vernetzen und zu bündeln. Auf der einen Seite entwickeln die Konsortien fachspezifische Lösungen für ihre Disziplin, auf der anderen Seite stehen sie im Verein in einem aktiven Austausch, um an disziplinübergreifenden Themen zu arbeiten. In derzeit fünf NFDI-Sektionen[5] erarbeiten Vertreter:innen aus verschiedenen Wissenschaftsdisziplinen fachübergreifende Lösungen für gemeinsame Herausforderungen. Die einzelnen Sektionen fokussieren sich dabei auf unterschiedliche Themen, seien es Herausforderungen im infrastrukturellen Bereich, auf Metadaten bezogen, rechtliche Aspekte betreffend, kompetenzbildend oder im Austausch mit weiteren Akteuren zum Beispiel aus der Wirtschaft. Das Basisdienstkonsortium Base4NFDI[6] fokussiert sich auf die Entwicklung gemeinsamer fachübergreifender Dienste wie IAM4NFDI[7] als Zugriffsmanagementsystem oder PID4NFDI[8] für eine dauerhafte Referenzierung von Datensätzen.

Der Bedarf an Fachkenntnissen in der Datenkompetenz steigt entsprechend auf allen Ebenen des Datenlebenszyklusprozesses, d. h. von der Erfassung der Rohdaten, zur Aufbereitung der Daten, um diese analysieren

3 https://www.ghga.de/de/
4 https://www.nfdi.de/konsortien/
5 https://www.nfdi.de/sektionen/
6 https://base4nfdi.de/
7 IAM4NFDI: IAM: Identity- und Access-Management, siehe: https://base4nfdi.de/projects/iam4nfdi
8 PID: Persistent Identifier, siehe https://base4nfdi.de/projects/pid4nfdi

zu können, bis hin zur Nachbereitung von Daten, um diese nachhaltig auffindbar auszugestalten. Jene unterstützenden Vorgänge müssen dezentral in den (Forschungs-) Einrichtungen etabliert werden, z. B. durch Fachpersonal wie FDM-Specialists; gleichzeitig besteht ein Bedarf an zentralen Strukturen aus technischer, organisatorischer und regulatorischer Sicht, insbesondere für die Nachnutzung von Daten in interdisziplinären Forschungsvorhaben. Ziel des NFDI-Vereins ist es gemäß § 2 Abs. 3 der NFDI-Satzung[9], eine „koordinierte, vernetzte Informationsinfrastruktur […] mit verlässlichen Diensten und Angeboten" zur Verfügung zu stellen und daher einen „standardisierten Umgang mit Forschungsdaten" und der flächendeckenden „Entwicklung disziplinübergreifender Metadatenstandards" zu schaffen. Um die (Daten-) Wertschöpfung für den Wissenschaftsstandort Europa zu steigern, wurden in den letzten Jahren zahlreiche EU-Rechtsakte erlassen, durch die die europäischen Datenstrategie, eine „branchenübergreifende Datenweitergabe zum Nutzen von Unternehmen, Forschenden und öffentlichen Verwaltungen" zu verwirklicht (EU-Kommission o. D.). Schätzungen besagen, dass die Datenwirtschaft im Jahr 2025 bereits 829 Milliarden Euro an Wert in der EU haben wird (EU-Kommission o. D.). Für Forschende haben diese Rechtsakte eine immense Relevanz, denn sie regeln Datenzugänge, z. B. im Data Act[10] oder Digital Services Act[11]. Allerdings erfordern die Rechtsakte auch entsprechende Umsetzungen auf nationaler Ebene, die aber noch andauern. Auch auf deutscher Ebene ist die im August 2023 durch das Bundeskabinett verabschiedete Datenstrategie mit dem Ziel angetreten, Daten effektiver zu nutzen (Bundesregierung 2023), z. B. durch das Datennutzungsgesetz und das Gesundheitsdatennutzungsgesetz.

Um Daten nachhaltig zu nutzen, gilt es, einige Faktoren zu beachten, weshalb der NFDI-Verein in den folgenden Unterkapiteln drei Wünsche an die Datenpolitik formuliert.

9 https://www.nfdi.de/wp-content/uploads/2021/05/Satzung-NFDI-eV.pdf
10 Data Act: Verordnung EU/2023/2854 vom 13.12.2023: OJ L, 2023/2854, 22.12.2023.
11 Digital Services Act: Verordnung EU/2022/2065 vom 19.12.2922: *OJ L 277, 27.10.2022, p. 1–102.*

2. Erster Wunsch: Dem Aufbau von Infrastrukturen muss das dauerhafte Commitment folgen.

Infrastrukturen stellen essentielle Rahmenbedingungen für die Funktionsfähigkeit eines Landes oder einer Organisation dar. Dabei umfassen Infrastrukturen nicht nur physische Strukturen wie Straßen- oder Eisenbahnnetze, sondern beinhalten zudem auch deren Management, damit verbundene Qualifikationen und vor allem das personelle Know-how, um die Einbindung und Koordination in bestehende Systeme zu gewährleisten. Eine eindeutige Abgrenzung verschiedener Infrastrukturen zueinander ist oft schwierig, da diese meist eng miteinander verzahnt sind und einander gegenseitig bedingen. Die Infrastrukturen sind ein wichtiger Teil der Daseinsvorsorge, die die Grundlage für die Lebensqualität und wirtschaftliche Entwicklung eines Landes liefern, weshalb es im Interesse des Staates ist, nicht nur für den Aufbau relevanter Infrastrukturen zu sorgen, sondern zudem auch den Erhalt der Infrastruktur sicherzustellen. Gut funktionierende Infrastrukturen werden oftmals nicht richtig wahrgenommen, erst bei einem Ausfall wird die Relevanz erkannt (z. B. Internetstörung, Brückensperrung, Stromausfall) (Star & Ruhleder 1996, S. 4f.).

Im Bereich der Wissenschaft sind Forschungsinfrastrukturen die notwendigen Grundvoraussetzungen zur Durchführung von verschiedenen Forschungsaktivitäten. Unter Forschungsinfrastrukturen fallen unter anderem die Laboratorien mit ihren Forschungsgeräten, Rechenzentren und Bibliotheken. Gerade in diesem Bereich wird deutlich, dass der entsprechenden Fachkompetenz und dem effizienten interpersonellen Austausch der beteiligten Personen eine hohe Bedeutung zukommt, denn ohne diese verlieren Forschungsinfrastrukturen ihre Funktion. Ein Staat, der den Wert von Forschung und Bildung erkannt hat, sollte entsprechend Ressourcen aufbringen, um gut funktionierende Forschungsinfrastrukturen aufrechtzuerhalten, damit Forscher:innen in der Lage sind, wertvolle und aussagekräftige Daten in ihren Experimenten zu erheben.

Zwei Formen von Infrastrukturen, die im Rahmen der Digitalisierung an Bedeutung gewonnen haben und derzeit entsprechend weiter aufgebaut werden, sind Informations- und Dateninfrastrukturen.

Informationsinfrastrukturen sind nicht nur technische Dienste und Angebote, sondern sämtliche organisatorischen Prozesse und forschungsrelevanten Methoden (RfII 2016, S. 12). Für den Austausch und die Vernetzung ist die Standardisierung in einer Infrastruktur „zwingende Voraussetzung" weswegen neben der Hardware auch die „Menschen, Praktiken und Soft-

ware“ zentral sind (Strecker u.a. 2023, S. 41f.). Dementsprechend umfassen Dateninfrastrukturen neben Informationsinfrastrukturen auch Services (inkl. Hard- und Software) für die Nutzung und Speicherung von Daten. Zu diesen Services gehören weitere Akteure wie Rechenzentren, Archive, Initiativen etc. Der Austausch mit diesen Akteuren ist grundlegend, um bestehende Lösungsmodelle auch für andere zu adaptieren. Die Bedeutung und der Bedarf nach einem Austausch zu diesen Themen zeigte sich zum Beispiel bei der ersten Conference on Research Data Infrastructure (CoRDI), die im September 2023 in Karlsruhe stattfand und mit fast 700 Teilnehmenden sehr gut besucht war.

2.1 Eine Infrastruktur durch Aufgabenvielfalt

Die Vision des NFDI-Vereins[12] lautet: „NFDI: Daten als gemeinsames Gut für exzellente Forschung, organisiert durch die Wissenschaft in Deutschland“. Das bedeutet unter anderem, bestehende Datensilos abzubauen und digitale Daten verfügbar und verknüpfbar auszugestalten, weil der digitale Wandel den Wissenschaften neue Möglichkeit bietet (DFG 2020). Inzwischen werden in der Wissenschaft Daten meist digital erhoben, doch auch für die Forschung, die auf analogen Informationen wie archäologischen Artefakten, Bodenproben etc. beruhen, ist eine Überführung in eine digitale Repräsentation Voraussetzung, um durch größere oder verknüpfte Datensätze den wissenschaftliche Erkenntnisgewinn zu befördern. Dadurch kann z. B. das Verständnis von Mikroorganismen erweitert (siehe NFDI4Microbiota), schnelleres Kunststoff-Recycling entwickelt (siehe NFDI4Chem) oder Kulturerbstätten digital kartiert werden (siehe NFDI4Objects). Gemeinsame Lösungen sind dabei wichtig, weil es neben Standardisierungen und technischer Umsetzung, auch um eine „rechtliche Infrastruktur“ geht (Hennemann et al. 2024), welche den Datenlieferant:innen und Nutzer:innen ihre Rechte (z.B. auf Privatsphäre, auf Information, auf Selbstbestimmung) gewährleistet und für die Forschung durch datenschutzrelevante Einwilligungen, Ethikkomitees oder Datenspenden essentielle Aufgabenbereiche sind.

Es sollte daher auch das Ziel der Datenpolitik sein, die Interessen des Einzelnen und die Aufgabenvielfalt der Datenakteure (wie NFDI, Forschungsdatenzentren (FDZ), Rechenzentren, Archive) zu gewährleisten.

12 https://www.nfdi.de/verein/

Durch gegenseitige Kontrolle und unterschiedliche Verantwortlichkeiten sind die Daten nicht nur zentral für Wenige verfügbar, womit aktiv der Entstehung von Datenmonopolen entgegengewirkt wird. Entsprechend sollten Infrastrukturen für Akteure des Gemeinwohls – wie es öffentliche Forschungseinrichtungen, Nicht-Regierungs-Organisationen (NGOs) oder Medien sind – zugänglich sein, um datenbasierte Innovationen und datenbasierte Kontrollmechanismen zu gewährleisten. Denn in einem föderierten System bedarf es gemeinwohlorientierter Datenakteure wie NFDI oder FDZ, um Daten aufzufinden und Zugang entsprechend dem Schutzgehalt der Daten zu erhalten. Dabei steigt der Arbeitsaufwand für die Langzeitarchivierung von Datensätzen und aufgrund der oftmals disziplinspezifischen Standards und Konzeptionierungen sind die Datensätze für zukünftige interessierte (Wissenschafts-)Communitys schwer zugänglich (für Biosammlungen: Bishop & Hank 2016, S. 7). Obgleich bedarf es einer zuverlässigen Langzeitarchivierung von relevanten Datensätzen wie z. B. Zeitzeugen-Interviews oder aufwendig erhobener Daten von Versuchsfahrzeugen mit (kostspieligen) Laserscannern und Kameras (siehe NFDI4Ing). Die Aufgaben entlang des Datenlebenszyklus sind von verschiedenen Datenakteuren organisatorisch, technisch und personell mit gemeinsamen Schnittstellen und Regeln (wie Metadaten und standardisierten Prozessen) auszugestalten, um „energieeffiziente, sichere und moderne Dateninfrastrukturen" (BMBF 2023) langfristig zu gewährleisten.

2.2 Verstetigung von Forschungsdateninfrastrukturen

Um Planungssicherheit für Forschungseinrichtungen zu schaffen, bedarf es einer verlässlichen Forschungsdateninfrastruktur, die über eine nachhaltige Finanzierung verfügt, um so den Datenaustausch langfristig gesichert ausgestalten zu können (SPD-Arbeitsgruppe 2023).

(1) „May all your problems be technical" [... mit Infrastrukturen ...] wird Jim Gray[13] von Prof. Borgman (2023) zitiert, denn Infrastrukturen besitzen zusätzlich zu den technischen auch lokale, soziale und globale Dimensionen, z. B. bei der Einbettung in andere Systeme (Star &

13 Turing Award Gewinner für seine Forschungsverdienste im Bereich Datenbanken und Transaktionsverarbeitung sowie technische Führung bei der Systemimplementierung: https://amturing.acm.org/award_winners/gray_3649936.cfm.

Ruhleder 1996, S. 5). Daraus ergeben sich laut Borgman (2023) weitere Fragen: Welche Daten sind nachnutzbar und wie? Welche Ressourcen gibt es? Welche Governance wird geschaffen? Welche Risiken gibt es? Wissenschaftsdisziplinen haben unterschiedliche Sprachen, Vokabulare, rechtliche Unterschiede, sodass die Disziplinen ihr Fachverständnis übersetzen müssen, um gemeinsame Lösungen für diese Fragestellungen zu finden. Das Urheberrecht ist zentral bspw. für Bilder- und Textkorpora, weniger hingegen für Labordaten der Chemie. Infrastrukturen und Datenmittler, wie es Datenräume sind, benötigen daher zuverlässige Strukturen und Governance[14].

(2) Forschungsdaten und Auswertungssoftware sind Ergebnisse der Forschungsarbeit (bspw. zu Castell et al. 2024), jedoch nicht gleichermaßen prestigeträchtig wie Publikationen in Fachzeitschriften. Es bedarf eines Kulturwandels in der Wissenschaft, um auch die Veröffentlichung von Forschungsdatensätzen als wichtigen Beitrag für die Wissenschaft anzuerkennen. Außerdem benötigt es die Entwicklung einer guten Fehlerkultur, denn Forschende schrecken vor der Veröffentlichung ihrer Forschungsdatensätze aus Furcht zurück, dass Unstimmigkeiten in den Daten und Analysen festgestellt werden könnten. Dabei könnte ein Lernen am eigenen Datensatz durch nachnutzende Forschende ermöglicht werden, wodurch Open Science stärker gelebt würde (Herres-Pawlis et al. 2022, S. 2).

(3) Sichere und effiziente Dateninfrastrukturen sind letztlich das Fundament für einen gesicherten Datenaustausch; nur mit dem langfristigen Ausbau, der Koordination der Infrastruktur-Akteure und einer verlässlichen Finanzierung kann Vertrauen in den Datenaustausch auch für andere Datenakteure wie Wirtschaftsunternehmen geschaffen werden (Stüwe 2023, ähnlich Riphan 2023). Schließlich sind Services in der Datensicherheit oder Authentifizierungsstruktur stetig weiter zu entwickeln und zu pflegen. Bereits die EU-Expertengruppe zu Data Sharing kritisierte, dass fehlendes Vertrauen der Datenakteure aufgrund von Intransparenz, mangelnder Datenkompetenz und der Abwesenheit ethischer Ansätze das größte Hindernis im Datenaustausch seien (EU-Kommission 2020, S. 8, 49ff.).

Ziel ist es, Forschende zu befähigen, Daten gemäß der FAIR-Prinzipien zu erheben und zu speichern, sodass auch andere auf ihre Forschungsdaten

14 Siehe hierzu auch der Beitrag von Reiberg, Niebel und Schmitz in diesem Band.

ohne zeitaufwendige Datenaufbereitung zurückgreifen können. So können aus diesen bestehenden Forschungsdatensätzen neue verknüpfte, aufbereitete Datensätze entstehen, die wiederum weiterverwendet werden können. Um die bestmögliche Lösung für die Datensätze zu finden, müssen ausreichend Unterstützungsangebote wie Helpdesks der NFDI-Konsortien oder entsprechende Workshops[15] bereitgestellt werden.

3. Zweiter Wunsch: Innovationschancen für alle durch gerechten Datenaustausch

Daten aus den verschiedenen Wissenschaftsdisziplinen und Wirtschaftssektoren sind unterschiedlich in ihren Charakteristika und Interpretationsvorgehensweisen und liegen oftmals als dezentrale, unstrukturierte Datensätze ab, sodass sie nur mit unverhältnismäßigem Aufwand nachnutzbar sind. Dabei teilen die verschiedenen Datenakteure ähnliche Sorgen beim Datenaustausch: Der Verlust vor der Datenkontrolle, Haftungsrisiken, Reputationsverluste, Rechtsverstöße im Bereich des Datenschutzes, des Vertragsrechts (siehe Non-Disclosure Agreements) oder dem Recht auf geistiges Eigentum. Die hohen administrativen Aufwände für die Rechteklärung eines Datenzugangs belasten insbesondere kleinere und mittelständische Unternehmen sowie kleinere Forschungseinrichtungen. Die Rechtsunsicherheiten sind unterschiedlicher Natur, von oftmals heterogenen oder fehlenden Zugangsregeln, bis hin zu einer Vielzahl an bereichsspezifischen Regelungen wie im Sozial-, Archiv- und Urheberrecht (NFDI-Sektion ELSA 2023, S. 12, RatSWD 2023). Diese Verständigungshürde wird durch unterschiedliche föderale Handhabungen und Zusammenarbeit, z. B. im Registerrecht und Datenschutz, verstärkt (Sachverständigenrat 2023, S. 12; zu Registerdaten: RatSWD 2023). Im Jahresgutachten 2023 kritisieren die Wirtschaftsweisen, dass belastbare Aussagen zu relevanten Themen aufgrund einer fehlenden Dateninfrastruktur scheitern (Sachverständigenrat 2023, S. 389ff.).

Standardisierte Prozesse, gerade in der Datenbereitstellung, mindern die Risiken für die verschiedenen Beteiligten durch klare rechtliche Rahmenbedingungen, z. B. hinsichtlich des Datenzugangs, der Datensicherheit und -weitergabe (NFDI 2022). Aufgrund standardisierter Datenformate

15 wie bspw. der Workshop von Text+: „Wohin damit? Storing and reusing my language data", siehe Bericht: https://textplus.hypotheses.org/6074.

und Authentifizierungssysteme können Daten, Analyseverfahren und entsprechende Software ausgetauscht und ggf. verknüpft werden. Dabei gilt es, die Schutzgehalte von Daten wie Geheimnisschutz zu beachten und sensible personenbezogene Daten wie politische Einstellungen oder sexuelle Orientierung zu schützen, indem spezielle Zugangsmöglichkeiten genutzt werden. Das Five-Safes-Modell[16] zeigt zum Beispiel anhand von fünf Risikodimensionen die empfohlene Art des Datenzugangs auf. So verwenden auch die Forschungsdatenzentren bereits – je nach Datensensibilität – verschiedene Zugriffsmöglichkeiten auf Daten. Auf der anderen Seite müssen die Pflichten wie die Verantwortung der Datensicherheit, -schutz, Anonymisierung oder auch Ausschluss von kommerzieller Nutzung geregelt sein. An dieser Stelle spielen bei sensiblen Daten die verschiedenen Datentreuhand-Modelle sowie Datenräume zunehmend eine größere Rolle[17]. Für gemeinwohlorientierte Forschung sollte der Datenzugang nur „in gut begründeten Ausnahmefällen" verwehrt werden (Stüwe 2023); denn die Erkenntnisse kommen allen zu Gute (NFDI-Sektion ELSA 2023a, S. 2).

3.1 Herausforderungen für die Datennutzung aus dem Blick des Datenschutzes

Im Bereich der Forschung mit personenbezogenen Daten gibt es durchaus bereits Privilegien für die Forschung in verschiedenen Rechtsbereichen (Hilgendorf 2023, Podszun 2023, Specht-Riemenschneider 2021), wenngleich die Suche nach der korrekten gesetzlichen Grundlage für Forschende enorme Unsicherheiten birgt; nicht zuletzt aufgrund der möglichen Sanktionen (Boehm & Hallinan 2023, S. 36). Datenschutzrechtliche Einwilligungen sind ein Instrument, mit dem betroffene Personen über ihr Recht auf Selbstbestimmung informiert werden. Im Forschungsumgang mit personenbezogenen Daten sind Einwilligungen ein Instrument, um Personen über die Verwendung der Daten und ihre Rechte wie Widerruf zu informieren. Forschende, die mit personenbezogenen Daten in Forschungsprojekten arbeiten, werden bei der Erstellung solcher Einwilligungen für die

16 Siehe: https://ukdataservice.ac.uk/help/secure-lab/what-is-the-five-safes-framework/

17 Siehe auch der Beitrag von Püschel & Lassak (2023) auf der Jahreskonferenz der Plattform Privatheit. https://plattform-privatheit.de/p-prv-wAssets/Assets/Jahreskonferenz2023/Praesentation/Pueschel_Zukunftsmodell-Datentreuhaender.pdf

jeweiligen Forschungsteilnehmenden tlw. durch virtuelle Assistenten wie das Tool IVA2[18] des Konsortiums BERD@NFDI unterstützt.

Die Datenbereitstellung für die Sekundärnutzung ist dabei besonders komplex aufgrund nationaler Unterschiede. Es bleibt zu klären, inwiefern es einer neuen Rechtsgrundlage bedarf, wenn die weitere Verarbeitung nicht mehr mit dem primären Zweck als vereinbar angesehen wird (Boehm & Hallinan 2023, S. 39f., Specht-Riemenschneider 2021, S. 28ff.). Nach der Datenschutzgrundverordnung (DSGVO)[19] ist es zwar möglich, im Rahmen des öffentlichen Interesses eine Änderung des Verwendungszweckes für Archivzwecke, Forschungszwecke oder statistische Zwecke vorzunehmen, dieser muss aber mit dem ursprünglichen Zweck der Daten vereinbar sein (Specht-Riemenschneider 2021, S. 31). Problematisch ist auch die Verknüpfung verschiedener Datensätze, weil die gesetzlichen Erlaubnisgrundlagen in den jeweils relevanten Gesetzen fehlen (Sachverständigenrat 2023, S. 393ff.; RatSWD 2023, S. 2ff.).

So sind die Überschneidungen von der DSGVO mit dem Bundesdatenschutzgesetz (BDSG) sowie mit zahlreichen Landesgesetzen „selbst für Experten nicht immer [in einer] durchsichtigen Weise" (Hilgendorf 2023, S. 59), weswegen der scheidende Bundesdatenschutzbeauftragte Kelber[20] für die Sekundärnutzung eine „länderübergreifende, einheitliche Regelung" empfiehlt, da Forschung dem Gemeinwohl dient und somit im öffentlichen Interesse ist (Kelber, 2023, S. 19). Nichtsdestotrotz müssen die Rechte von Forschungsteilnehmenden, deren personenbezogene Daten verwendet werden, mit den Privilegien für die Forschung in Einklang gebracht werden, denn auch hier gibt es Pflichten wie die Datenminimierung oder frühzeitige Pseudonymisierung, bzw. besser eine Anonymisierung durch unabhängige Stellen (Kelber 2023, S. 19). Ziel sollte es stets sein, die Forschungsteilnehmenden, deren personenbezogene Daten genutzt werden, als Betroffene miteinzubeziehen, denn je höher die Gefahr der Re-Identifizierung, desto höher die Transparenzverpflichtungen. Das bedeutet, dass Forschende technische und organisatorische Sicherheitsmaßnahmen umsetzen sollten, die überprüfbar sein müssen – ergo müssen Mindeststandards festgelegt sein. Für die Sekundärnutzung könnten auch Datenzugangsansprüche für die Forschung maßgeblich durch Forschungsklauseln erleichtert werden (Specht-Riemenschneider 2021, S. 27ff.).

18 Siehe: https://www.berd-nfdi.de/iva2/

19 Datenschutzgrundverordnung: EU/2016/679. *OJ L 119, 4.5.2016, p. 1–88.*

20 Amtszeit 7. Januar 2019 bis voraussichtlich 6. Juli 2024

Ziel des Forschungsdatengesetzes sollte es daher sein, Forschung und Datenschutz auszubalancieren und bestehende Defizite beim Datenzugang und der -verknüpfung zu beheben. Die Herausforderung des Datenschutzes ist zwar nur auf personenbezogene Daten bezogen, dennoch veranschaulicht sie gut, welchen weiteren Herausforderungen Forschende auch in anderen Bereichen wie dem Urheberrecht begegnen: Auch wenn Forschungsprojekte verstärkt grenzüberschreitend und interdisziplinär durchgeführt werden, sind die Regelungen oftmals stark föderal geprägt. Mit zunehmenden Vernetzungen wie bspw. durch den European Health Data Space[21], ist es daher wichtig Datenschutz von Anfang an mit zu berücksichtigen, um nicht anschließend in kostenintensiven Korrekturen diesen nachzubessern. Der Schutz der Privatsphäre sollte dem Fortschritt und Forschung nicht untergeordnet sein, noch diesen entgegenstehen, sondern sollten diese als gleichwertig angesehen und von Anfang an bedacht und umgesetzt werden (Kelber 2023, S. 22f.).

3.2 Potenzial ungenutzt, Anreize benötigt, Standards essentiell

Es gilt, Partnerschaften und Kooperationen durch Datenzugänge gemäß der FAIR Prinzipien zu fördern und damit gleiche Wettbewerbsbedingungen für Unternehmen, Forschung und Zivilgesellschaft auszugestalten. In Deutschland werden etwa 80 Prozent der industriell erzeugten Daten nicht weiterverwendet, oft aufgrund mangelnden Wissens (Bundesregierung 2023). In diesem Zusammenhang beteiligt sich NFDI an FAIR Data Spaces[22], wodurch ein offenes Ökosystem zwischen Wirtschaft und Wissenschaft zur Nutzung von Daten ohne Kontrollverlust geschaffen werden soll. Unternehmen profitieren bei einer solchen Zusammenarbeit nicht nur von den Datensätzen der Forschung, sondern auch von anderen Aspekten der akademischen Einrichtungen, bspw. die Verwendung von hoch entwickelten Messgeräten; dies erspart Investitionen in diesem Bereich (Stahl et al. 2024, S. 2).

Gemeinsame Datenstandards führen zu strukturierten, qualitätsgesicherten Datensätzen, die über Metadaten und Ontologien auffindbar und über geeignete Schnittstellen nutzbar und verknüpfbar sind. Die Forderungen nach einem Datenzugangsrecht für die Forschung sind dabei nicht neu,

21 Siehe: https://european-health-data-space.com/
22 Siehe: https://www.nfdi.de/fair-data-spaces/?lang=en

schließlich bieten „mehrdimensionale Datenverwendung“ sowohl Chancen für die unternehmerische Wertschöpfung als auch für die Forschung über Sektorengrenzen hinweg (Stifterverband 2024). An dieser Stelle könnte das Forschungsdatengesetz bestehende Kooperationsmodelle sichern, z. B. zwischen Forschungseinrichtungen, Rechenzentren und Gedächtniseinrichtungen (NFDI-Sektion ELSA 2023a, S. 15).

4. Dritter Wunsch: Gemeinsame Werte auch in der Datenpolitik schützen

Die Datenpolitik steht vor der großen Aufgabe, eine beständige Datendemokratie in Zeiten des digitalen Wandels zu schaffen, denn dieser Wandel eröffnet nicht nur viele Chancen, sondern birgt auch Risiken wie Datenmissbrauch. Solche Gefahren für Menschen und Demokratie müssen in Betracht gezogen werden, wenngleich das oberste Ziel stets das Wohl und die Würde des Menschen ist (Art. 1 der EU-Grundrechte-Charta[23]); dieser Fokus auf die Individuen ändert sich auch nicht in den digitalen Rechten und Grundsätzen, denn Menschen sollten stets die freie Wahl in der Service- und Algorithmennutzung innehaben (EU-Kommission 2022, S. 4). Die EU läutete mit der Datenschutzgrundverordnung, dem Digital Services Act (DSA), dem Data Governance Act (DGA)[24] sowie dem Data Act eine neue Ära der Datenregulierung ein. Da globale Unternehmen ihre Geschäftsmodelle auch außerhalb der EU entsprechend den Regulierungen anpassen, die sie befolgen müssen, um auf dem europäischen Binnenmarkt aktiv zu sein („Brussels Effect“), werden die europäischen Datengesetze auch über der EU hinaus ihre Wirkung entfalten (Bradford 2019). Dieser Effekt ist aber eher auf wirtschaftliches Kalkül zurückzuführen als auf eine überlegene EU-Gesetzgebung (Hilgendorf 2023, S. 47). Um die Datenakteure des Gemeinwohls – Wissenschaft, NGOs und Medien – in einem FAIRen Datenökosystem für ihre Aufgaben der Wissensgenerierung und -vermittlung zu befähigen, benötigt es daher weiterführende gesetzliche Regelungen.

23 Siehe: *OJ C 326, 26.10.2012, p. 391–407.*
24 Data Governance Act: Verordnung EU/2022/868. *OJ L 152, 3.6.2022, p. 1–44.*

4.1 FAIRe Datendemokratien

In einem FAIRen Datenökosystem (mit Datenzugängen gemäß der FAIR-Prinzipien) bedarf es der Aufgabenvielfalt verschiedener Datenakteure, um Datenmonopole zu verhindern und um eine allgemeine Zugänglichkeit zu gewährleisten. Daher sollten Daten so offen und transparent wie möglich ausgetauscht werden. Öffentliche Forschungseinrichtungen sind dem Ziel des gesellschaftlichen Erkenntnisgewinn verpflichtet und somit als relevante Datenakteure bei Dateninfrastrukturen insbesondere in Bereichen der Daseinsvorsorge wie Agrarwirtschaft, Energie, Umwelt, Gesundheit oder Mobilität zu etablieren (NFDI-Sektion ELSA 2023a, S. 3; Hilgendorf 2023, S. 55). Um den Datenzugang für die Forschung auszugestalten, benötigt es weiterführende Rechte wie das Forschungsgeheimnis, um sensible Forschungsdaten besonders zu schützen (RatSWD 2022, S. 5), ggf. auch vor behördlichem Zugriff. Das Bundesverfassungsgericht (BVerfG) betonte zum Beispiel in einem Fall[25], bei dem Strafrechtsbehörden aufgrund eines Tatverdachts Zugriff auf Forschungsdaten verlangten, dass die Forschungsfreiheit nicht angemessen berücksichtigt wurde. Die Forschungsfreiheit umfasst „auch die Erhebung und Vertraulichkeit von Daten im Rahmen wissenschaftlicher Forschungsprojekte als Bestandteil", weil die sensible Datenerhebung von Betroffenen „nur unter der Bedingung von Vertraulichkeit erhoben werden" können (Bundesverfassungsgericht 2023, Rn. 2a). Um Forschende daher vor unerlaubtem Zugriff auf Daten zu schützen, empfiehlt Koethke (2023) ein Beschlagnahmeverbot; ähnliche Vorschläge für eine Verschwiegenheitspflicht folgten von NFDI und RatSWD (NFDI-Sektion ELSA 2023a, S. 3; RatSWD 2022). In einer FAIRen Datendemokratie ist es daher wichtig, Akteure des Gemeinwohls mit Rechten und Pflichten auszustatten, sodass sie ihre Aufgaben des wissenschaftlichen Erkenntnisgewinns oder der Wissensvermittlung, erfüllen können. Gleichzeitig müssen kollidierende Rechte stets genau betrachtet werden[26], um nicht eines der Rechte zu beeinträchtigen.

25 Die Verfassungsbeschwerde wurde wegen Fristverletzung für unzulässig erklärt; dennoch bewertete das BVerfG den Sachverhalt.

26 Kelber (2023, S. 14) verweist auf den vom Bundesverfassungsgericht entwickelten Grundsatz der „Praktischen Konkordanz" für die Kollision der Forschungsfreiheit mit dem Recht auf Selbstbestimmung, um möglichst einen praktikablen Kompromiss der Rechte zu erzielen.

4.2 Der ausgestaltete Datenzugang in der Datenpolitik

Daten werden als „das neue Öl" bezeichnet, doch Daten sind keine statische Ressource, die in ihren Verarbeitungsprozess aufgebraucht werden (Seitz-Moskaliuk 2022). Damit sollte so vielen wie möglich Zugang auf diese Quelle gewährt werden, was aber leider nicht immer gegeben ist. Einerseits generieren Menschen stetig neue Daten (z. B. im Smart Home), welche bislang nur den Herstellern bzw. Plattformbetreibern zur Verfügung stehen, nicht aber denjenigen, die diese Daten durch ihre Nutzung erzeugen. Andererseits sind die Daten des Individuums oft erst in der Verknüpfung mit anderen Daten nützlich, z. B. beim Microtargeting.

Der Ruf der Wissenschaft und Zivilgesellschaft nach Datenzugang zu großen Plattformen war bereits zunehmend lauter geworden, weshalb die EU mit dem Art. 40 des DSA reagierte, der einen Datenzugang für Forschende bei großen Plattformen schafft. Dabei werden die genaueren Verfahren noch auf nationaler Ebene ausgehandelt. Die Regelung gewährleistet den Forschenden einen gleichberechtigten Zugang zu qualitativ hochwertigeren Daten, um gesellschaftlich relevante Aspekte (z. B. Desinformationen) zu untersuchen; dafür benötigen Forschende gesicherte (Server-)Infrastrukturen, um diese Datenressourcen der Plattformen auf systemische Risiken hin zu analysieren (Klinger & Ohme 2023, S. 6). Der kürzlich in Kraft getretenen Data Act zielt auf einen innovativen Datenmarkt ab, indem darin die Weitergabe von Daten des Internet of Things (IoT) aus Industrie und Privathaushalten bestimmt wird. Zentral sind dabei die Datenzugangs- und Entscheidungsrechte (z. B. zur Datenspende) der Endnutzer:innen, die so zu „Schiedsrichter" werden (Podzun 2023, S. 23).

Auf den deutschen Vorschlag, auch der Forschung ein direktes Datenzugangsrecht im Data Act einzuräumen, einigten sich die Mitgliedstaaten jedoch nicht, sodass Forschungseinrichtungen in Form der Datenspende durch Nutzende (Art. 5 Data Act), oder als öffentliche Stellen bei „außergewöhnlicher Notwendigkeit", z. B. Naturkatastrophen, Zugänge erhalten (Art. 14 Data Act). Damit werden die Prozesse, die es benötigt, um Daten zu erhalten, zu bereinigen und zu analysieren, nicht ausreichend betrachtet, denn hierfür benötigt es Know-how, Hardware und Methoden, die nicht erst im Notstand geschaffen werden können (NFDI-Sektion ELSA 2022, S. 3f.). Daher will der DGA den Datenaustausch zwischen Privatpersonen, Unternehmen und der öffentlichen Hand erleichtern, indem neue Akteure wie Datentreuhänder und Datenmittler etabliert werden, an welche Nut-

zer:innen ihre Daten zur Gemeinwohlförderung spenden können[27]. So sollen datenaltruistische Organisationen entstehen, die den freien Datenfluss fördern und von einer Stelle – in Deutschland durch die Bundesnetzagentur – registriert werden; erste Pläne zur gemeinsamen Koordination verhandeln sechs Behörden[28] im Digitalen Cluster Bonn (BSI 2024).

Die neueste europäische Errungenschaft ist der Artificial Intelligence Act (AIA), welcher weltweit eine der ersten Regulierungsmaßnahmen für die Technologie der Künstlichen Intelligenz (KI) darstellt (BMJ 2024). Anhand eines risikobasierten Ansatzes werden die Pflichten strenger, je höher das Risiko für Menschen wird. Der AIA enthält kein Recht auf Datenzugang für Forschende, jedoch sind für KIs neben Rechenleistung auch die Trainingsdatensätze entscheidende Komponenten. KIs werden erfolgversprechender, wenn sie auf guten Trainingsdatensätze aufbauen; solche Datensätze gibt es auch in der Forschung. Der AIA als letzter und die DSGVO als eine der ersteren Datenpolitik-Rechtsakte kommen hier wieder zusammen: Werden personenbezogene Daten verarbeitet, haben die Betroffenen – auch in einer teilautomatisierten Verarbeitung, welche im Verlauf von KI-Anwendungen und selbstlernenden KIs denkbar ist – das Recht auf Widerruf oder Löschung, sodass eine praktische Umsetzung neue Fragen aufwirft (Boehm & Hallinan 2023, S. 35). Dabei ist das Zusammenspiel der neuen Rechtsakte aufgrund des schnellen Regulierungstempos nicht in Gänze geklärt, sodass Hilgendorf diese anhand der klassischen Regeln für Normenkollisionen (Vorrang des höheren, neueren, spezielleren Gesetzes) untersucht und zu keinem „befriedigenden Ergebnis" kommt (Hilgendorf 2023, S. 65).

5. Fazit

Ziel der deutschen Digitalpolitik ist es, vertrauenswürdige Datenflüsse und nachhaltige, globale digitale Infrastrukturen mit offenen Schnittstellen zu stärken (Bunderegierung 2023b). Zentral sind dafür Dateninfrastruktur-Betreiber und Vertrauensstellen hinsichtlich sensibler Daten, wie Datentreuhand-Modelle oder Datenräume. NFDI ist eine Informationsinfrastruktur und legitimiert als Stimme der deutschen Wissenschaftslandschaft

27 Siehe der Beitrag von Johannes u. Nebel in diesem Band.

28 Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Bundesamt für Justiz (BfJ), Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Bundeskartellamt (BKartA), Bundesnetzagentur (BNetzA).

für das Thema Forschungsdaten. So kann NFDI durch personelles Know-how, Tools und Services maßgeblich zum Aktionsplan Forschungsdaten beitragen. Dafür benötigt es Rechtssicherheit beim Datenaustausch und der Sekundärnutzung von Daten. Hier sind sowohl die europäischen und nationalen Gesetzgeber aufgefordert, für Forschende erfüllbare Rahmenbedingungen durch datenpolitische Rechtsakte zu schaffen (Forschungsklauseln, diskriminierungsfreie Datenzugänge, Schutz der Forschungsdaten). Für einen vertrauensvollen Austausch von Daten benötigen Dateninfrastrukturen eine verlässliche langfristige Finanzierung, um Datensicherheit, -souveränität und Unterstützungsangebote (wie Helpdesks etc.) leisten zu können. Nur so gelingt die Vernetzung mit den weiteren Datenakteuren und eine nachhaltige Infrastruktur sowohl auf organisatorischer, technischer und rechtlicher Ebene kann entstehen.

Literatur

BMBF (2023): Aktionsplan Forschungsdaten. URL: https://www.bmbf.de/bmbf/de/forschung/digitale-wirtschaft-und-gesellschaft/aktionsplan-forschungsdaten/aktionsplan-forschungsdaten_node.html (besucht am 15.03.2023).

BMJ (2024): Rahmen für Künstliche Intelligenz in der EU steht (Pressemitteilung). URL: https://www.bmj.de/SharedDocs/Pressemitteilungen/DE/2024/0202_KI-VO.html?cms_mtm_campaign=linksFromNewsletter (besucht am 15.03.2023).

Bishop, Bradley W. and Hank, Carolyn (2016): Data curation profiling of biocollections. Proc. Assoc. Info. Sci. Tech., 53: 1-9. https://doi.org/10.1002/pra2.2016.14505301046

Boehm, Franziska & Hallinan, Dara (2023): Der besondere Schutz der Forschung in der Datenschutz-Grundverordnung. In: Roßnagel, Alexander & Wallmann Astrid (Hrsg.): *Stärkung der Forschung durch Datenschutz*. Baden-Baden: Nomos, S. 31-52.

Borgmann, Christine (2023): Knowledge Infrastructures: The Invisible Foundation of Research Data. URL: https://zenodo.org/doi/10.5281/zenodo.8344853

Bradford, Anu (2019): *The Brussels Effect: How the European Union Rules the World* Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

BSI (2024): Digital Cluster Bonn. URL: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2024/240115_DigitalCluster.html (besucht am 15.03.2023).

Bundesregierung (2023): Weiterentwicklung der Datenstrategie. URL: https://www.bundesregierung.de/breg-de/themen/digitalisierung/datenstrategie-2023-2216620 (besucht am 15.03.2023).

Bundesverfassungsgericht (2023): Pressemitteilung Nr. 90/2023. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2023/bvg23-090.html (besucht am 15.03.2023).

zu Castell, Wolfgang, Dransch, Doris, Juckeland, Guido et al. (2024): Towards a Quality Indicator for Research Data publications and Research Software publications. URL: https://arxiv.org/pdf/2401.08804.pdf (besucht am 15.03.2023).

DFG (2020): Digitaler Wandel in den Wissenschaften. URL: https://zenodo.org/doi/10.5281/zenodo.4191344

EU-Kommission (2018): Directorate-General for Research and Innovation: Cost of not having FAIR research data. Cost-Benefit analysis for FAIR research data. URL: https://data.europa.eu/doi/10.2777/02999 (besucht am 15.03.2023).

EU-Kommission (2020): Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing. URL: https://data.europa.eu/doi/10.2759/731415 (besucht am 15.03.2023).

EU-Kommission (2022): Europäische Erklärung zu den digitalen Rechten und Grundsätzen für die digitale Dekade. Brüssel: COM/2022/28 final.

EU-Kommission (o.D.): Europäische Datenstrategie. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de (besucht am 15.03.2023).

Hennemann, M., von Lewinski, K., Wawra, D., Widjaja, T. (2024): Vektoren der Datenpreisgabe (5:20min). URL: https://stiftungdatenschutz.org/veranstaltungen/unsere-veranstaltungen-detailansicht/datentag-preisgabe-von-daten-440#lg=1&slide=1 (besucht am 15.03.2023).

Herres-Pawlis, Sonja, Andres, Ann-Christin, Bach, Felix et al. (2022): Working Group Charter Error Management and No Blame Culture, Version 1.0. URL: https://doi.org/10.5281/zenodo.6475492

Hilgendorf, Eric (2023): Vom Datenschutz zum Datenhandel – Friktionen in der europäischen Datenpolitik. In: Roßnagel, Alexander & Wallmann Astrid (Hrsg.): *Stärkung der Forschung durch Datenschutz*. Baden-Baden: Nomos, S. 53-74.

Kelber, Ulrich (2023): Wissenschaftliche Forschung – selbstverständlich mit Datenschutz. In: Roßnagel, Alexander & Wallmann Astrid (Hrsg.): *Stärkung der Forschung durch Datenschutz*. Baden-Baden: Nomos, S. 13-30.

Klinger, Ulrike & Ohme, Jakob (2023): Was die Wissenschaft im Rahmen des Datenzugangs nach Art. 40 DSA braucht. Berlin: Weizenbaum Institut: https://doi.org/10.34669/WI.WPP/8.1

Koethke, Kira (2023): Forschungsfreiheit im Strafprozess. URL: https://verfassungsblog.de/forschungsfreiheit-im-strafprozess/ (besucht am 15.03.2023).

NFDI (2022). Recht auf Datenzugang für öffentliche Forschung schafft gesellschaftlichen Mehrwert. URL: https://www.nfdi.de/positionspapier-recht-auf-datenzugang-fuer-oeffentliche-forschung-schafft-gesellschaftlichen-mehrwert/ (besucht am 15.03.2023).

NFDI-Sektion ELSA (2022): Stellungnahme zum EU Data Act. URL: https://www.nfdi.de/nfdi-veroeffentlicht-stellungnahme-zum-eu-data-act/ (besucht am 15.03.2023).

NFDI-Sektion ELSA (2023): Stellungnahme zur öffentlichen Konsultation zum Forschungsdatengesetz. URL: https://www.nfdi.de/wp-content/uploads/2023/05/NFDI-Stellungnahme-zum-Forschungsdatengesetz.pdf (besucht am 15.03.2023).

Podszun, Rupprecht (2023): *Der EU Data Act und der Zugang zu Sekundärmärkten am Beispiel des Handwerks*. Baden-Baden: Nomos.

RatSWD (2022): Eckpunkte für ein Forschungsdatengesetz. URL: https://www.konsortswd.de/wp-content/uploads/RatSWD-Positionspapier-Eckpunkte-fuer-ein-Forschungsdatengesetz.pdf (besucht am 15.03.2023).

RatSWD (2023): Nutzung von Registerdaten für Zwecke der Forschung sichern. URL: https://www.konsortswd.de/wp-content/uploads/RatSWD-Positionspapier-Nutzung-von-Registerdaten.pdf (besucht am 15.03.2023).

RfII (2016): Leistung aus Vielfalt. URL: https://rfii.de/?p=1998 (besucht am 15.03.2023).

Riphahn, Regina T. (2023): Die deutsche Dateninfrastruktur aus Sicht der empirischen Wirtschaftsforschung. *Wirtschaftsdienst*, 103(1), S. 24-28. https://doi.org/10.2478/wd-2023-0011

Sachverständigenrat (2023): Jahresgutachten 2023/24. URL: https://www.sachverstaendigenrat-wirtschaft.de/jahresgutachten-2023.html (besucht am 15.03.2023).

Seitz-Moskaliuk, Hendrik (2022): Oil, wind and NFDI. URL: https://www.youtube.com/watch?v=FENvW21NXV4 (besucht am 15.03.2023).

SPD-Arbeitsgruppe (2023): Eckpunkte AG Bildung und Forschung der SPD-Fraktion zum Forschungsdatengesetz. URL: https://www.ruppert-stuewe.de/eckpunktepapier-spd-forschungsdatengesetz/ (besucht am 15.03.2023).

Specht-Riemenschneider, Louisa (2021): Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität. URL: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf (besucht am 15.03.2023).

Stahl, Florian, Hamann, Andreas, Hoff, Kai & Kockelmann, Kai (2024). Collaboration Models Between Industry and Academia. Whitepaper on behalf of the Section Industry Engagement of the National Research Data Infrastructure (NFDI). Zenodo. https://doi.org/10.5281/zenodo.10473579

Star, Susan Leigh & Ruhleder, Karen (1996): Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research*, 7(1): 111-134, http://dx.doi.org/10.1287/isre.7.1.111.

Stifterverband (2024): Datagroup Business2Science. URL: https://www.stifterverband.org/datagroup (besucht am 15.03.2023).

Strecker, Dorothea, Bossert, Lukas C. & Demandt, Évariste (2021): Das Versprechen der Vernetzung der NFDI. Bausteine *Forschungsdatenmanagement*, (3), S. 39–55. https://doi.org/10.17192/bfdm.2021.3.8336

Stüwe, Ruppert (2023): Daten für die Forschung (Gastbeitrag). URL: https://www.jmwiarda.de/https-www.jmwiarda.de-2023-11-07-daten-fuer-die-forschung/ (besucht am 15.03.2023).

Sure-Vetter, York, Lübke, Eva, Kraft, Sophie, & Seitz-Moskaliuk, Hendrik. (2021, November 17). Nationale Forschungsdateninfrastruktur (NFDI) e. V. - Satzungsvorstellung. Zenodo. https://doi.org/10.5281/zenodo.5735196

Wilkinson, Mark, Dumontier, Michel, Aalbersberg, IJsbrand Jan et al. (2016): The FAIR Guiding Principles for scientific data management and stewardship. *Scientific Data* 3, 160018. https://doi.org/10.1038/sdata.2016.18

3 Regulierung des Datenteilens

Europäische KI-Regulierung: Auf der Suche nach verbindlichen Ansätzen für Nachhaltigkeit und Inklusion

Marco Wedel, Antonios Hazim und Alexandra Wudel

Zusammenfassung

Die europäischen Institutionen haben einen regulatorischen Rahmen zur Verwirklichung eines Ökosystems für vertrauenswürdige und exzellente Künstliche Intelligenz (KI) in der Europäischen Union verhandelt, den Artificial Intelligence Act (EU AI-Act). Der Gesetzgebungsprozess zur Erarbeitung dieser Verordnung war flankiert von politischen Dokumenten, denen beste Absichten in Bezug auf nachhaltige und inklusive Ansätze zur Etablierung vertrauenswürdiger KI zu entnehmen sind. Zu fragen bleibt, ob sich diese Absichten auch in den konkreten Anforderungen des entsprechend verbindlichen Rechtsaktes widerspiegeln. Zusammenfassend entsteht der Eindruck, dass die Gesetzgebenden in Bezug auf nachhaltige und inklusive Ansätze für gemeinsame KI-Systeme verbindliche Regelungen vermeiden.[1]

1. Einleitung

Am 08. Dezember 2023 konnten Entscheidungsträger:innen der EU-Institutionen im sog. Trilogverfahren[2] nach einem 36-stündigen Verhandlungsmarathon eine politische Einigung zum weltweit ersten Regulierungsansatz für Künstliche Intelligenz (KI) erzielen, dem sog. EU AI-Act (Euractiv 2023). Was als eine Initiativstellungnahme zu KI des Europäischen Wirtschafts- und Sozialausschuss im Jahr 2016 begann (EWSA 2016) und sich im Rahmen eines ordentlichen Gesetzgebungsverfahrens aktuell in der

1 Diese Arbeit entstand im Rahmen des vom Bundesministerium für Arbeit und Soziales geförderten Projekts KIDD. Mehr Informationen zum Projekt: kidd-prozess.de (letzter Aufruf 04.06.2024).

2 In Zusammenhang mit dem ordentlichen Gesetzgebungsverfahren der Europäischen Union ist ein Trilog eine informelle interinstitutionelle Verhandlung, an der Vertreter des Europäischen Parlaments, des Rates der Europäischen Union und der Europäischen Kommission teilnehmen (EUR-Lex 2024).

finalen Umsetzungsphase befindet (Legislative Observatory 2024), wird nach Veröffentlichung im Amtsblatt und zwei Jahre nach Inkrafttreten – voraussichtlich also im Jahre 2026 – verpflichtend anzuwenden sein. Durch die Wahl einer Verordnung als Rechtsinstrument hat der EU AI-Act dann allgemeine Geltung, ist in allen Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat (Art. 288 Abs. 2 AEUV).

Der Gesetzgebungsprozess zur Erarbeitung dieser Verordnung war flankiert von politischen Erklärungen, denen beste Absichten in Bezug auf nachhaltige und inklusive Ansätze zur Etablierung von vertrauenswürdiger KI zu entnehmen sind. Bereits in der benannten Initiativstellungnahme des EWSA ist davon die Rede, dass im Umgang mit KI gesellschaftliche Einbindung, Vertrauen und ein Konsens über die nachhaltige Weiterentwicklung von KI gewährleistet werden müssen (EWSA 2016: S. 3). Für die Hochrangige Expertengruppe für Künstliche Intelligenz (HEG-KI) sind „Vielfalt, Nichtdiskriminierung und Fairness" sowie „Gesellschaftliches Wohlergehen" Kernforderungen für eine vertrauenswürdige KI (Hochrangige Expertengruppe 2019a: S. 10).

Die Europäische Kommission kommt in diesem Zusammenhang zu dem Schluss, dass es hierfür ein „Ökosystem der Exzellenz" und ein „Ökosystem des Vertrauens" bedarf, mit einer Governance-Struktur, die größtmögliche Beteiligung aller Interessenträger:innen gewährleistet (Kommission 2020: S. 29). Das Europäische Parlament kann sich in seinen Stellungsnahmen den Positionen im Wesentlichen anschließen und ist der Auffassung, dass alle neuen Regulierungsrahmen für KI die Menschenwürde, die Autonomie und die Selbstbestimmung des Einzelnen achten, Schaden abwenden und Fairness, Inklusion und Transparenz fördern müssen. KI-Systeme sollten von Regierungen und Unternehmen zum Wohle der Menschen und des Planeten eingesetzt werden und zur Erreichung der Ziele nachhaltige Entwicklung, Umweltschutz, Klimaneutralität und Kreislaufwirtschaft beitragen (European Parliament 2020: Punkt 3. u. 51).

Zusammenfassend lässt sich hier ein inter-institutioneller Konsens der EU-Institutionen dokumentieren, der u. a. nachhaltige und inklusive Ansätze samt inklusiver Gestaltungsprozesse für KI-Welten in den Fokus rückt. Die Etablierung und Verortung entsprechender Prozesse als immanenter Bestandteil verbindlicher Rechtsakte wären nun folgerichtig in den Entwurfstexten eines zukünftigen EU AI-Acts zu vermuten und sollten sich in den konkreten Anforderungen des dann verbindlichen Rechtsaktes widerspiegeln.

Seit der politischen Einigung vom 08. Dezember 2023 liegt ein Textentwurf des zukünftigen EU AI-Acts als „*provisional agreement resulting from interinstitutional negotiations*" (European Parliament 2024a) vor, der eine erste und vergleichende Analyse in Bezug auf die Integration der zuvor beschriebenen Ansätze ermöglicht. Dieser nimmt den finalen Gesetzestext im Idealfall vor seiner tatsächlichen Veröffentlichung vorweg. Im Februar 2024 steht der Gesetzgebungsprozess kurz vor dem Abschluss. Die Ausschüsse für bürgerliche Freiheiten, Justiz und Inneres (LIBE) und für Binnenmarkt und Verbraucherschutz (IMCO) des Europäischen Parlaments haben den endgültigen Text in einer gemeinsamen Abstimmung am 13. Februar 2024 mit einer überwältigenden Mehrheit (71 Ja-Stimmen, 8 Nein-Stimmen und 7 Enthaltungen) bereits angenommen. Die Verhandlungsführer des Rates billigten den Text ebenfalls im Februar 2024. Der AI-Act wurde auf der Plenartagung des Parlaments am 13.03.2024 verabschiedet, die endgültige Billigung durch den Rat erfolgte am 21.05.2024 (European Parliament 2024, Council of the European Union 2024a).

Das Ziel des Beitrages ist es, den europäischen Gesetzgebungsprozess zu KI am Beispiel des EU AI-Acts in Bezug auf das Versprechen einer nachhaltigen und inklusiven Gestaltung von KI-Systemen kritisch zu analysieren. Die Leitfrage lautet: (Wo) Gibt es verbindliche Anforderungen zur nachhaltigen und inklusiven Gestaltung von KI-Systemen in der europäischen Regulierung?

Hierzu werden im Sinne einer vergleichenden Policy-Analyse anhand des Policy-Cycles die im Gesetzgebungsverfahren durch die Institutionen zum Ausdruck gebrachten Positionen in der Phase des „Agenda-Settings" und in der Phase der „Policy-Formulation" untersucht (Sabatier 2007). Im Fokus stehen hierbei die Positionen zu Nachhaltigkeit, Inklusion und die im Gesetzgebungsverfahren herausgearbeitete Notwendigkeit zur *AI Literacy*. Analysiert werden die Positionen der Europäischen Kommission (2021), des Rates der EU (2022) und des Europäischen Parlaments (2023). Referenz sind die von HEG-KI konsolidierten Prinzipien und Kernforderungen, die in ihrer Essenz den durch die Institutionen während des „Agenda-Settings" formulierten Anspruch an eine KI-Regulierung zusammenfassen (Wedel 2023). Nach einer Darstellung jener Prinzipien und Kernforderungen wird vergleichend untersucht, wo, in welcher Form und Ausführlichkeit bzw. wie verbindlich sich entsprechende Anforderung zu Nachhaltigkeit, Inklusion und *AI Literacy* in den Verordnungsentwürfen wiederfinden. Weiterhin wird analysiert, welche Positionen sich in den Verhandlungen durchsetzen konnten.

2. Ethische Prinzipien und Kernforderungen

Im Zuge der institutionellen Problemwahrnehmung und Agenda-Setzung zum europäischen Policy-Prozess rund um den AI-Act, berief die Kommission im Jahr 2018 die zuvor bereits erwähnte HEG-KI ein und beauftragte sie, einen Entwurf für KI-Ethik-Leitlinien auszuarbeiten (Europäische Kommission 2018: S. 9).

Die HEG-KI, mit 51 Expert:innen und Vertreter:innen aus Wirtschaft, Wissenschaft und weiteren Interessengruppen besetzt, erarbeitete neben Ethik-Leitlinien (Hochrangige Expertengruppe 2019a) auch eine Definition von KI (Hochrangige Expertengruppe 2019b) und eine „Assessment List for Trustworthy Artificial Intelligence (ALTAI)" (Hochrangige Expertengruppe 2020).

Die wichtigsten Aspekte der Ethik-Leitlinien sollen nachfolgend auf Basis der benannten Primärquellen zusammengefasst werden. Hierzu wird aus einer Textstelle, die als wissenschaftliche Analyse des Mit-Autors Wedel (2023: S. 70 ff.) bereits vorliegt, zitiert:

„‚Eine vertrauenswürdige KI zeichnet sich durch drei Komponenten aus, die während des gesamten Lebenszyklus des Systems erfüllt sein sollten: a) Sie sollte rechtmäßig sein und somit alle anwendbaren Gesetze und Bestimmungen einhalten, b) sie sollte ethisch sein und somit die Einhaltung ethischer Grundsätze und Werte garantieren und c) sie sollte robust sein, und zwar sowohl in technischer als auch sozialer Hinsicht, da KI-Systeme selbst bei guten Absichten unbeabsichtigten Schaden anrichten können' (Hochrangige Expertengruppe 2019a: S. 2).

In diesem Zusammenhang werden vier ethische Grundsätze und damit verbundene Werte herausgearbeitet, die einen auf Grundrechten beruhenden Ansatz verfolgen und bei der Entwicklung, Einführung und Verwendung von KI-Systemen eingehalten werden müssen (vgl. Hochrangige Expertengruppe 2019a, S. 2): die ‚Achtung der menschlichen Autonomie, Schadensverhütung, Fairness und Erklärbarkeit'.

Aus diesen vier Grundsätzen leitet die HEG-KI sieben Kernforderungen ab, die es durch technische und nicht-technische Methoden umzusetzen gilt:

Es muss gewährleistet sein, dass die Entwicklung, Einführung und Nutzung von KI-Systemen die Anforderungen an vertrauenswürdige KI erfüllen: 1) Vorrang menschlichen Handelns und menschliche Aufsicht, 2) technische Robustheit und Sicherheit, 3) Schutz der Privatsphäre und Datenqualitätsmanagement, 4) Transparenz, 5) Vielfalt, Nichtdiskriminierung

und Fairness, 6) gesellschaftliches und ökologisches Wohlergehen sowie 7) Rechenschaftspflicht' (vgl. Hochrangige Expertengruppe 2019a: S. 3).

Alle Anforderungen sind in Bezug auf ihre Bedeutung gleichranging und enthalten systemische, individuelle und gesellschaftliche Aspekte (vgl. Hochrangige Expertengruppe 2019a: S. 17 f.). In Bezug auf die Forderungen eines Vorrangs menschlichen Handelns und menschliche Aufsicht wird auf Grundrechte verwiesen, wie sie etwa in der EU-Grundrechtscharta niedergeschrieben sind: Würde des Menschen, Freiheiten, Gleichheit, Solidarität, Bürgerrechte, Justizielle Rechte (vgl. Europäische Union 2010). Mit technischer Robustheit und Sicherheit werden Aspekte wie ‚Widerstandsfähigkeit gegen Angriffe und allgemeine Sicherheit', Zuverlässigkeit und Reproduzierbarkeit adressiert. Der Schutz der Privatsphäre und Datenqualitätsmanagement meint ‚Achtung der Privatsphäre, Qualität und Integrität der Daten sowie Datenzugriff'. Transparenz umfasst die ‚Nachverfolgbarkeit, Erklärbarkeit und Kommunikation'. Unter der Überschrift ‚Vielfalt, Nichtdiskriminierung und Fairness' wird die Vermeidung unfairer Verzerrungen, die Zugänglichkeit und ein universeller, d. h. barrierefreies Design von KI-Systemen, sowie die Beteiligung der Interessenträger zusammengefasst. Der Aspekt des gesellschaftlichen und ökologischen Wohlergehens wird durch die Schlagworte ‚Nachhaltigkeit und Umweltschutz, soziale Auswirkungen, Gesellschaft und Demokratie' präzisiert. Die Rechenschaftspflicht verweist auf Aspekte externer Überprüfbarkeit und Meldepflichten zur Vermeidung negativer Auswirkungen mit entsprechenden Rechtsmitteln (vgl. Hochrangige Expertengruppe 2019a: S. 17 f.)

Die HEG-KI greift die Forderungen des EWSA (2016), des Europäischen Parlaments (2017) und des Europäischen Rates (2017) nach einem menschenkontrollierten KI-Ansatz auf und erklärt darüber hinaus, dass alle KI-Systeme – also auch nicht Mensch-Maschine-Systeme – auf den Menschen ausgerichtet sein müssen (vgl. Hochrangige Expertengruppe 2019a: S. 5).

‚Wir sind der Ansicht, dass es im Kontext des schnellen technologischen Wandels unabdingbar ist, dass Vertrauen auch in Zukunft das Element bleibt, das Gesellschaften, Gemeinschaften, Wirtschaftsräume und nachhaltige Entwicklung zusammenhält. Deshalb bestimmen wir vertrauenswürdige KI als unsere grundlegende Ambition, denn Menschen und Gemeinschaften können der Entwicklung und Anwendung von Technologien nur dann vertrauen, wenn ein klarer und umfassender Rahmen existiert, der Vertrauenswürdigkeit gewährleistet' (vgl. Hochrangige Expertengruppe 2019a: S. 5 f.)."

Natürlich kann und soll die HEG-KI nicht den demokratischen Willensbildungsprozess ersetzen und gewünschte Ergebnisse qua Expert:innenmeinung postulieren. Spannend ist also die Frage, ob und wie diese ethischen Prinzipien und Kernforderungen von den die Gesellschaft repräsentierenden Akteur:innen aufgenommen und ggf. im Gesetzestext berücksichtigt werden. Schaut man sich die Verordnungsentwürfe der Europäischen Kommission (2021), des Rates der EU (2022) und des Europäischen Parlaments (2023) vor diesem Hintergrund an, findet sich der beschriebene Anspruch grundsätzlich in allen Gesetzesentwürfen der Institutionen wieder. Die Bedeutung und Wirkmächtigkeit, die den benannten Aspekten zugestanden wird, unterscheidet sich in den Zugängen der drei Institutionen allerdings erheblich. Explizit Bezug genommen auf die Kernforderungen der HEG-KI wird nur im Textentwurf des Europäischen Parlaments (2023: 127 f.). Dies, nachdem in einer „Opinion of the Committee on Legal Affairs (…) on the proposal" der Verweis auf die Vorarbeit der HEG-KI mit dem Änderungsvorschlag der Integration eines Artikels zum Thema „General principles applicable to all AI systems" eingebracht wurde:

> „ Amendment 42: Proposal for a regulation Article 4 a (new)
> Article 4 a – General principles applicable to all AI systems
> 1. All AI operators shall respect the following general principles that establish a high-level framework that promotes a coherent human-centric European approach to ethical and trustworthy Artificial Intelligence, which is fully in line with the Charter as well as the values on which the Union is founded:
> • 'human agency and oversight' means that AI systems shall be developed and used as a tool that serves people, respects human dignity and personal autonomy, and that is functioning in a way that can be appropriately controlled and overseen by humans.
> • 'technical robustness and safety' means that AI systems shall be developed and used in a way to minimize unintended and unexpected harm as well as being robust in case of unintended problems and being resilient against attempts to alter the use or performance of the AI system so as to allow unlawful use by malicious third parties.
> • 'privacy and data governance' means that AI systems shall be developed and used in compliance with existing privacy and data protection rules, while processing data that meets high standards in terms of quality and integrity.

> • 'transparency' means that AI systems shall be developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system as well as duly informing users of the capabilities and limitations of that AI system and affected persons about their rights.
> • 'diversity, non-discrimination and fairness' means that AI systems shall be developed and used in a way that includes diverse actors and promotes equal access, gender equality and cultural diversity, while avoiding discriminatory impacts and unfair biases that are prohibited by Union or national law.
> • 'social and environmental well-being' means that AI systems shall be developed and used in a sustainable and environmentally friendly manner as well as in a way to benefit all human beings, while monitoring and assessing the longterm impacts on the individual, society and democracy" (Committee on Legal Affairs 2022: S. 23 f.).

Im abschließenden Entwurf des Parlaments findet sich der Änderungsvorschlag des Rechtsausschusses weitestgehend unverändert wieder. In Ergänzung wird darüber hinaus ein Verweis auf „foundational models" eingearbeitet, da in der Zwischenzeit (hier die Jahre 2022 und 2023) die öffentliche Debatte rund um das Auftreten von ChatGPT und anderen Generativen KI-Systemen auch Einzug in den Policy-Diskurs des AI-Acts gefunden hat. Weiterhin wurde ein Verweis ergänzt, wonach die Prinzipien nicht nur zu respektieren, sondern von den Marktteilnehmer:innen auch aktiv umzusetzen seien, um KI im Einklang mit diesen Grundsätzen zu entwickeln und einzusetzen:

> "Amendment 213: Proposal for a regulation - Article 4 a (new)
> Article 4 a – General principles applicable to all AI systems
> All operators falling under this Regulation shall make their best efforts to develop and use AI systems or foundation models in accordance with the following general principles establishing a high-level framework that promotes a coherent human-centric European approach to ethical and trustworthy Artificial Intelligence, which is fully in line with the Charter as well as the values on which the Union is founded" (European Parliament 2023: S. 127 f.).

Im Ergebnis des Trilogs findet sich ein expliziter Verweis auf die ethischen Prinzipien und Kernforderungen des HEG-KI (Hochrangige Expertengruppe 2019a) im AI-Act schlussendlich nicht (!) wieder. Der entspre-

chende Artikel 4 a wurde aus dem „Provisional agreement resulting from interinstitutional negotiations" (European Parliament 2024b) gestrichen. Der Rechtsausschuss und das Parlament konnten sich nicht durchsetzen. Dem Leak zum „AIAct_four-column document" des Journalisten Luca Bertuzzi folgend, den dieser im Rahmen der Trilog-Verhandlungen auf LinkedIn veröffentlicht hat, ist zusätzlich zu entnehmen, dass weder im Ursprungsentwurf der Kommission noch im Entwurf des Rates ein solcher Verweis angedacht wurde (Bertuzzi 2023).

Tatsächlich rühmt sich die Ratspräsidentschaft in einem zusammenfassenden Bericht an die ständigen Repräsentanten der Mitgliedstaaten, dass *„to ensure a high level of protection of health, safety and fundamental rights enshrined in the Charter, which includes democracy, rule of law and environmental protection"* zwar als Teil des Anwendungsbereichs in Artikel 1 der zukünftigen Verordnung aufgenommen wird, aber *„all subsequent references in the text to the risks addressed by the Regulation only include risks to health, safety and fundamental rights, in line with the Council's mandate"* (Council of the European Union 2024b: S. 2). Es entsteht der Eindruck, dass ein expliziter Verweis auf die ethischen Prinzipien, hier insbesondere als Verweis auf die Kernforderung einer ökologischen Nachhaltigkeit, ausdrücklich nicht erwünscht ist. Deutlich wird dies auch in Artikel 40 (1c), wo der Vorschlag des Parlaments (hier Amendement 440), auch die am Normungsprozess beteiligten Akteure mögen sich später an den Prinzipien für eine vertrauenswürdige KI orientieren (European Parliament 2023: S. 218), dahingehend korrigiert wurde, dass *„actors involved in the standardisation process shall seek to promote investment and innovation in AI, including through increasing legal certainty, as well as competitiveness and growth of the Union market"* (Council of the European Union 2024b: S. 154). Hier wird also die „Vertrauenswürdigkeit" zugunsten der „Exzellenz" im Text ersetzt und damit *de facto* hintangestellt.

3. AI Literacy als Voraussetzung für nachhaltige und inklusive Gestaltungsansätze

Eine vertrauenswürdige KI, so das HEG-KI (Hochrangige Expertengruppe 2019a: S. 28 f.), beruht auf einer sachkundigen Beteiligung der Intressenträger:innen. Hierbei spielen die Aus- und Weiterbildung, so die HEG-KI weiter, eine wichtige Rolle. Es gilt, individuelle Kompetenzen aufzubauen und die „Verbreitung der Kenntnisse über die potenziellen Auswirkungen

von KI-Systemen unter der Bevölkerung sicherzustellen". Dies auch, um die Menschen zu befähigen, an der Gestaltung von gesellschaftlichen Entwicklungen teilzuhaben (Hochrangige Expertengruppe 2019a: S. 29). In diesem Sinne sollten „(g)rundlegende KI-Kompetenzen […] in der gesamten Gesellschaft gefördert werden" (Hochrangige Expertengruppe 2019a, S. 29).

Es ist erneut der Rechtsausschuss des Parlaments, der diesen Gedanken durch eine Ergänzung in den Gesetzestext zu integrieren sucht. Hierbei werden u. a. der Verweis auf die Notwendigkeit von *AI Literacy* als Grundlage für demokratische Kontrolle *und* die Verantwortung aller Akteur:innen, die Entwicklung eines ausreichenden Niveaus an KI-Kenntnissen zu fördern, als Grundsätze herausgearbeitet:

> „Amendment 6 und 7: Proposal for a regulation Recital 14 a (new) and 14 b (new)
> (14a) For this Regulation to be effective, it is essential to address the issue of the digital divide and, therefore, it should be accompanied by a policy of education, training and awareness as regards these technologies that ensures a sufficient level of AI literacy.
> (14b) 'AI literacy' refers to skills, knowledge and understanding that allows providers, users and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause and thereby promote its democratic control. AI literacy should not be limited to learning about tools and technologies, but should also aim to equip providers and users with the notions and skills required to ensure compliance with and enforcement of this Regulation. It is therefore necessary that the Commission, the Member States as well as providers and users of AI systems, in cooperation with all relevant stakeholders, promote the development of a sufficient level of AI literacy, in all sectors of society, for citizens of all ages, including women and girls, and that progress in that regard is closely followed" (Committee on Legal Affairs 2022: S. 5 f.).

Das Parlament schließt sich den Einlassungen des Rechtsausschusses an, übernimmt diese weitestgehend (hier als 9b), hält es aber nicht für notwendig herauszustellen, dass hierfür eine besondere bildungspolitische Anstrengung notwendig sei. Der als 14a formulierte Anspruch wird entsprechend nicht übernommen:

> Amendment 28: Proposal for a regulation Recital 9 b (new)
> (9b) 'AI literacy' refers to skills, knowledge and understanding that allows providers, users and affected persons, taking into account their respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause and thereby promote its democratic control. AI literacy should not be limited to learning about tools and technologies, but should also aim to equip providers and users with the notions and skills required to ensure compliance with and enforcement of this Regulation. It is therefore necessary that the Commission, the Member States as well as providers and users of AI systems, in cooperation with all relevant stakeholders, promote the development of a sufficient level of AI literacy, in all sectors of society, for people of all ages, including women and girls, and that progress in that regard is closely followed" (European Parliament 2023: S. 19).

Im Provisional Agreement finden sich die Grundsätze wie nachstehend aufgeführt neu zusammengestellt. Auffällig ist, dass AI Literacy hier kurzerhand zum handelnden Subjekt gemacht wird, welches Individuen befähigt, entsprechende Kompetenzen aufzubauen (AI Literacy should…). Verantwortliche Akteur:innen sind damit nicht benannt bzw. zukünftig zu schaffende Institutionen (Artificial Intelligence Board) und ganz allgemein Stakeholder, die in Zusammenarbeit mit der Kommission und den Mitgliedstaaten freiwillige Verhaltenskodizes erarbeiten sollen, werden unverbindlich benannt:

> „(9b) In order to obtain the greatest benefits from AI systems while protecting fundamental rights, health and safety and to enable democratic control, AI literacy should equip providers, deployers and affected persons with the necessary notions to make informed decisions regarding AI systems. These notions may vary with regard to the relevant context and can include understanding the correct application of technical elements during the AI system's development phase, the measures to be applied during its use, the suitable ways in which to interpret the AI system's output, and, in the case of affected persons, the knowledge necessary to understand how decisions taken with the assistance of AI will impact them. In the context of the application this Regulation, AI literacy should provide all relevant actors in the AI value chain with the insights required to ensure the appropriate compliance and its cor-

rect enforcement. Furthermore, the wide implementation of AI literacy measures and the introduction of appropriate follow-up actions could contribute to improving working conditions and ultimately sustain the consolidation, and innovation path of trustworthy AI in the Union. The European Artificial Intelligence Board should support the Commission, to promote AI literacy tools, public awareness and understanding of the benefits, risks, safeguards, rights and obligations in relation to the use of AI systems. In cooperation with the relevant stakeholders, the Commission and the Member States should facilitate the drawing up of voluntary codes of conduct to advance AI literacy among persons dealing with the development, operation and use of AI" (European Parliament 2024b: S. 11).

Was folgt nun aus den allgemeinen Grundsätzen? Für den Rechtsausschuss sollten sich diese in einem eigens hierzu erarbeiteten Artikel 4 b widerspiegeln. Demnach ist es die Aufgabe der EU und ihrer Mitgliedstaaten, *AI Literacy* zu fördern, um eine demokratische Kontrolle von KI-Systemen zu ermöglichen. Auch Anbieter:innen und Nutzer:innen stehen hier in der Verantwortung, Grundbegriffe und Kenntnisse über KI-Systeme zu vermitteln und zu lernen. Nicht zuletzt ist dies auch eine Voraussetzung, um die Einhaltung und Durchsetzung der Verordnung selbst zu gewährleisten.

„Amendment 43: Proposal for a regulation - Article 4 b (new)
Article 4 b – AI Literacy
When implementing this Regulation, the Union and the Member States shall promote measures and tools for the development of a sufficient level of AI literacy, across sectors and taking into account the different needs of groups of providers, users and affected persons concerned, including through education and training, skilling and reskilling programmes and while ensuring proper gender and age balance, in view of allowing a democratic control of AI systems.
Providers and user of AI systems shall promote tools and take measures to ensure a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the environment the AI systems are to be used in, and considering the persons or groups of persons on which the AI systems are to be used.
Such literacy tools and measures shall consist, in particular, of the teaching and learning of basic notions and skills about AI systems and their

functioning, including the different types of products and uses, their risks and benefits and the severity of the possible harm they can cause and its probability of occurrence.
A sufficient level of AI literacy is one that contributes, as necessary, to the ability of providers and users to ensure compliance and enforcement of this Regulation" (Committee on Legal Affairs 2022: S. 25 f.).

Das Parlament schließt sich den Einlassungen des Rechtsausschusses an und übernimmt diese weitestgehend, ersetzt unter Ziffer 2 allerdings *user* durch *deployer*.

"Amendment 214: Proposal for a regulation - Article 4 b (new)
Article 4 b – AI Literacy
When implementing this Regulation, the Union and the Member States shall promote measures for the development of a sufficient level of AI literacy, across sectors and taking into account the different needs of groups of providers, deployers and affected persons concerned, including through education and training, skilling and reskilling programmes and while ensuring proper gender and age balance, in view of allowing a democratic control of AI systems.
Providers and deployers of AI systems shall take measures to ensure a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on which the AI systems are to be used.
Such literacy measures shall consist, in particular, of the teaching of basic notions and skills about AI systems and their functioning, including the different types of products and uses, their risks and benefits.
A sufficient level of AI literacy is one that contributes, as necessary, to the ability of providers and deployers to ensure compliance and enforcement of this Regulation" (European Parliament 2023: S. 130 f.).

Aus dem *Provisional Agreement* wird ersichtlich, dass sich das Parlament (und der Rechtsauschuss) in weiten Teilen auch hier nicht durchsetzen konnten. Dass die EU und ihre Mitgliedstaaten einen Beitrag zur *AI Literacy* leisten sollen, ist demnach nicht mehr vorgesehen. Nur *providers and deployers* stehen zukünftig in der Verantwortung, Grundlagenwissen für den Betrieb und die Nutzung von KI-Systemen innerhalb der eigenen Belegschaft zu fördern. Voraussetzungen für die Ausübung der demokratischen

Kontrolle und für die Einhaltung sowie Durchsetzung der Verordnung müssen im Sinne des Artikels 4 b und im Ergebnis der EU AI-Acts damit zukünftig nicht geschaffen werden:

> „Article 4 b – AI Literacy
> Providers and deployers of AI systems shall take measures to ensure, to their best extent, a sufficient level of AI literacy of their staff and other persons dealing with the operation and use of AI systems on their behalf, taking into account their technical knowledge, experience, education and training and the context the AI systems are to be used in, and considering the persons or groups of persons on which the AI systems are to be used" (European Parliament 2024b: S. 93) .

Ein Blick in das „AIAct_four-column document" des Journalisten Luca Bertuzzi verrät auch hier, dass weder im Ursprungsentwurf der Kommission noch im Entwurf des Rates die Idee der Förderung von AI Literacy für eine Befähigung der europäischen Bevölkerung eine Rolle gespielt haben (Bertuzzi 2023).

4. Verhaltenskodizes für nachhaltige und inklusive Gestaltungsansätze

Wie in der Einleitung bereits erwähnt, ist gesellschaftliches und ökologisches Wohlergehen eine Kernforderung der HEG-KI (Hochrangige Expertengruppe 2019a: S. 29 f.). Für die Expert:innen bedeutet dies, dass nicht nur die Daten so inklusiv wie möglich sein müssen, sondern die Berücksichtigung und Einbindung aller betroffenen Interessenträger:innen während des gesamten KI-Lebenszyklus und die Sicherstellung eines gleichberechtigten Zugangs durch inklusive Gestaltungsprozesse zu erfolgen hat (Hochrangige Expertengruppe 2019a: S. 13 u. 22). Es ist wichtig, so die Expert:innen weiter, dass die Teams, die nunmehr immer autonomere KI-Systeme entwerfen, entwickeln, erproben, warten, bereitstellen und/oder beschaffen, die Vielfalt der Nutzer:innen und die Gesellschaft im Allgemeinen widerspiegeln (Hochrangige Expertengruppe 2019a: S. 29). „Dazu zählt auch die Berücksichtigung der natürlichen Umwelt und anderer Lebewesen, die Teil des menschlichen Ökosystems sind, sowie ein nachhaltiger Ansatz, der das Gedeihen zukünftiger Generationen ermöglicht" (Hochrangige Expertengruppe 2019a: S. 48).

Ein Verweis auf diese Grundsätze findet sich bereits in der ersten Entwurfsfassung der Kommission wieder. Allerdings soll es sich hier nicht um

verpflichtende Mindestmaßnahmen handeln – wie etwa die Transparenzpflichten für gewisse KI-Systeme nach Artikel 52 (European Commission 2021: S. 76) oder die verpflichtenden Anforderungen an Hochrisiko-KI-Systeme entsprechend Kapitel 2 (European Commission 2021: S. 52 ff.) – sondern um freiwillige Verhaltenskodizes. Demnach wäre es wünschenswert, weitere Anforderungen zu erfüllen, die sich beispielsweise auf die ökologische Nachhaltigkeit, die barrierefreie Zugänglichkeit für Menschen mit Behinderungen, die Beteiligung von Interessenträger:innen an der Konzeption und Entwicklung von KI-Systemen oder die Vielfalt der Entwicklungsteams beziehen (European Commission 2021: S. 79). Diese freiwilligen Verhaltenskodizes können dann von den KI-System-Anbietenden oder deren Interessenvertretungen selbst aufgestellt werden (ebd.):

> „Article 69 – Codes of Conduct
> 1. …
> 2. The Commission and the Board shall encourage and facilitate the drawing up of codes of conduct intended to foster the voluntary application to AI systems of requirements related for example to environmental sustainability, accessibility for persons with a disability, stakeholders participation in the design and development of the AI systems and diversity of development teams on the basis of clear objectives and key performance indicators to measure the achievement of those objectives.
> 3. Codes of conduct may be drawn up by individual providers of AI systems or by organisations representing them or by both, including with the involvement of users and any interested stakeholders and their representative organisations. Codes of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems" (European Commission 2021: S. 80).

Der Rat übernimmt im Wesentlichen den Vorschlag der Kommission und ergänzt im Sinne einer wirtschaftsinnovativen Exzellenz, dass jene freiwilligen Verhaltenskodizes die spezifischen Interessen und Bedürfnisse von KMUs und Start-Ups berücksichtigen sollten und auch die Pflichten der Nutzer:innen im Zusammenhang mit KI-Systemen in den Blick zu nehmen seien. Verbraucher:innenschutz wird hier also zu einer Verbraucher:innenpflicht. Im Sinne einer souveränen Handlungskompetenz für nachhaltige Entwicklung ist dies ein zwar berechtigtes Anliegen, wirkt im beschriebenen Kontext aber fast ein bisschen zynisch. So sollen also jene Nutzer:innen, deren Perspektiven aufgrund von Barrieren und nicht-inklusiven, nicht-nachhaltigen Strukturen ungehört bleiben, entsprechend

stärker verpflichtet werden, sich einzubringen. Als läge das Problem einer mangelnden Beteiligung ursächlich an einem fehlenden Engagement oder Beteiligungswillen eben jener Personengruppe. Das ist ein bemerkenswerter Ansatz:

> "Article 69 – Codes of conduct for voluntary application of specific requirements
> 1. …
> 2. The Commission and the Member States shall facilitate the drawing up of codes of conduct intended to encourage the voluntary application to all AI systems of specific requirements related, for example, to environmental sustainability, including as regards energy-efficient programming, accessibility for persons with a disability, stakeholders participation in the design and development of the AI systems and diversity of development teams on the basis of clear objectives and key performance indicators to measure the achievement of those objectives. The Commission and the Member States shall also facilitate, where appropriate, the drawing of codes of conduct applicable on a voluntary basis with regard to users' obligations in relation to AI systems.
> 3. Codes of conduct applicable on a voluntary basis may be drawn up by individual providers of AI systems or by organisations representing them or by both, including with the involvement of users and any interested stakeholders and their representative organisations, or, where appropriate, by users with regard to their obligations. Codes of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems.
> 4. The Commission and the Member States shall take into account the specific interests and needs of SME providers, including start-ups, when encouraging and facilitating the drawing up of codes of conduct referred to in this Article "(Council of the European Union 2022: S. 175)."

Im Entwurf des Parlaments spiegelt sich ein deutlicher Neuformulierungsansatz wider, der erneut die ethischen Prinzipien der HEG-KI stärker und expliziter aufnimmt. Auch der Ansatz zur Förderung einer allgemeinen AI Literacy wird hier wieder aufgenommen, die Anforderungen an gesellschaftliches und ökologisches Wohlergehen stärker betont. An der Freiwilligkeit dieser Verhaltenskodizes will auch das Parlament nichts ändern. Gleichwohl sollen an der Erarbeitung der Verhaltenskodizes nun auch Wissenschaftler:innen, Gewerkschafter:innen und Verbraucher:innenschützer:innen beteiligt werden.

"Amendments 634, 635, 636: Proposal for a regulation – Article 69 – paragraph 2-4
2. Codes of conduct intended to foster the voluntary compliance with the principles underpinning trustworthy AI systems, shall, in particular:
(a) aim for a sufficient level of AI literacy among their staff and other persons dealing with the operation and use of AI systems in order to observe such principles;
(b) assess to what extent their AI systems may affect vulnerable persons or groups of persons, including children, the elderly, migrants and persons with disabilities or whether measures could be put in place in order to increase accessibility, or otherwise support such persons or groups of persons;
(c) consider the way in which the use of their AI systems may have an impact or can increase diversity, gender balance and equality;
(d) have regard to whether their AI systems can be used in a way that, directly or indirectly, may residually or significantly reinforce existing biases or inequalities;
(e) reflect on the need and relevance of having in place diverse development teams in view of securing an inclusive design of their systems;
(f) give careful consideration to whether their systems can have a negative societal impact, notably concerning political institutions and democratic processes;
(g) evaluate how AI systems can contribute to environmental sustainability and in particular to the Union's commitments under the European Green Deal and the European Declaration on Digital Rights and Principles.
3. Codes of conduct may be drawn up by individual providers of AI systems or by organisations representing them or by both, including with the involvement of users and any interested stakeholders, including scientific researchers, and their representative organisations, in particular trade unions, and consumer organisations. Codes of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems. Providers adopting codes of conduct will designate at least one natural person responsible for internal monitoring.
4. The Commission and the AI Office shall take into account the specific interests and needs of SMEs and start-ups when encouraging and facilitating the drawing up of codes of conduct " (European Parliament 2023: S. 300. ff.).

Im *Provisional Agreement* wird deutlich, dass sich an dieser Stelle das Parlament stärker durchsetzen konnte. Der Verweis auf ethische Grundsätze und Kernforderungen in Anlehnung an das HEG-KI findet sich im finalen Gesetzentwurf damit als freiwillige Auflage zukünftig zu erarbeitender Verhaltenskodizes wieder. Diese Erarbeitung soll dann auch unter Beteiligung zivilgesellschaftlicher Organisationen erfolgen:

> "Article 69 – Codes of conduct for voluntary application of specific requirements
> 1. …
> 2. The AI Office and the Member States shall facilitate the drawing up of codes of conduct concerning the voluntary application, including by deployers, of specific requirements to all AI systems, on the basis of clear objectives and key performance indicators to measure the achievement of those objectives, including elements such as, but not limited to:
> (a) applicable elements foreseen in European ethic guidelines for trustworthy AI;
> (b) assessing and minimizing the impact of AI systems on environmental sustainability, including as regards energy-efficient programming and techniques for efficient design training and use of AI;
> (c) promoting AI literacy, in particular of persons dealing with the development, operation and use of AI;
> (d) facilitating an inclusive and diverse design of AI systems, including through the establishment of inclusive and diverse development teams and the promotion of stakeholders' participation in that process;
> (e) assessing and preventing the negative impact of AI systems on vulnerable persons or groups of persons, including as regards accessibility for persons with a disability, as well as on gender equality.
> 3. Codes of conduct may be drawn up by individual providers or deployers of AI systems or by organisations representing them or by both, including with the involvement of deployers and any interested stakeholders and their representative organisations, including civil society organisations and academia. Codes of conduct may cover one or more AI systems taking into account the similarity of the intended purpose of the relevant systems.
> 4. The AI Office, and the Member States shall take into account the specific interests and needs of SMEs, including start-ups, when encouraging and facilitating the drawing up of codes of conduct " (European Parliament 2024b: S. 199).

Im Vergleich der Positionen aller beteiligten Institutionen wird deutlich, dass zwar alle Akteur:innen die Idee von nachhaltigen und inklusiven Ansätzen benennen und aufgreifen, sich verpflichtende Ansätze für KI-Systeme aber aus keinem der hierfür eingebrachten Entwürfe ableiten lassen. Im Ergebnis bleibt darüber hinaus für alle vorgestellten Entwürfe einigermaßen unklar, wer die freiwilligen Verhaltenskodizes am Ende umsetzen soll. Es werden lediglich unterschiedliche Akteurskonstellationen benannt, die bei der Erarbeitung der Kodizes beteiligt werden sollten. Im *Provisional agreement* heißt es dann lediglich „*voluntary application, including by deployers*" (European Parliament 2024b: S. 11). Welche weiteren Akteurskonstellationen sich darüber hinaus sinnvollerweise angesprochen fühlen könnten, bleibt also weitestgehend unklar.

5. Analyse und Fazit

Das Ziel des Beitrages ist es, den europäischen Gesetzgebungsprozess zu KI am Beispiel des EU AI-Acts in Bezug auf das Versprechen einer nachhaltigen und inklusiven Gestaltung von KI-Systemen kritisch zu analysieren. Die Leitfrage lautet: (Wo) Gibt es verbindliche Anforderungen zur nachhaltigen und inklusiven Gestaltung von KI-Systemen in der europäischen Regulierung?

Hierfür wurden die Verordnungsentwürfe der EU-Kommission (2021), des Rates der EU (2022), des EU-Parlaments (2023) und des Trilogs – hier als *Provisional agreement resulting from interinstitutional negotiations* (European Parliament 2024b) – gegenübergestellt.

Als Referenz für nachhaltige und inklusive Ansätze wurden die Ethik-Leitlinien für eine vertrauenswürdige KI der im Zuge des Policy-Prozesses eingesetzten HEG-KI (Hochrangige Expertengruppe 2019a) herangezogen. Dass sich im Zuge der Agenda-Setzung ein inter-institutioneller, hier zunächst politischer, Konsens der EU-Institutionen dokumentieren lässt, der u. a. nachhaltige und inklusive Ansätze samt inklusiver Gestaltungsprozesse für KI-Welten vorsieht, wurde als Teil der Einleitung herausgearbeitet. Zu Fragen bleibt, ob sich diese Absichten auch in den konkreten Anforderungen eines entsprechend verbindlichen Rechtsaktes widerspiegeln. Im Ergebnis der Analyse lautet die Antwort auf diese Frage: Eher nicht, d. h. konkrete, also verbindliche Anforderungen in Bezug auf nachhaltige und inklusive Gestaltungsansätze von KI-Systemen lassen sich über die vorge-

sehene Möglichkeit der Erarbeitung von freiwilligen Verhaltenskodizes hinaus im wahrscheinlich abschließenden Gesetzestext nicht identifizieren.

Mit Art. 69 der Verordnung gibt es zwar grundsätzlich einen Ansatz, dieser ist indes freiwillig. Ob und inwiefern von dieser Möglichkeit zukünftig überhaupt Gebrauch gemacht wird, bleibt abzuwarten. Es entsteht der Eindruck, dass es sich bei diesem Artikel um ein klassisches Feigenblatt handelt. Im schlechtesten Fall würde dies in der Praxis dazu führen, dass inklusive und nachhaltige Gestaltungsansätze eben nicht umgesetzt werden.

Auch der aus bildungswissenschaftlicher Sicht nachvollziehbare und gebotene Ansatz der HEG-KI, dass „(g)rundlegende KI-Kompetenzen […] in der gesamten Gesellschaft gefördert werden", wird im AI-Act nicht verankert (vgl. Hochrangige Expertengruppe 2019a: S. 29). Die vom Parlament zunächst übernommene und eingebrachte Vorstellung, wonach es die Aufgabe der EU und ihrer Mitgliedstaaten sei, *AI Literacy* zu fördern, findet sich im Gesetzestext nicht wieder. Nur *providers and deployers* stehen zukünftig in der Verantwortung, Grundlagenwissen für den Betrieb und die Nutzung von KI-Systemen innerhalb der eigenen Belegschaft zu fördern (European Parliament 2023: S. 167. f.). Die Förderung von *AI Literacy* wird hier also im Wesentlichen und zweckgebunden an die Wirtschaft übertragen.

Zusammenfassend entsteht der Eindruck, dass der Gesetzgeber in Bezug auf nachhaltige und inklusive Ansätze für gemeinsame KI-Systeme verbindliche Regelungen vermeidet und ein supranationales bzw. nationales Bekenntnis zur staatlichen Förderung von KI-Kompetenzen in der Bevölkerung als Anspruch aus der in Rede stehenden Verordnung unterlässt. Zwar erlaubt die hier vorliegende Analyse kein grundsätzliches Urteil über den EU AI-Act, der als weltweit erster Regulierungsansatz für KI – so die Meinung der Autor:innen – durchaus zu beeindrucken vermag, in Bezug auf nachhaltige und inklusive Ansätze für gemeinsame IT-Welten ist die hier vorliegende Analyse dennoch ernüchternd.

Literatur

Bertuzzi, Luca (2023): AIAct_final_four-columns21012024.pdf. www.linkedin.com/posts/luca-bertuzzi-186729130_aiactfinalfour-column21012024pdf-activity-7155091883872964608-L4Dn?utm_source=share&utm_medium=member_desktop (Abfrage 28.05.2023).

Committee on Legal Affairs (2022): Opinion of the Committee on Legal Affairs for the Committee on the Internal Market and Consumer Protection and the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). 12.9.2022. https://artificialintelligenceact.eu/wp-content/uploads/2022/09/AIA-JURI-Rule-57-Opinion-Adopted-12-September.pdf www.europarl.europa.eu/doceo/document/JURI-PA-719827_EN.pdf (Abfrage 28.06.2024).

Council of the European Union (2022): Proposal for a Regulation of the European Parliament and of the Councillaying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts – General. data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf (Abfrage 28.05.2023).

Council of the European Union (2024a): Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI. Press release. www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/ (Abfrage 31.05.2024).

Council of the European Union (2024b): Note. From: Presidency. To: Permanent Representative Committee. No. Cion doc.: 8115/21. Subject: Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts - Analysis of the final compromise text with a view to agreement-Brussels, 26 January 2024 (OR. en). 5662/24. LIMITE.

EUR-Lex (2024): Glossary of Summaries. Trilog. eur-lex.europa.eu/DE/legal-content/glossary/trilogue.html (Abfrage: 28.02.2024).

Euractiv (2023): European Union squares the circle on the world's first AI rulebook. www.euractiv.com/section/artificial-intelligence/news/european-union-squares-the-circle-on-the-worlds-first-ai-rulebook (Abfrage: 28.02.2024).

Europäische Kommission (2018): Mitteilung der Kommission an das Europäischen Parlaments, den Europäischen Rat, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Koordinierter Plan für künstliche Intelligenz. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0795 (Abfrage: 15.05.2022).

Europäische Kommission (2020): Weissbuch. Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_de (Abfrage 28.05.2023).

Europäischer Wirtschafts- und Sozialausschuss, EWSA (2016): Künstliche Intelligenz – die Auswirkungen der künstlichen Intelligenz auf den (digitalen) Binnenmarkt sowie Produktion, Verbrauch, Beschäftigung und Gesellschaft (Initiativstellungnahme), https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/artificial-intelligence-consequences-artificial-intelligence-digital-single-market-production-consumption-employment-and (Abfrage 15.05.2023).

Europäische Kommission (2018): Koordinierter Plan für künstliche Intelligenz. COM(2018) 795 final. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0795 (Abfrage: 15.05.2022).

Europäische Kommission (2020): Weissbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen. ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_de (Abfrage 28.05.2023).

European Commission (2021): Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206 (Abfrage 03.06.2023).

European Parliament (2020): Legislative Entschließung des Europäischen Parlaments vom 20. Oktober 2020 mit Empfehlungen an die Kommission zu dem Rahmen für die ethischen Aspekte von künstlicher Intelligenz, Robotik und damit zusammenhängenden Technologie. europarl.europa.eu/doceo/document/TA-9-2020-0275_DE.html (Abfrage 28.05.2023).

European Parliament (2023): Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html (Abfrage 03.06.2023).

European Parliament (2024a): Gesetz über künstliche Intelligenz: Parlament verabschiedet. Pressemittelung. https://www.europarl.europa.eu/news/de/press-room/20240308IPR19015/gesetz-uber-kunstliche-intelligenz-parlament-verabschiedet-wegweisende-regeln (Abfrage 16.05.2024).

European Parliament (2024b): Provisional agreement resulting from interinstitutional negotiations. Proposal for a regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts 2021/0106(COD)(COM(2021)0206 – C9-0146(2021) – 2021/0106(COD)). www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/CJ40/AG/2024/02-13/1296003EN.pdf (Abfrage 28.02.2024).

Hochrangige Expertengruppe (2019a): Unabhängige Hochrangige Expertengruppe für Künstliche Intelligenz. Eingesetzt durch die Europäische Kommission im Juni 2018. Ethik-Leitlinien für eine vertrauenswürdige KI, op.europa.eu/de/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1 (Abfrage: 17.05.2022).

Hochrangige Expertengruppe (2019b): Unabhängige Hochrangige Expertengruppe für Künstliche Intelligenz. Eingesetzt durch die Europäische Kommission im Juni 2018. Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete. Für die Zwecke der Gruppe entwickelte Definition, https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf (Abfrage: 17.05.2024).

Hochrangige Expertengruppe (2020): Independent High-Level Expert Group on Artificial Intelligence. Set up by the European Commission. The assessment List for Trustworthy Artificial Intelligence (ALTAI) for self assessment, digital-strategy.ec.europa.eu/de/node/806 (Abfrage: 17.05.2022).

Legislative Observatory (2024): 2021/0106(COD). Artificial Intelligence Act. https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0106(COD)&l=en (Abfrage 28.02.2024).

Legislative Train Schedule (2024): Artificial Intelligence act. In "A Europe for the Digital Age". https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence (Abfrage 28.02.2024)

Sabatier, Paul A. (2007): The Need for Better Theories, in: Sabatier, P.A. (ed.). *Theories of the Policy Process*. 2nd Edition. Boulder: Westview Press, S. 3-17.

Wedel, Marco (2023): Digitalisierung, Künstliche Intelligenz und die Rolle der Arbeitslehre - Ein methodischer Ansatz für eine Kritikalitätsbewertung von KI im Unterricht. In: Bartsch, Silke und Friese, Marianne (Hrsg.): *Fachdidaktik Arbeitslehre - Grundlagen und Impulse*. Bielefeld: wbv. S. 67-83. DOI: http://doi.org/10.3278/9783763974559.

Öffentliche Verwaltung als Katalysator für selbstbestimmtes Datenteilen: Digitale Nachweise auf Basis von Registerdaten

Gunnar Hempel, Michael Kubach

Zusammenfassung

In einer Kooperation der beiden Schaufensterprojekte ID-Ideal und ONCE wird im Rahmen des Förderprogramms „Sichere Digitale Identitäten" des Bundesministeriums für Wirtschaft und Klimaschutz mit der „kommunalen Datenkarte" eine digitale Identitätslösung pilotiert und evaluiert, die Bürgern ein Werkzeug an die Hand gibt, digitale Nachweise zu generieren und die Weitergabe von Daten und Nachweisen selbst zu bestimmen. Die Lösung basiert auf einem Self-Sovereign Identity (SSI) Ansatz und einer Identity Wallet Applikation, die auf allen Android und Apple Smartphones mit aktuellen Betriebssystemversionen lauffähig ist. Ziel ist es, ein ausreichend hohes Sicherheits- und Datenschutzniveau mit einer niedrigen Schwelle für die Nutzerinnen und Nutzer zu kombinieren.

In beiden Schaufensterprojekten spielt die Vernetzung kommunaler Dienstleistungen eine wichtige Rolle. Dazu gehören neben Verwaltungsdienstleistungen im engeren Sinne auch Angebote wie der öffentliche Personennahverkehr, Stadtbibliotheken, Museen und Sporteinrichtungen. Die Digitalisierung dieser Dienstleistungen ist eine zentrale Aufgabe. Die Bereitstellung und Verwaltung geprüfter Nachweise mit möglichst geringem Zeit- und Arbeitsaufwand für alle Akteure ist in diesem Ökosystem von entscheidender Bedeutung. Mit der kommunalen Datenkarte kann der Bürger diese Nachweise nun selbst kontrollieren und für die Inanspruchnahme kommunaler Dienstleistungen nutzen. Die so erhaltenen Daten genießen ein hohes Maß an Vertrauen und Glaubwürdigkeit, da sie aus kommunal geführten Registern stammen.

1. Einleitung

Die Digitalisierung von Verwaltungsprozessen ist ein elementares Ziel, um öffentliche Dienstleistungen effizienter, zugänglicher und benutzerfreund-

licher zu gestalten. Dies gilt insbesondere auch für die kommunale Daseinsvorsorge. Im Rahmen der kommunalen Daseinsvorsorge stellen Gemeinden wirtschaftliche, soziale und kulturelle Dienstleistungen für ihre Bürger, z. B. durch öffentliche Einrichtungen oder Infrastruktur im öffentlichen Interesse, bereit. Für zahlreiche Anwendungsfälle werden Sondernutzungsmöglichkeiten und Tarifmodelle angeboten, die sich an Nutzereigenschaften orientieren. Bestimmte Personengruppen erhalten beispielsweise Ermäßigungen oder haben gesonderten Zugang. Um diese Leistungen in Anspruch zu nehmen, sind in der Regel Nachweise zu erbringen, beispielsweise durch einen Sozialpass, einen Schülerausweis oder auch durch den Nachweis, in einer Gemeinde gemeldet zu sein. Hierfür ist die Verarbeitung von personenbezogenen Daten der Bürger erforderlich. Die Erbringung der Nachweise erfolgt heute noch überwiegend auf analogem Wege, durch persönliche Vorlage bzw. Abholung entsprechender Dokumente, seltener auf dem Postweg. Dies belastet Verwaltungen angesichts einer angespannten Personaldecke und stellt eine Hürde für Bürger dar, ihnen zustehende Leistungen in Anspruch nehmen zu können. Auch der weitere Kontext der (stockenden) Digitalisierung der Verwaltung ist hier zu betrachten. Das Onlinezugangsgesetz (OZG) sollte eigentlich die Verfügbarkeit von digitalen Verwaltungsleistungen verbessern. In der Umsetzung konnte es jedoch trotz „Booster" die gesteckten Ziele nicht erreichen (Röhl 2023), so dass ein OZG 2.0 erarbeitet wurde.[1]

Eine zentrale Herausforderung bei der Digitalisierung von Verwaltungsdienstleistungen ist die Verfügbarkeit geeigneter digitaler Nachweise für die Bürger. Die Online-Ausweisfunktion des Personalausweises (eID), die als universelles und sicheres Identifizierungsmittel für verschiedene Online-Dienste fungieren könnte, findet bisher nur geringe Nutzung unter den Bürgern (und ist auch für viele Diensteanbieter aufwändig einzubinden). Obwohl technisch jeder Personalausweis dazu fähig ist (Stand Juni 2023 waren rund 62 Millionen gültige Personalausweise im Umlauf, rund 88 % mit aktivierter Online-Ausweisfunktion – ca. 55 Millionen) (Krempl 2023), haben laut eGovernment Monitor nur 14 % der in 2023 befragten Bürger die Funktion jemals genutzt. Dies liegt unter anderem an der mangelnden Bekanntheit seiner Funktionen, geringer Unterstützung durch Diensteanbieter, eines nicht wahrgenommenen Nutzens sowie einer

1 Dieses scheiterte jedoch im März 2024 im Bundesrat und bei Verfassung dieses Beitrages war die weitere Entwicklung unklar.

oft als umständlich wahrgenommenen Handhabung – auch wenn diese in der letzten Zeit immer weiter vereinfacht wurde. Mangelndes Vertrauen spielt nur eine untergeordnete Rolle (D21/TU München 2023). Das Vorhaben der Entwicklung einer etwas Nutzerfreundlicheren Smart-eID, welche die Übertragung der Online-Ausweisfunktion auf das Smartphone in ein zertifiziertes sicheres Hardwareelement (ausschließlich für die Online-Nutzung) ermöglichen hätte sollen, wurde Ende 2023 gestoppt (Steiner 2023). Derzeit läuft die Entwicklung einer European Digital Identity Wallet (EUDI Wallet), die auch der deutsche Staat seinen Bürgern anbieten und in seine Verwaltungsleistungen einbinden soll. Diese Entwicklung wird jedoch nach aktuellem Zeitplan frühestens 2026/2027 abgeschlossen sein (European Commission 2024). Die Folge ist, dass vielen Bürgern derzeit faktisch die Grundlage fehlt, um von digitalen Verwaltungsdienstleistungen vollumfänglich profitieren zu können.[2] Um diese Hürde zu überwinden, bedarf es einer gezielten Strategie: Einerseits muss die Benutzerfreundlichkeit des digitalen Personalausweises verbessert werden, um die Akzeptanz und Nutzungsbereitschaft zu erhöhen. Andererseits können jedoch auch alternative digitale Identitätsnachweise, wie die im Folgenden beschriebene „kommunale Datenkarte", gefördert und ihre Anwendung vereinfacht werden, um eine breitere Basis für digitalen Zugang zu Dienstleistungen zu schaffen, die nicht unbedingt das hohe Vertrauensniveau des Personalausweises mit Online-Ausweisfunktion benötigen. Eine Kombination aus technischer Optimierung und der Schaffung von diversen, benutzerorientierten Identifikationsmöglichkeiten könnte die Teilhabe aller Bürger an der digitalen Verwaltung verbessern.[3]

Vor diesem Hintergrund gewinnt außerdem die Wahrung des Datenschutzes eine zusätzliche Dimension. Personenbezogene Daten, deren Verarbeitung für den Erhalt kommunaler Leistungen oftmals erforderlich sind, müssen geschützt werden, um das Vertrauen der Bürger in digitale Verwaltungsprozesse zu stärken. Im Sinne des Grundrechts auf informationelle Selbstbestimmung soll es jeder betroffenen Person möglich sein, grundsätzlich selbst über die Verarbeitung ihrer personenbezogenen Daten zu bestimmen. Die Europäische Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG) und die für die Verwaltung der Länder

2 Diese steht aber auch einer mangelhaften verwaltungsinternen Digitalisierung gegenüber – letztlich handelt es sich um ein Art Henne-Ei-Problem.

3 Andere europäische Länder, etwa die Nachbarn Österreich und Dänemark, sind hier bedeutend weiter.

geltenden jeweiligen Datenschutzgesetze geben diesbezüglich zahlreiche Vorgaben für die Verarbeitung personenbezogener Daten vor. Dies betrifft insbesondere die Rechtsgrundlagen für die Verarbeitungen, Vorgaben für Informationsvermittlung und Auskunftserteilung zu den Verarbeitungen sowie Vorgaben zu technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten.

Das in diesem Beitrag vorgestellte Konzept einer „kommunalen Datenkarte" als digitales Äquivalent zu herkömmlichen Nachweisen verfolgt daher zwei wesentliche Ziele: die Vereinfachung des Zugangs zu kommunalen Leistungen und die strikte Einhaltung des Datenschutzes. Durch die Verwendung von Self-sovereign Identity Technologie können Bürger ihre Daten sicher in einer digitalen Wallet auf ihrem Smartphone verwalten und bei Bedarf vorlegen, ohne mehr Daten als notwendig preiszugeben.[4] Dies stellt einen wichtigen Schritt in Richtung einer modernen, serviceorientierten und datenschutzkonformen Verwaltung dar.

Das Ziel des Beitrags ist es, das Konzept der kommunalen Datenkarte zur Diskussion zu stellen. Zunächst erfolgt eine eingehendere Darstellung der Motivation für das gewählte Konzept angesichts vorhandener Alternativen sowie eine Skizzierung der technischen Realisierung. Anschließend wird auf die Pilotierung im Rahmen der Schaufensterprojekte „Sichere Digitale Identitäten" (SDI-Schaufenster) des Bundesministeriums für Wirtschaft und Klimaschutz (Bundesministerium für Wirtschaft und Klimaschutz 2024) eingegangen. Hiervon abgeleitet werden schlussendlich Thesen, die Potenziale und Herausforderungen der kommunalen Datenkarte zusammenfassen.

4 Als Folge des Digital Markets Acts der EU (DMA 2022) lassen sich Applikationen auf Smartphones auch ohne Nutzung eines App-Stores der Smartphone-(Betriebssystem-)Herstellern installieren. Die ID-Daten der Nutzenden werden beim Self-Sovereign Identity Ansatz (siehe Abschnitt 2.2) auf dem Smartphone verwaltet und nicht zu den Smartphone-(Betriebssystem-)Herstellern übertragen. Es existieren Android Smartphones, welche sich vollständig ohne Google Account nutzen lassen. Insofern besteht bei der ohnehin optionalen Nutzung digitaler Wallets auf aktuellen Smartphones weder ein Zwang zur Nutzung von App-Stores, noch ein Zwang zu Konten bei Apple und Google.

2. Die Kommunale Datenkarte: Konzept, Umsetzung und Pilotierung

In einer Kooperation der beiden Schaufensterprojekte ID-Ideal[5] und ONCE[6] wird im Rahmen des Förderprogramms „Sichere Digitale Identitäten" des Bundesministeriums für Wirtschaft und Klimaschutz mit dem Konzept der „kommunalen Datenkarte" seit 2021 eine digitale Identitätslösung entwickelt und evaluiert, die Bürgern ein Werkzeug an die Hand gibt, digitale Nachweise auf Basis kommunaler Registerdaten (z. B. aus dem Melderegister für Daten und dem Passregister für Lichtbild) zu erzeugen und die Weitergabe von Daten und Nachweisen selbst zu bestimmen. In beiden Schaufensterprojekten spielt die Erleichterung der digitalen Bereitstellung kommunaler Dienstleistungen eine große Rolle. Dazu gehören neben Verwaltungsleistungen im engeren Sinne auch Angebote wie öffentlicher Nahverkehr, städtische Bibliotheken, Museen und sportliche Einrichtungen. Die Nutzung dieser Dienstleistung ist in der Regel an den Nachweis bestimmter Merkmale gebunden. Dieser wird klassisch durch Vorlage und Sichtprüfung von Dokumenten, wie einer Meldebescheinigung, eines Bibliotheksausweises etc. erbracht. Die Digitalisierung der Dienstleistungen erfordert die Übertragung dieses Vorganges in digitale Prozesse, um keinen Medienbruch zu erzeugen und diese Leistungen werden teilweise online, aber auch vor Ort erbracht. Ein digitaler Nachweis auf dem Smartphone sollte sich also online, aber auch vor Ort nutzen lassen (Beispiel: Ausleihe eines digitalen Buches von Zuhause, aber auch Ausleihe eines physischen Buches in der Bibliothek). Die digitale Bereitstellung und Verwaltung geprüfter Nachweise mit möglichst geringem Zeit- und Arbeitsaufwand für alle Akteure ist damit in diesem Ökosystem von entscheidender Bedeutung. Das folgende Kapitel diskutiert zunächst knapp, ob für die Digitalisierung der deutschen Verwaltung tatsächlich noch eine weitere digitale Identitätslösung notwendig ist und stellt dann das Konzept der kommunalen Datenkarte vor.

2.1 Noch eine weitere Identitätslösung?

Sinn und Zweck der kommunalen Datenkarte ist es, mit der Lösung einen in mehrfacher Hinsicht niederschwelligen digitalen Nachweis zu ent-

5 https://id-ideal.de
6 https://once-identity.org

wickeln. Niederschwellig, um Hürden der Digitalisierung für den Nutzer (aber auch hinsichtlich der Einbindung in die Prozesse der Diensteanbieter, siehe unten) abzubauen. Hier kann die Verwendung einer Smartphone-App (kommunale Datenkarte) mit einer angebundenen Wallet einen nutzerfreundlichen Einstieg schaffen, der aus der Verwendung von existierenden Smartphone Wallets beispielsweise für Kino- und Flugtickets bekannt ist. Die Nutzung der Corona-Warn-App mit Impfnachweis während der Covid-19 Lockdowns hat die Bürger zudem an den Umgang mit Nachweisen auf dem Smartphone und die Interaktion mit QR-Codes gewöhnt, so dass es sich hier für sie um ein vertrautes Interaktionsparadigma handelt. Smartphone Wallets nach dem Self-Sovereign-Identity Prinzip stellen zudem die Kontrolle des Nutzers über seine Daten und deren Verwendung ins Zentrum. Der Nutzer sieht und bestimmt, welche Daten er für welche Dienstleistung er an welche Organisation freigibt und erhält eine Historie seiner Nutzungen. Der Wallet-Ansatz kann potenziell für ein breites bzw. wachsendes Spektrum von Dienstleistungen eingesetzt werden. Die Bedienungsoberfläche einer Wallet kann fortlaufend an die Bedürfnisse von Nutzern und mögliche Erweiterungen des Funktionsumfangs angepasst werden, ohne dass sich der Nutzer grundlegend umgewöhnen muss. Die in der Wallet gespeicherten Nachweise können ohne den Umgang mit einer Smartcard und NFC-Schnittstelle genutzt werden, was in der Praxis der Nutzung des Personalausweises mit Online-Ausweisunktion derzeit zu bedeutenden Abbruchraten führt.

An dieser Stelle ist gleichfalls die Frage zu stellen, inwieweit die eID, welche beispielsweise über den Personalausweis eingesetzt werden kann, diese Funktionen nicht bereits erfüllt. Die Einbindung der eID in die hier diskutierten Anwendungen ist für viele Diensteanbieter aufgrund der hohen technischen Anforderungen und Kosten der eID-Nutzung derzeit nicht sinnvoll darstellbar. Insofern sind auch die Schwellen zum Einsatz bzw. zur Prozessintegration auf dieser Seite zu senken. Auch die weniger aufwendige Integration von Benutzerkonten (z. B. BundID) ist dennoch mit signifikanten Hürden verbunden. In diesem Fall wird dann auch wieder der Nutzer mit mindestens drei Technologien (Fachverfahren, Nutzerkonto und AusweisApp bzw. zukünftig vermutlich EUDI Wallet) und unterschiedlichen User Interfaces konfrontiert. Einfache, medienbruchfreie, schnelle und integrative Prozesse, insbesondere auch vor Ort, sind so nicht ohne weiteres umsetzbar. BundID und die (zwischenzeitlich eingestellte) SmarteID (welche die Nutzung der Online-Ausweisfunktion ohne das Halten des Personalausweises an das Smartphone für die Nutzung der NFC-Schnitt-

stelle ermöglichen sollte) sind nur für die Nutzung von Onlinediensten ausgelegt. Sie liefern auch kein verifiziertes Lichtbild des Bürgers mit sich, welches eine einfach Sichtprüfung ermöglicht. Auch wenn ein Bürger also meint, seine sichere digitale Identität auf dem Smartphone dabei zu haben, so kann er sie doch nicht für „vor Ort"-Anwendungen nutzen. Hierzu müsste er wieder auf den physischen Personalausweis zurückgreifen. Dies ist den Bürgern sicherlich kaum zu vermitteln. Bislang schwer absehbar ist, inwieweit die EUDI Wallet über den digitalen Führerschein (mDL – mobile Drivers' License) hinaus solche vor Ort Anwendungen unterstützen wird.

Weiter ist auch der Umfang der Attribute maßgebend dafür, welche kommunalen Anwendungen mit einer digitalen Identität unterstützt werden. Der Datensatz aus dem Melderegister kann umfangreicher sein als der eID-Datensatz. Er kann beispielsweise Informationen zum Zuzugsdatum oder zur Adresse des Nebenwohnsitzes aus einem kommunalen Melderegister enthalten, die für bestimmte kommunale Szenarien benötigt werden. Außerdem lässt sich eben ein verifiziertes Lichtbild aus dem Passregister mit ableiten. Den konkreten Attributumfang bestimmt schließlich die Kommune nach den Erfordernissen der in ihrem Hoheitsbereich zu unterstützenden Anwendungsprozesse. Eine Interoperabilität der kommunalen Datenkarte zwischen Kommunen erfordert aber sicherlich die Definition eines Sets an Basisattributen sowie eines standardisierten Regelwerks. Dies ist erst mittelfristig erreichbar – kurzfristig liegt der Fokus darum auf der lokalen Anwendung. Die konkrete Umsetzung sowie technische Basis der kommunalen Datenkarte wird im folgenden Abschnitt dargestellt.

2.2 Praktische Realisierung

Die technische Grundlage der kommunalen Datenkarte basiert auf der Self-Sovereign Identity (SSI)-Technologie. SSI repräsentiert ein Paradigma, das jedem Individuum ermöglicht, Besitz und Kontrolle über seine digitale Identität und die damit verbundenen Daten auszuüben, ohne auf Intermediäre oder zentrale Autoritäten angewiesen zu sein (Allen 2016). Diese Autonomie in der digitalen Identitätsverwaltung wurzelt in der Idee, dass ebenso wie in der realen Welt jedes Individuum selbstverantwortlich für seine Identitätsnachweise ist. Die konzeptionelle Herkunft der SSI kann auf die Fortschritte in verteilten Register-Technologien (DLT - Distributed Ledger Technology), insbesondere der Blockchain, zurückgeführt werden,

welche Mechanismen für dezentrales Vertrauen und Sicherheit ohne eine zentrale Überwachungsinstanz bietet.

Für SSI-Ansätze spielen Verifiable Credentials (VCs) eine entscheidende Rolle. VCs sind digitale Zertifikate, die von einer vertrauenswürdigen Entität ausgestellt werden und bestimmte Ansprüche über eine Person oder Entität bestätigen. Diese Zertifikate sind so gestaltet, dass sie von Dritten privatsphärenfreundlich verifiziert werden können, ohne dass die ursprünglich herausgebende Entität kontaktiert werden muss (W3C 2022). Grundsätzlich sind auch sogenannte Zero Knowledge Proofs realisierbar, welche beispielsweise einen Volljährigkeitsnachweis ohne Offenlegung des zugrunde liegenden Geburtsdatums ermöglichen. VCs beruhen also auf kryptographischen Methoden, die es ermöglichen, die Echtheit, Integrität und Nichtabstreitbarkeit der Credentials zu gewährleisten. Somit bilden sie die Grundlage für eine vertrauensvolle und gleichzeitig datenschutzfreundliche digitale Interaktion.

Die kommunale Datenkarte nutzt eine Identity Wallet Applikation, welche als eine sichere Speicher- und Präsentationsumgebung für VCs auf Smartphones mit gängigen Betriebssystemen wie Android und iOS dient. Es wird sichergestellt, dass Nutzende ohne die Notwendigkeit spezieller Hardware (wie high-end Smartphones mit zertifizierten Hardwaresicherheitselementen wie bei der Smart-eID) oder aufwendiger Prozesse, wie etwa dem fehleranfälligen Auslesen von NFC-Chips (wie bei der Online-Ausweisfunktion des Personalausweises), Zugang zu ihren digitalen Identitätsnachweisen erhalten.

Grundsätzlich ist auch eine Interoperabilität der SSI-basierten kommunalen Datenkarte mit europäischen Initiativen angestrebt. Die Vorgaben und Standards, die durch die eIDAS-Verordnung (eIDAS 2.0) und das Architecture Reference Framework (ARF) (eIDAS Expert Group 2024) für die EU Digital Identity Wallet (EUDI Wallet) definieren und derzeit in den EU Large Scale Pilot Projekten (LSP) (EU Commission 2024) erprobt werden, dienen als Leitlinien. Da die Arbeiten an der Architektur und der EUDI Wallet derzeit jedoch noch nicht abgeschlossen sind, muss sich zeigen, inwieweit eine Interoperabilität möglich ist oder die kommunale Datenkarte vielmehr eine Ergänzung oder Brückentechnologie bis zur Verfügbarkeit der EUDI Wallet darstellt.

Die kommunale Datenkarte dient somit als ein verifizierbarer digitaler Nachweis (Verifiable Credential), der durch die Nutzung von SSI-kompatiblen Systemen innerhalb der kommunalen IT-Infrastruktur (kommunalen IT-Fachverfahren) generiert und verwaltet werden kann. Der Ausstellungs-

prozess dieses Nachweises bedient sich vertrauenswürdiger Datenquellen der öffentlichen Verwaltung, wie beispielsweise Melderegister (Register auf Landes- oder kommunaler Ebene), um die Authentizität und Zuverlässigkeit der digitalen Identität des Bürgers zu gewährleisten. Vom Bürger wird er über die App und die Wallet auf handelsüblichen Smartphones verwaltet und mittels dieser für den Zugang zu Anwendungen online und vor Ort genutzt.

Personenbezogene Daten werden gemäß den rechtlichen Rahmenbedingungen durch kommunale Behörden im Zuge administrativer Verfahren erfasst – beispielsweise bei der An- und Ummeldung des Wohnsitzes oder der Beantragung von Ausweisdokumenten – und von den jeweiligen kommunalen Einrichtungen verwaltet sowie aktualisiert. So werden sie im Melderegister gespeichert und gepflegt.

Der Nutzer der App, in der Rolle der betroffenen Person, kann nach Art. 15 Abs. 1 S. 1 DSGVO gegenüber der registerführenden Behörde (Verantwortlicher) generell Auskunft darüber verlangen, ob personenbezogene Daten verarbeitet werden und – sofern eine solche Verarbeitung vorliegt – auch über diese Daten selbst Auskunft zu erhalten. Wird das Auskunftsersuchen elektronisch eingereicht, so ist der Verantwortliche nach Maßgabe des Art. 15 Abs. 3 S. 1 und 3 DSGVO und unter Berücksichtigung des § 10 BMG angehalten, eine Kopie der verarbeiteten personenbezogenen Daten im Sinne einer elektronischen Bereitstellung in gängigem Format zu übermitteln. Der Auskunftsanspruch kann praktisch vom Nutzer direkt aus der App elektronisch eingereicht, die Kopie der verarbeiteten personenbezogenen Daten in einem elektronischen Format empfangen werden.

Die Daten aus dieser Auskunftserteilung (z. B. XML, PDF) werden hieraufhin aus der Datei entnommen und als das Verifiable Credentials der kommunalen Datenkarte in die Wallet übertragen. Im Rahmen der Projekte ID-Ideal und ONCE wurde dies technisch bereits prototypisch realisiert. Hierzu kooperierten Anbieter kommunaler Fachverfahren, öffentliche IT-Dienstleister, Entwickler von SSI-Backend und Wallet-Lösungen und Kommunen für den Zugang zu den Registern und kommunale Angebote.

Für die kommunale Datenkarte ist ein Basisdatenset von Angaben wie Name, Geburtsdatum, Wohnadresse, Familienstatus sowie Daten bezüglich der Anmeldung oder des Zuzugs in die betreffende Kommune angedacht, das im Zuge der Pilotierung noch weiter zu spezifizieren ist. Die kommunale Verwaltung bestätigt durch ein qualifiziertes digitales Siegel ausschließlich, dass die Daten zum Zeitpunkt der Ausgabe im Melderegister so vorhanden waren. Die rechtliche Zulässigkeit einer Ergänzung um das

digitale Lichtbild aus dem Pass- oder Personalausweisregister ist derzeit Gegenstand juristischer Abklärungen. Dem Bürger ist es nun möglich, die erhaltenen Nachweise eigenständig zu verwalten und für die Nutzung kommunaler (oder darüber hinaus gehender) Angebote heranzuziehen. Die Annahme ist, dass die aus den kommunalen Registern bezogenen Daten von den Akzeptanzstellen, zu denen ja insbesondere Angebote der jeweiligen Kommune zählen, als vertrauenswürdig erachtet werden.

2.3 Pilotierung der kommunalen Datenkarte im Rahmen der Forschungsprojekte

Das Konzept der kommunalen Datenkarte wird im Rahmen der SDI-Schaufenster ONCE und ID-Ideal in mehrere Stufen praktisch getestet. Es wurden etwa User Interface Mockups sowie Test Credentials für die kommunale Datenkarte in der Wallet erstellt und die Usability mit Bürgern erprobt. Eine kommunale Pilotimplementierung erfolgt schließlich in Zusammenarbeit mit der Landeshauptstadt Dresden.

In einem ersten Schritt werden verifizierbare Daten zu einer Person aus dem kommunalen Melderegister in ein Basis-Credential überführt, welches in einer Wallet gespeichert werden kann. Es kann fortan als Nachweis im kommunalen Umfeld für die Inanspruchnahme ausgewählter kommunaler Dienstleistungen verwendet werden. Das Credential ermöglicht es prinzipiell, einzelne Attribute des Datensatzes zu einer Person aus der Wallet heraus automatisiert in ausgewählten Anwendungsszenarien für kommunale Dienstleistungen zu präsentieren, auszulesen oder in Formulare einzufügen.

In einem zweiten Schritt ist die Infrastruktur der Verwaltung anzupassen. Ziel ist es, die Fachabteilungen, welche Verifiable Credentials ausstellen, prüfen und akzeptieren müssen, mit Softwarekomponenten zur Realisierung der gesamten Prozesskette auszustatten.

Diese Aufgaben obliegen prinzipiell der Kommune, was zumindest dahingehend sinnvoll ist, dass sie bedarfsgerecht und entsprechend der jeweils vorhandenen kommunalen IT-Landschaft gelöst werden müssen. Idealerweise erfolgt die Bereitstellung der technischen Komponenten zukünftig auch in Form von Software Development Kits (SDK) zur Integration in kommunale Anwendungen und kommunale Hintergrundsysteme (ID-Ideal/ONCE 2023).

Für die Anwendung der kommunalen Datenkarte in kommunalen Test-Szenarien werden gegenwärtig zwei Ansätze verfolgt:

a) Beantragung eines kommunalen Berechtigungsnachweises – Dresden-Pass

Der Dresden-Pass berechtigt zum kostengünstigeren Besuch kultureller Einrichtungen der Landeshauptstadt Dresden und des Freistaates Sachsen in der Stadt Dresden, zur kostenlosen Mietrechtsberatung sowie zur Inanspruchnahme von Ermäßigungen bei der Dresdner Verkehrsbetriebe AG (DVB AG). Anspruch auf den Dresden Pass haben Einwohner mit Hauptwohnsitz in Dresden, die ausgewählte Sozialleistungen beziehen (Landeshauptstadt Dresden 2022). Ausstellende Behörde des Dresden Passes ist das Sozialamt der Landeshauptstadt.

Für die Beantragung verifiziert sich der Antragsteller mit seinem Basis-Credential aus seiner Wallet gegenüber der ausstellenden Behörde und erhält von dieser den Dresden Pass als Verifiable Credential (Dresden Pass Credential) in seine Wallet übertragen. Das Dresden Pass Credential ist ab diesem Zeitpunkt gültig bis zum Widerruf (in der Regel 1 Jahr, angelehnt an die Dauer des Bezugs der Sozialleistungen) und berechtigt den Inhaber dazu, Vergünstigungen in den zahlreichen Einrichtungen der Stadt zu beanspruchen.

Der Inhaber muss für die Ermäßigungen lediglich, vor Ort (z. B. via QR-Scan) oder online seine Wallet mit dem Serviceanbieter verbinden und das Dresden Pass Credential präsentieren.

b) Nachweis der Berechtigung zur Teilnahme an einem Bürgerbegehren

Ein Bürgerbegehren nach § 25 Abs. 1 SächsGemO eröffnet Bürgern in Sachsen die Möglichkeit zur politischen Mitbestimmung. Das Bürgerbegehren ist als ein Antrag der Bürger einer Gemeinde auf einen Bürgerentscheid zu verstehen, bei dem die Bürgerschaft (anstelle des Stadtrates) direkt über Angelegenheiten der Gemeinde entscheiden kann. Die Themen und Inhalte für einen Bürgerentscheid sind kommunalpolitische Sachfragen, für die der Stadtrat zuständig ist (Stadt Leipzig 2024).

Antragsberechtigter Bürger ist nach § 15 Abs. 1 i. V. m. § 16 Abs. 1 S. 2 SächsGemO, wer am Tag der Unterzeichnung des Bürgerbegehrens Deutscher im Sinne von Artikel 116 Abs. 1 GG ist oder die Staatsangehörigkeit eines Mitgliedstaates der Europäischen Union besitzt, das 18. Lebensjahr vollendet hat und seit mindestens drei Monaten in der Gemeinde wohnt.

Die Besonderheit dieses Szenarios liegt darin, dass die Berechtigung zur Teilnahme davon abhängt, wie lange die Person bereits in der Gemeinde wohnt. Dieser Nachweis kann nicht anhand eines Passes oder Personalausweises geführt werden, da diese Information nicht aus dem Dokument bzw. dem zugehörigen Datensatz aus der eID ersichtlich sind. Für die Nachweisführung sind vielmehr Informationen aus dem kommunalen Melderegister (Einwohnermeldeamt) erforderlich.

Mit der kommunalen Datenkarte wäre der Nachweis generell möglich. Jedoch kommt im Fall des Bürgerbegehrens noch eine weitere Besonderheit hinzu. Die Beantragung hat nach § 25 Abs. 1 S. 1 SächsGemO schriftlich zu erfolgen, die elektronische Form ist explizit ausgeschlossen.

Der Ausschluss der elektronischen Form führt dazu, dass Mitarbeiter der Stadt Dresden die Gültigkeit der Unterschriften zum Bürgerbegehren, immerhin mind. 5 % der Wahlberechtigten Dresdener[7], händisch prüfen müssen, was in der jüngeren Vergangenheit personelle Aufwendungen von bis zu 6 Vollzeitäquivalenten über mehrere Wochen hinweg verursacht hat. Für die Testung des Szenarios wird deshalb eine Ausnahmeregelung im Rahmen einer Experimentierklausel nach § 20 Sächsisches E-Government-Gesetz für eine Reallabor sondiert, um die Auswirkungen und Potentiale der elektronischen Form in diesem Szenario zu untersuchen.

3. Zwischenfazit aus der Entwicklung und Pilotierung

Die Realisierung des SSI-Ansatzes erfordert eine gewisse Transformation herkömmlicher Prozessabläufe und Strukturen. In technischer Hinsicht müssen Prozesse re-moduliert, Systeme angepasst oder neu errichtet werden. Das Personal muss entsprechend qualifiziert und es müssen notwenige Kompetenzen aufgebaut werden, um die Serviceangebote zu bewirtschaften und auch dem Nutzer die Anwendung zu erklären und bei Bedarf zu unterstützen.

In organisatorischer Hinsicht sind auf kommunaler Ebene die notwenigen Strukturen und Verantwortlichkeiten (Governancestrukturen) zu schaffen. Konkret ist hierfür ein gültiger Rechtsrahmen zu schaffen, federführende und beteiligte Stellen zu legitimieren und entsprechende personelle und finanzielle Mittel bereitzustellen.

7 Ab ca. 20.000 Unterschriften.

3.1 Rechtlich-organisatorische Einordnung der Akteure, Rollen und Prozessabläufe

Für den Einsatz der kommunalen Datenkarte in der Praxis, sind die rechtlichen Voraussetzungen zu schaffen. Die rechtlich zuständige Stelle, die als Kontrollorgan (und juristische Person) die hierfür geltenden Regeln formuliert, für verbindlich erklärt und auch ihre Einhaltung überwacht, muss nach den geltenden deutschen Staatsstrukturprinzipien nach Art. 20 Abs. 1 GG als ein rechtssetzendes staatliches Organ demokratisch legitimiert sein. Auf kommunaler Ebene ist die Gemeinde, bzw. der Stadt- oder Gemeinderat als Hauptorgan der Gemeinde, ermächtigt, für ihren Wirkungsbereich Rechtsvorschriften zu schaffen. Sachliche und räumliche Grenzen sind hierbei zu beachten, ein hinreichender Bezug zum eigenen Gebiet, entweder weil ein Vorgang dort stattfindet oder eine Leistung dort angeboten und erbracht wird oder weil die zugehörigen Einwohner allein oder hauptsächlich dort betroffen oder begünstigt sind. Eine Begünstigung und Erstreckung der Nutzungsbedingungen im Hinblick auf öffentliche Einrichtungen der Gemeinde (§ 10 Abs. 2, 5 SächsGemO) kommt generell auch im Hinblick auf Gäste oder Nicht-Gemeindeansässige in Betracht. Dies gilt gleichfalls für rechtlich selbstständige Anstalten wie Verbände und privatrechtsförmige kommunale Unternehmen, die auch gebietsfremden Kunden frei zugängliche Leistungen anbieten und die die Reichweite Ihrer Tätigkeiten nicht auf das Gebiet der Kern-Gemeinde begrenzen (z. B. Personenbeförderung, Sparkassen, etc.). Die Gemeinde (Stadt- oder Gemeinderat sowie bei entsprechender Zuständigkeit Bürgermeister und Oberbürgermeister) ist damit befugt, Regeln in rechtsverbindlicher Form als Satzung oder innerhalb der Gemeindeverwaltung (z. B. Sozialamt) durch „Richtlinien" aufzustellen und zu ändern. Die konkret zuständige Stelle ergibt sich aus dem Organisationsplan beziehungsweise aus der erlassenen Hauptsatzung der Gemeinde (§ 4 Abs. 2 SächsGemO), im Hinblick auf den Einsatz von finanziellen und personellen Ressourcen arbeiteten eine federführende Stelle und andere Stellen zusammen.

Der Herausgeber (herausgebende Stelle) der kommunalen Datenkarte wird diesen Bestimmungen unterstellt. Er verantwortet die Prozessschritte zur Integration der Daten in das Basis-Credential und dessen Ablage in der Wallet, und damit sowohl den Vorgang der Übernahme der Daten aus der elektronisch bereitgestellten Auskunft (z. B. PDF) in die Wallet, der Übermittlung oder zur Verfügung Stellung von Daten innerhalb des kommunale Datenkarte-Ökosystems als auch die maßgebliche Steuerung und Kontrolle

der vorausliegenden Vorgänge. Hier ist auch an die Schaffung und/oder Bereitstellung der Wallet oder deren Vergabe an Dritte und dabei auch die Weitergabe der erforderlichen Informationen an die für den Herausgeber tätig werdenden (juristischen) Personen (Dritte) zu denken. Die herausgebende Stelle ist dann, neben der erstmaligen Ausgabe der kommunalen Datenkarte auch für das Überwachen der Regeln des Umlaufs, auch für das Aus-dem-Verkehr-ziehen bei Wegfall der Gültigkeit zuständig.

Inhaber kann allgemein jede zu identifizierende Person sein, die im Fall der kommunalen Datenkarte zu einer für bestimmte Funktionen oder Maßnahmen berechtigten Personengruppe (hier natürliche Personen) gehört (z. B. Berechtigte für Sozialleistungen). Abhängig vom Berechtigungszweck kann dabei z. B. das Alter ein wesentliches Differenzierungsmerkmal sein (generell Geschäftsfähigkeit nach § 104 BGB, Vergünstigungen für Minderjährige oder Senioren). Im Fall der Nationalität als Differenzierungsmerkmal ist der allgemeine Gleichheitssatz (Art. 3 Abs. 1 GG) zu beachten. Sofern der Inhaber den Nachweis aufgrund der Zugehörigkeit zu einer Organisation (juristischen Person) erhält, ist die Organisationszugehörigkeit die differenzierende Eigenschaft (z. B. Mitgliedsausweis).

Die Rolle als Inhaber setzt voraus, dass die jeweilige Person unmittelbarer Besitzer (i.S.v. § 854 BGB) der einzusetzenden Hardware (als Speicher der elektronischen Informationen) für die kommunale Datenkarte ist. Bei Software oder elektronischen Informationen für Nachweise, ist ein „Besitz" nur an dem physischen Trägermedium möglich, da Software insoweit keine Sach-Qualität zukommt. Entsprechend ergeben sich statt Besitz- oder Eigentumsrechten vielmehr Verfügungsrechte aus den Vorschriften des Immaterialgüterrechtes.

Die kommunale Datenkarte wird zum Nachweis der Identität und/oder einer Berechtigung gegenüber Akzeptanzstellen (Verifier) eingesetzt. Je nach rechtlichem Rahmen erfolgt hier neben der Identifizierung des Inhabers auch eine Verifizierung der Akzeptanzstelle als des „richtigen" Vertragspartners. Nur dann, wenn die betreffende Stelle im Rahmen der gesetzlich oder vertraglich gestalteten Kommunikation auch berechtigt ist, die Echtheit und Richtigkeit der Daten des Inhabers zu prüfen, handelt diese Stelle als Verifier. Soweit der Verifier eine andere öffentliche Stelle des herausgebenden Trägers ist, aber auch bei („eigenen") öffentlichen Unternehmen, kann sich die Pflicht zur Anerkennung der mit der kommunalen Datenkarte nachgewiesenen Eigenschaften direkt auf verbindliche Regelungen der Gemeinde stützen. Im Fall von privaten Unternehmen

als Akzeptanzstelle muss eine Anerkennungspflicht vertraglich begründet werden. Im Hinblick auf den Inhaber liegt hier ein Vertrag zugunsten Dritter vor. Bei der Ausgestaltung und beim Abschluss dieser vertraglichen Vereinbarungen ist die kommunale Seite an die haushaltsrechtlichen und kommunalwirtschaftlichen Grundsätze gebunden.[8]

Im Sinne der verfassungsrechtlich garantierten kommunalen Selbstverwaltung obliegt es hier dem Aufgabenbereich der Gemeinde, den Service für die kommunale Datenkarte zu errichten und zu betreiben. Hierfür kann sie sich eigener hinreichend kontrollierter öffentlicher Unternehmen in öffentlicher oder privater Rechtsform bedienen. Da Gemeinden generell kostendeckend arbeiten müssen, können kommunale Dienstleistungen (bei entsprechender Satzung) auch gegen Entgelt (Gebühr oder privatrechtlicher Preis) angeboten werden.

Im Rahmen der Servicebereitstellung sind natürlich die technischen, organisatorischen und tatsächlichen Anforderungen an Hard- und Software sowie Schnittstellen zu beachten, welche gesetzlich reguliert sind. So ist an eine entsprechende Offline-Nutzbarkeit und Barrierefreiheit zu denken, sowie gleichermaßen auch an (technische) Anforderungen (Smartphone) an den Nutzer und dessen Fähigkeiten. Die Verantwortlichkeit des Herausgebers bzw. Betreibers unterschiedet sich im Hinblick auf Datenschutz, Datensicherheit und Datensicherung nicht grundsätzlich von herkömmlichen Anforderungen an Betreiber „herkömmlicher" Identifizierungs- und Authentifizierungsbetreiber (physische Karten). Die Akzeptanz der Nachweise in dem kommunalen Datenkarten-Ökosystem sollte von der Gemeinde in ein Regelwerk überführt werden.

3.2 (Europa-) rechtliche Entwicklungen

Mit der Verordnung 910/2014 der EU über Electronic Identification, Authentication and Trust Services (eIDAS 2014) wurde 2014 ein Rahmen geschaffen, um die gegenseitige Anerkennung der verwendeten Identifizierungsmittel und Vertrauensdienste sowie deren Interoperabilität zu fördern. Die Verordnung dient der Stärkung des Vertrauens in elektronische Transaktionen im Binnenmarkt, indem eine gemeinsame Grundlage für eine sichere elektronische Interaktion zwischen Bürgern, Unternehmen und

8 Dies geht aus einer für das Projekt ID-Ideal erstellten Stellungnahme aus 2024 hervor.

öffentlichen Verwaltungen geschaffen wird, wodurch die Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels in der Union erhöht wird.[9]

Mit der der Novellierung vom 11. April 2024 (EU Parliament 2024) werden mit Artikel 6a digitale Brieftaschen/Wallets als zentrales Element und weitgehend einheitliches Mittel zur Identifizierung in der EU eingeführt. Jeder Mitgliedstaat ist nach Artikel 6a Abs. 2 verpflichtet, eine notifizierte European Digital Identity Wallet (EUDI Wallet) herauszugeben. Jede natürliche und juristische Person muss einen nahtlosen Zugang bekommen (Artikel 6a Abs. 1). Die EUDI Wallet muss sowohl gesetzliche Daten zur Identifizierung einer Person enthalten und auch elektronische Attribute online und offline managen können (Artikel 6a Abs. 3 lit. a). Sie muss Schnittstellen für Vertrauensdiensteanbieter bieten, welche Attributsbescheinigungen herausgeben können. Vorgesehen ist, dass die EUDI Wallet neben (direkten) hoheitlichen Attributen (High Level of Assurance, Type 1, communication protocol: OpenID4VC (OpenID for verifiable credentials)) wie solche aus dem Personalausweis auch solche Nachweise unterstützen soll, die nicht dem High Level of Assurance und/oder dem OpenID4VC Protokoll entsprechen (Type 2). Mit der vorgesehenen Konfiguration wird das Imitieren und Verwalten von Diensten wie der kommunalen Datenkarte über die EUDI Wallet generell möglich.

4. Potenziale und Herausforderungen der kommunalen Datenkarte für selbstbestimmtes Datenteilen

Die Erfahrungen aus der Pilotierung der kommunalen Datenkarte sowie die Betrachtung der Entwicklungen im Umfeld der Schaufensterprojekte ermöglicht die Formulierung einer Reihe von Thesen, die im Folgenden erläutert werden. Sie leiten die weiteren Forschungs- und Entwicklungsarbeiten rund um das Konzept und werden hiermit zur breiteren Diskussion gestellt.

Die Implementierung der kommunalen Datenkarte, die auf der Technologie der Self-Sovereign Identity (SSI) fußt, bietet neue Perspektiven im Umgang mit personenbezogenen Daten und weist das Potenzial auf, die Datenhoheit der Bürger signifikant zu stärken. SSI ermöglicht es Nutzern, ihre Identitätsdaten eigenständig zu verwalten und zu kontrollieren,

9 Erwägungsgrund 2 der eIDAS-VO.

was eine wesentliche Abkehr von zentralisierten Identitätsmanagementsystemen darstellt. Dies trägt zu einem verbesserten Datenschutz bei, da die Datenverarbeitung und -speicherung dezentralisiert wird und Bürger genau bestimmen können, welche Daten sie für welche Zwecke freigeben. Indem die kommunale Datenkarte verifizierbare digitale Nachweise, die aus zuverlässigen Quellen wie dem Melderegister der öffentlichen Verwaltung stammen, in einer mobilen Wallet zugänglich macht, werden nicht nur Verwaltungsprozesse effizienter gestaltet, sondern es wird auch die Selbstbestimmung des Einzelnen über seine persönlichen Daten gefördert. Faktisch werden zahlreiche digitale Verwaltungsprozesse so erst möglich.

Die Verfügbarkeit von Werkzeugen, wie der kommunalen Datenkarte, die selektive Datenbereitstellung ermöglichen, könnte das Verhalten der Bürger im Umgang mit ihren personenbezogenen Daten entscheidend verändern. Die Hypothese, dass Bürger solche Spielräume aktiv nutzen werden, fußt auf dem zunehmenden Bewusstsein für Datenschutz und dem Wunsch nach mehr Kontrolle über die eigenen Daten. Mit einer SSI-basierten Lösung haben sie die bedienungsfreundliche Möglichkeit, selbst zu entscheiden, welche Informationen sie für welche Dienste freigeben, und können diese Datenfreigabe jederzeit widerrufen. Dies stärkt nicht nur das Vertrauen in digitale Dienstleistungen, sondern erhöht auch die Bereitschaft, digitale Verwaltungsdienste in Anspruch zu nehmen. Voraussetzung hierfür ist jedoch, dass die Bürger sowohl über das nötige Wissen verfügen, um die Technologien adäquat zu nutzen, als auch dass die Dienste selbst benutzerfreundlich und leicht zugänglich gestaltet sind. Damit diese Potenziale voll ausgeschöpft werden können, müssen die öffentlichen Verwaltungen und Dienstleister sicherstellen, dass die Schnittstellen und Prozesse für die Datenbereitstellung an die Bedürfnisse der Bürger angepasst sind und eine ausreichende Aufklärung über die Funktionsweise und Vorteile der selektiven Datenbereitstellung erfolgt.

Die Annahme, dass sowohl private als auch öffentliche Anbieter digitaler Dienstleistungen Konzepte zur Datenminimierung und zur Datensparsamkeit aufgreifen, solange dies ihre Wertschöpfung und Kostenstruktur unberührt lässt, spiegelt eine pragmatische Herangehensweise an das Datenschutzprinzip der Datenminimierung wider. Unter der Voraussetzung, dass durch die Beschränkung auf das Notwendigste keine finanziellen Einbußen oder Einbußen in der Servicequalität entstehen, könnten Anbieter geneigt sein, weniger Daten zu sammeln und zu verarbeiten. Dieses Vorgehen wäre nicht nur konform mit datenschutzrechtlichen Anforderungen, wie sie etwa die DSGVO vorschreibt, sondern könnte auch das Vertrauen

der Nutzer stärken und somit langfristig zur Kundenbindung beitragen. Darüber hinaus senkt es das Risiko aus potenziellen Datenabflüssen. Um dieses Potenzial zu realisieren, ist es jedoch erforderlich, dass die Anbieter den Mehrwert der Datenminimierung erkennen und ihnen der Umstieg auf diese so leicht wie möglich gemacht wird.

Es wurden jedoch auch noch einige Herausforderungen deutlich. Mit der kommunalen Datenkarte, wie generell mit SSI Credentials, erhalten Bürger die Möglichkeit, signierte Nachweise aus vertrauenswürdigen Quellen einfach weiterzugeben. Diese Nachweise könnten auch für potenzielle Angreifer äußerst wertvoll sein und es sind Situationen denkbar, in denen von einem selbstbestimmten Datenteilen nicht mehr die Rede sein kann. Illustriert werden kann dies mit dem Bild des 800-Pfund Gorillas: *„"What do you give an 800-pound gorilla?", answer: "Anything that it asks for". Examples of such 800-pound gorillas are some big-tech websites, immigration offices and uniformed individuals alleging to represent law-enforcement. Also, the typical client-server nature of web transactions reinforces this power imbalance, where the human party behind its client agent feels coerced into surrendering personal data as otherwise they are denied access to a product, service or location.*" (van Deventer 2020). Die Daten der kommunale Datenkarte müssen entsprechend gegen solche 800-Pfund Gorillas abgesichert werden. Hierzu können etwa Maßnahmen getroffen werden, die lediglich zertifizierten Stellen erlauben, auf diese Daten zuzugreifen – wie es im Falle des Berechtigungszertifikates des Personalausweises bereits praktiziert wird und wofür bereits verschiedene technische Ansätze für Wallets existieren. Diese zusätzliche Governance-Anforderung ist jedoch nicht ohne wesentliche Nachteile, erschwert sie doch wiederum die Adoption der Technologie durch Serviceanbieter.

Die fortlaufende Dynamik regulatorischer Entwicklungen sowie der technologischen Basis stellt darüber hinaus eine wesentliche Herausforderung für Projekte wie die Implementierung der kommunalen Datenkarte dar. Sowohl auf deutscher (Onlinezugangsgesetz, gestoppte Einführung der Smart-eID, etc.) wie auf europäischer Ebene mit eIDAS 2.0 und der EUDI Wallet ist der Wandel die einzige Konstante. Dies führt jedoch dazu, dass es aus Sicht vieler Beteiligter noch keinen Sinn ergibt, sich bereits jetzt auf eine bestimmte Lösung festzulegen. Beispielsweise wird dann argumentiert, dass die europäische Lösung in mehr oder weniger naher Zukunft ohnehin bald alle anderen Lösungen ersetzen wird. Entsprechend mache die Integration einer Lösung derzeit wenig Sinn. Gleichzeitig entwickeln sich auch Standards und Protokolle der SSI-Technologie kontinuierlich

weiter, Inkompatibilitäten bestehen und teilweise ist der technologische Reifegrad noch nicht begrenzt. Auch dies verstärkt die nachvollziehbare Tendenz zahlreicher Entscheider, erst einmal abzuwarten, bis sich eine stabile technische Basis herausgebildet hat. Schließlich will man nicht aufs falsche Pferd setzen und in einer technologischen Sackgasse enden. Das Resultat dieser Entscheidungen ist dann jedoch ein faktischer Stillstand.

5. Fazit

Self-Sovereign Identity und Wallets sind Werkzeuge, um digitale Identität von Personen und Organisationen zu verwalten, Identitäts- und Berechtigungsnachweise zu erbringen und zu kontrollieren, aber auch um Daten auszutauschen und die Verarbeitung zu legitimieren. Für die Nutzer dieser Werkzeuge bieten sie neue Möglichkeiten im Hinblick auf Selbstbestimmtheit und Transparenz. Im Hinblick auf die Digitalisierungsbestrebungen eröffnen sich neue Gestaltungsräume, um die Aufwände für die Datenhaltung zu minimieren, die Qualität von Daten zu verbessern und Daten interessengerechter verarbeiten zu können. Es 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 Akzeptanz sind neben den technischen Weiterentwicklungen, der Schlüssel zu diesen Verbesserungen. Diese Potentiale zu heben, ist deshalb Gegenstand weiterer interdisziplinärer Forschung.

Literatur

Allen, Christopher (2016): The Path to Self-Sovereign Identity. GitHub. URL: https://github.com/ChristopherA/self-sovereign-identity (besucht am 5.2.2024).

Bundesministerium für Wirtschaft und Klimaschutz (2024): Schaufenster Sichere Digitale Identitäten. URL: https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/sichere_digitale_ident.html (besucht am 8.2.2024).

D21 und TU München (2023): eGovernment MONITOR 2023. URL: https://initiatived21.de/uploads/03_Studien-Publikationen/eGovernment-MONITOR/2023/egovernment_monitor_23.pdf (besucht am: 6.2.2024).

van Deventer, Oskar (2020): Verify the verifier: anti-coercion by design | TNO. tno.nl/en. URL: https://www.tno.nl/en/newsroom/insights/2020/10/verify-verifier-anti-coercion-design/ (besucht am: 25.3.2024).

DGA (2022): Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868&from=EN (besucht am: 25.3.2024).

DMA (2022): Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). URL: https://eur-lex.europa.eu/eli/reg/2022/1925/oj (besucht am: 25.3.2024).

eIDAS (2014): Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32014R0910 (besucht am: 25.3.2024).

eIDAS 2.0 (2024): Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1183&qid=1716387048511 (besucht am 20.5.2024)).

eIDAS Expert Group (2024): EUDI Wallet - Architecture and Reference Framework 1.3.0. URL: https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.3.0/ (besucht am: 25.3.2024).

EU Commission (2024): What are the Large Scale Pilot Projects - EU Digital Identity Wallet. URL: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/What+are+the+Large+Scale+Pilot+Projects (besucht am: 25.3.2024).

European Commission (2024): EU Digital Identity Wallet Home - EU Digital Identity Wallet. URL: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/ (besucht am: 25.3.2024).

ID-Ideal und ONCE (2023): Anforderungen aus Sicht der SDI-Schaufenster ONCE und ID-Ideal an die Entwicklung der EUDI Wallet. URL: https://id-ideal.de/wp-content/uploads/2024/01/Anforderungen-an-EUDIW-aus-Sicht-von-ONCE-ID-Ideal.pdf (besucht am: 25.3.2024).

Krempl, Stefan (2023): Smart-eID: Online-Ausweisen mit dem Handy soll von Ende 2023 an machbar sein. heise online. URL: https://www.heise.de/news/Smart-eID-Online-Ausweisen-mit-dem-Handy-soll-von-Ende-2023-an-machbar-sein-9304284.html (besucht am: 25.3.2024).

Landeshauptstadt Dresden (2022): Faltblatt Dresden Pass. URL: https://www.dresden.de/media/pdf/infoblaetter/faltblatt-dresden-pass.pdf (besucht am: 25.3.2024).

Röhl, Klaus-Heiner (2023): Verwaltungsdigitalisierung in Deutschland: Der Stand zum Zielzeitpunkt des Onlinezugangsgesetzes Anfang 2023. IW-Report 20/23.

Stadt Leipzig (2024): Bürgerbegehren und Bürgerentscheid - Stadt Leipzig. URL: https://www.leipzig.de/buergerservice-und-verwaltung/buergerbeteiligung-und-einflussnahme/buergerbegehren-und-buergerentscheid (besucht am: 25.3.2024).

Steiner, Falk (2023): *Smarte eID: Online-Ausweis wegen Haushaltslage vorerst gestoppt*. heise online. URL: https://www.heise.de/news/Smarte-eID-Online-Ausweis-wegen-Haushaltslage-vorerst-gestoppt-9576180.html (besucht am: 25.3.2024).

W3C (2022): Verifiable Credentials Data Model v1.1. W3C Recommendation. URL: https://www.w3.org/TR/vc-data-model/ (besucht am: 16.3.2022).

Die neue Ära des Datenhandels: Daten als Währung und Gegenleistung

Dagmar Gesmann-Nuissl und Stefanie Meyer

Zusammenfassung

Mit der Umsetzung der Digitale Inhalte-Richtlinie und der Warenkaufrichtlinie in das deutsche BGB (§§ 327 ff. BGB) ist eine bereits seit längerem ausgeübte Praxis gesetzlich präzisiert worden: Das Bezahlen mit Daten. Das neu geschaffene Datenschuldrecht bewegt sich auf der Schnittstelle zwischen Vertragsrecht und Datenschutzrecht. Dabei entsteht ein Spannungsverhältnis zwischen der Etablierung einer erfolgreichen Datenwirtschaft auf Basis privatautonomer vertragsrechtlicher Beziehungen einerseits und der Sicherstellung der digitalen Datensouveränität der Verbraucher andererseits. Bezogen auf Verträge über digitale Produkte stellen sich vor allem vertragsrechtliche Fragen, etwa zum Zustandekommen und der Ausgestaltung der Vertragsverhältnisse. Dem gegenüber stehen datenschutzrechtliche Fragestellungen, die von den schuldrechtlichen Voraussetzungen unberührt bleiben (§ 327q BGB). Dort stehen die Informiertheit und die Freiwilligkeit der Einwilligung in die Datenverarbeitung sowie die Wahrung datenschutzrechtlicher Grundsätze, wie das Kopplungsverbot, im Vordergrund (Art. 7 DSGVO). Eine erfolgreiche Datenökonomie muss dieses Spannungsverhältnis auflösen, wobei die subjektive (souveräne) Willensbildung der Verbraucher, die sowohl im Rechtsbindungswillen als auch in der wirksamen datenschutzrechtlichen Einwilligung zum Ausdruck kommt, oberste Priorität genießt. Um beides gleichermaßen zu sichern, wird ein übersichtliches und leicht zugängliches Portal zum Schutz der Datensouveränität in der Datenwirtschaft vorgeschlagen. Es zeigt dem Verbraucher auf einen Blick den Wert seiner Daten in Bezahlvorgängen, was seine Willensbildung unterstützt sowie seiner Entscheidungsfreiheit dient und zugleich seine Datensouveränität wahrt. Dieser Beitrag befasst sich mit den rechtlichen Grundlagen, die bei der Entwicklung eines solchen Portals zu berücksichtigen sind.

„Not everything that can be counted counts and not everything that counts can be counted."[1]

1. Einleitung

Im Jahre 2011 wurde ein bemerkenswerter Eintrag in das Guinness-Buch der Rekorde vorgenommen: Das US-amerikanische Unternehmen *See Virtual Worlds* hat den virtuellen Planeten „Calypso" für einen Preis von 6 Millionen US-Dollar gekauft.[2] Aber auch spezifische Items in ausgewählten Computerspielen erzielen – gemessen an der Virtualität der Produkte – hohe Preise: Zuletzt wurde z. B. das Schwert „Schallende Wut" innerhalb des Computerspieles *Diablo 3* für 40 Milliarden „Gold" verkauft, was einem Wert von 14.000 US-Dollar entspricht.[3]

Rechtsgeschäfte mit virtuellen Gegenständen sind nicht neu. Wurden sie bislang dem Rechtskauf (§ 453 BGB) oder atypischen Verträgen (§§ 311, 241 ff. BGB) zugeordnet, sind durch die Digitale Inhalte-Richtlinie (DIRL – Richtlinie (EU) 2019/770), die Warenkaufrichtlinie (WKRL – Richtlinie (EU) 2019/771) und deren Umsetzung in das nationale Recht in den §§ 327 ff. BGB spezielle Regelungen hinzugetreten, die bestimmte Aspekte zu digitalen Produkten verbraucherschützend „vor die Klammer ziehen". Bezogen auf sog. digitale Inhalte bestimmt der Wortlaut des § 327 Abs. 1, Abs. 3 BGB nun ausdrücklich, dass solche virtuellen Gegenstände wahlweise gegen Entgelt, gegen Bezahlung von Wertedarstellungen (wie das „Gold" in *Diablo 3*) oder aber gegen das Bereitstellen von Daten erworben werden können. Letzteres wirft Fragen auf, namentlich, wie genau aufkommende Konflikte zwischen dem Privat- und Datenschutzrecht behandelt werden müssen, damit schuld- und datenschutzrechtliche Rechte und Pflichten in gleichem Maße beachtet und in Einklang gebracht werden können.

Der folgende Beitrag nimmt sich dieser Problematik an. Dabei werden zunächst die rechtlichen Grundlagen betrachtet, die bei der Entwicklung

1 *Cameron*, Informal Sociology, a Casual Introduction to Sociological Thinking, 1963: Random House; zuweilen wird dieses Zitat aber auch Albert Einstein (1955), Hilliard Jason, Stephen Ross, Lord Platt oder George Pickering zugerechnet.

2 https://www.guinnessworldrecords.com/world-records/92207-most-valuable-virtual-object (abgerufen am 18.04.2024), wobei in der dortigen Beschreibung als Käufer das Tochterunternehmen von *See Virtual Worlds* (*See Digital Studios*) genannt wird; der Rekord als solches wird dem Mutterkonzern zugschrieben.

3 https://www.esports.com/de/items-waffen-und-skins-5-spiele-mit-extrem-teuren-inhalten-215415 (abgerufen am 30.01.2024).

eines nutzerorientierten Werkzeugs berücksichtigt werden müssen, das der informierten ökonomischen Nutzung personenbezogener Daten bei der Bereitstellung digitaler Produkte dient. Ferner wird eine erste, initiale Idee zur praktischen Lösung vorgestellt.

2. Ökonomische Relevanz von Daten und deren rechtliche Grundlagen

Das wohl renommierteste Beispiel der Ökonomisierung von personenbezogenen Daten ist das Setzen sog. Cookie-Banner. Durch den Einsatz von Cookies auf Webseiten und der damit einhergehenden Verarbeitung personenbezogener Daten wird es dem Anbieter möglich, das Nutzerverhalten zu ermitteln und Werbung sowie zukünftige Angebote gezielter zu platzieren. Mit anderen Worten wird mit Cookies Geld verdient, da sich so die gewonnenen Nutzerdaten monetarisieren lassen. Letzteres geht allerdings nicht grenzenlos, sondern erfordert (sofern die Cookies nicht zwingend erforderlich sind, vgl. § 25 Abs. 2 Nr. 2 TTDSG) zumindest eine wirksame und informierte Einwilligung in die Datenverarbeitung seitens des Nutzers bzw. ein berechtigtes Interesse an der Weiterverarbeitung, die über ein voreingestelltes Ankreuzkästchen auf der Webseite des Anbieters hinausreichen muss.[4]

Personenbezogene Daten können allerdings noch in anderer Hinsicht Bestandteil von Leistungen oder Leistungsversprechen sein. Gerade im Umfeld digitaler Angebote werden viele Inhalte als „kostenlos" beworben, was aber lediglich bedeutet, dass für die Inhalte kein Entgelt zu entrichten ist, aber dennoch personenbezogene Daten – etwa in einem Registrierungsprozess oder während des sich daran anschließenden Nutzerverhaltens (z. B. Häufigkeit von Einkäufen, Art und Weise derselben) – erhoben werden.[5]

Die Wertschöpfung auf der Basis der erlangten Daten ist demnach vielfältig. Sie reicht von der Wertschöpfung durch das Kalibrieren bestimmter Vorhersagemodelle, über die Wertschöpfung durch Vorhersagen selbst, bis hin zu datenfinanzierten Geschäftsmodellen bzw. monetären Grundmodellen, die um eine Datenflusskomponente ergänzt werden.[6] Dabei sind

4 EuGH, Urt. v. 01.10.2019, Az. C-673/17, NJW 2019, 3433; vgl. Besprechung u.a. von *Gesmann-Nuissl*, InTeR 2019, 190 (190 ff.).
5 *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (84).
6 *Hacker*, ZfPW 2019, 148 (153-157).

die Verwertungsmethoden recht unterschiedlich. Zum Teil werden die erhobenen Daten weiterverkauft. Zunehmend interessanter gestaltet sich für die Verwerter allerdings die gezielte Ansprache von Nutzern in der personalisierten Werbung oder das Generieren eines Nutzerprofils.[7] Selbst eine Datenerhebung zu Marktforschungszwecken kann einen geldwerten Vorteil bringen, da sich selbst aus einem depersonalisierten Datensatz noch Gewinne erzielen lassen.[8]

In der Vergangenheit zeigte sich, dass trotz der bekannten Monetarisierungsmöglichkeit von Daten viele Nutzer dann doch recht freizügig bei der Herausgabe ihrer personenbezogenen Daten sind und damit prinzipiell eine „kostenfreie Leistung" erbringen. Gleichzeitig steigt ihr Wunsch nach dem umfassenden Schutz ihrer Persönlichkeitsrechte. Dieser Widerspruch zwischen der Freigiebigkeit des Einzelnen in Bezug auf seine personenbezogene Daten und dem Bedürfnis nach hinreichendem Grundrechtsschutz wird als *Privacy Paradox* bezeichnet.[9]

Der Schutzbedürftigkeit der Verbraucher nimmt sich nun die EU an, welche die DIRL und die WKRL mit dem Ziel in Kraft setzte, das Vertrauen der Verbraucher in Bezug auf den Erwerb digitaler Produkte und Waren mit digitalen Elementen von europäischen Unternehmen zu stärken und einen digitalen europäischen Binnenmarkt zu fördern.[10] Der Unionsgesetzgeber strebt gem. Art. 4 DIRL und Art. 4 WKRL eine Vollharmonisierung in allen Mitgliedstaaten an, sodass die Mitgliedstaaten entsprechende Vorschriften einführen und dabei die in den Richtlinien festgelegten Mindest- und Maximalstandards beachten müssen. Der nationale Gesetzgeber hat in Umsetzung der Richtlinien mit den §§ 327 ff. BGB spezielle Regelungen für Verbraucherverträge geschaffen, wobei die Grundsätze zum Schutze der Verbraucher gem. § 312 Abs. 1a BGB nach § 327 Abs. 3 BGB anzuwenden sind, wenn Verbraucher einem Unternehmer personenbezogene Daten bereitstellen oder sich hierzu verpflichten. Zu einer solchen Transaktion bedarf es einer informierten selbstbestimmten Entscheidung – sowohl bezogen auf den privatautonomen Vertragsschluss, als auch hinsichtlich der datenschutzrechtlich relevanten Herausgabe von Daten. Der Brücken-

7 *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (219); vgl. dazu auch *Gesmann-Nuissl/Meyer*, in: International Conference on Human-Agent Interaction (HAI '23), 2023.
8 *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (88).
9 *Norberg u.a.,* JCA 2007, 100 (100 ff.).
10 *Blassl*, WM 2023, 1907 (1908); *Bittner*, VuR 2022, 9 (9); *Meller-Hannich*, DAR 2021, 493 (494); *Stierle*, IPRB 2021, 66 (66); *Riehm/Abold*, CR 2021, 530 (530 f.).

schlag zwischen Privatautonomie und Datenschutz (wie ihn auch Art. 1 Abs. 3 DSGVO vorsieht) wurde durch die DIRL sowie die Regelungen der §§ 327 ff. BGB geschaffen[11] und zeigt sich überdies in § 327q BGB, wonach die Ausübung datenschutzrechtlicher Betroffenenrechte und die Abgabe datenschutzrechtlicher Erklärungen des Verbrauchers nach Vertragsschluss die Wirksamkeit des Vertrags unberührt lassen. Darauf wird an späterer Stelle noch einzugehen sein (siehe Kap. 4.2).

3. Anwendungsbereich des Datenschuldrechts

Die §§ 327 ff. BGB beziehen sich auf Verbraucherverträge über digitale Produkte.[12] Damit gelten die Regelungen nicht für jedwede Vertragsabschlüsse und nicht für alle am Rechtsverkehr Beteiligten, sondern nur für Verträge, die sich im digitalen Raum abspielen und schützenswerte Personengruppen (Verbraucher) betreffen.

Für die Definition von Verbraucherverträgen ist § 310 Abs. 3 BGB maßgeblich – es muss sich um einen Vertrag zwischen einem Unternehmer i. S. d. § 14 BGB und einem Verbraucher i. S. d. § 13 BGB handeln. Die §§ 327 ff. BGB umfassen damit alle Verbraucherverträge zur Bereitstellung digitaler Produkte, insbesondere Austauschverträge wie Kauf- oder Werkverträge oder Dauerschuldverhältnisse wie Miet-, Leasing- oder Dienstverträge.[13] Ein spezielles „Digitalvertragsrecht" mit einer B2C-Geltung wurde nicht geschaffen.[14]

Während die DIRL bereits in ihrem Titel die „Bereitstellung digitaler Inhalte und digitaler Dienstleistungen" getrennt aufführt, spricht § 327 Abs. 1 BGB zusammenfassend von digitalen Produkten. Allerdings gliedert sich auch dieser Begriff in die von der DIRL eingeführten Begrifflichkeiten „digitale Inhalte" und „digitale Dienstleistungen" auf, wie § 327 Abs. 2 BGB verdeutlicht. Es soll sichergestellt werden, dass die Definitionen technologieoffen bleiben und auch künftige Entwicklungen einbeziehen können.[15] Die Begründung zum Gesetzesentwurf verdeutlicht, dass nicht der Inhalt

11 *Schmitz/Buschuew*, MMR 2022, 171 (171).
12 Für einen Überblick, auch hinsichtlich der weitergehenden (Aktualisierungs-) Pflichten siehe: *Gesmann-Nuissl u.a.*, in: BSI- Tagungsband zum 18. Deutschen IT-Sicherheitskongress, 2022, 35 (35 ff.)
13 *Riehm/Abold*, CR 2021, 530 (531).; *Kirchhefer-Lauber*, JuS 2021, 1125 (1126 u. 1129).
14 *Blassl*, WM 2023, 1907 (1908).
15 BT-Drs. 19/27653, S. 38.

maßgeblich ist, sondern „die Art und Weise, wie die Daten reproduzierbar beziehungsweise wiedergabefähig festgehalten werden, nämlich in digitaler Form".[16] Digitale Inhalte sind gem. § 327 Abs. 2 S. 1 BGB bzw. Art. 2 Nr. 1 DIRL Daten, die in digitaler Form erstellt oder bereitgestellt werden. Darunter fallen etwa Computerprogramme, Anwendungen, Video-, Audio- und Musikdateien, digitale Spiele, elektronische Bücher und andere elektronische Publikationen.[17] Digitale Dienstleistungen nach § 327 Abs. 2 S. 2 BGB bzw. Art. 2 Nr. 2 DIRL sind Dienstleistungen, die dem Verbraucher die Erstellung, die Verarbeitung oder die Speicherung von Daten in digitaler Form oder den Zugang zu solchen Daten ermöglichen (Nr. 1) oder die gemeinsame Nutzung der vom Verbraucher oder von anderen Nutzern der entsprechenden Dienstleistung in digitaler Form hochgeladenen oder erstellten Daten oder sonstige Interaktionen mit diesen Daten ermöglichen (Nr. 2).[18] Dies umfasst Angebote wie Software-as-a-Service, Datei-Hosting, Cloud-Computing, gemeinsame Spiele, cloudbasierte Textverarbeitung, soziale Netzwerke, Portale oder Plattformen.[19] Daneben treten gem. § 327 Abs. 4 BGB digitale Produkte, die aufgrund eines Kundenwunsches speziell angefertigt wurden, wie etwa maßgeschneiderte Software oder 3D-gedruckte Waren. Ebenso gilt der Großteil der Vorschriften der §§ 327 ff. BGB (d. h. alle mit Ausnahme der §§ 327b und 327c BGB) für Verbraucherverträge über die Bereitstellung von körperlichen Datenträgern, die ausschließlich als Träger digitaler Inhalte dienen (§ 327 Abs. 5 BGB). Dies können DVDs, CDs, USB-Sticks oder Speicherkarten sein.

Zeitgleich mit der DIRL wurde die WKRL verabschiedet. Auch diese bezieht sich ausschließlich auf Verbraucherverträge (Art. 3 WKRL), die – ebenso wie die DIRL – auf körperliche Gegenstände („Waren", vgl. auch Art. 3 DIRL) anzuwenden ist. Beide Richtlinien sind eng miteinander verwoben, dennoch muss der Anwendungsbereich im Einzelfall abgegrenzt werden. Im Unterschied zur DIRL gilt die WKRL insbesondere nicht nur für digitale Produkte. Mit der Einführung des § 327a BGB hat der Gesetzgeber versucht, die Abgrenzung der Anwendungsbereiche zu verdeutlichen, indem er sog. „Paketverträge" eingeführt hat. Dies sind Verträge, die neben der Bereitstellung digitaler Produkte die Bereitstellung anderer Sachen oder

16 BT-Drs. 19/27653, S. 38.
17 ErwGr. 19 der DIRL sowie BT-Drs. 19/27653, S. 39.
18 Zur Abgrenzung von „digitalen Inhalten" und „digitalen Dienstleistungen" im Einzelnen: *Riehm*, RDi 2022, 209 (211).
19 ErwGr. 19 der DIRL sowie BT-Drs. 19/27653, S. 39.

die Bereitstellung anderer Dienstleistungen zum Gegenstand haben, § 327a Abs. 1 S. 1 BGB. Damit geht er über den Wortlaut der Richtlinie hinaus, da nicht mehr nur „Waren", sondern „Sachen" i. S. d. § 90 BGB umfasst sind. § 327a BGB umfasst konsequenterweise auch Verbindungen von digitalen Produkten und unbeweglichen Sachen.[20] Ein klassisches Beispiel, für das die §§ 327 ff. BGB im Rahmen eines Paketvertrages auf den Vertragsteil des digitalen Produktes Anwendung finden, ist der Kauf eines Fernsehers mit Streaming-Abonnement. Hingegen finden die Vorschriften der WKRL infolge deren nationaler Umsetzung im Sachmangel-Gewährleistungsrecht Anwendung, wenn die Waren, die digitale Produkte enthalten, so von den digitalen Produkten abhängig sind, dass die Funktion ohne sie nicht erfüllt werden kann (z. B. das Betriebssystem eines Staubsaugerroboters). IoT-Produkte sind damit einheitlich dem Anwendungsbereich der WKRL unterstellt; Gewährleistungsansprüche richten sich damit nach den aus § 437 BGB folgenden Rechten.[21]

Die Unterscheidung ist deshalb maßgeblich, da im Rahmen des Anwendungsbereichs der §§ 327 ff. BGB für die vertragliche Leistung ein „Preis" gezahlt werden muss, der in dieser Konstellation eben auch im Bezahlen mit digitalen Wertedarstellungen (§ 327 Abs. 1 S. 2 BGB, wie z. B. einer In-Game-Währung eines Computerspiels als digitales Produkt) oder im Bereitstellen von personenbezogenen Daten liegen kann (§ 327 Abs. 3 BGB). Da der Konflikt zwischen datenschutzrechtlichen Schutzbestimmungen und der Privatautonomie demnach nur im Anwendungsbereich der DIRL und folglich der §§ 327 ff. BGB auftreten kann, werden sich die folgenden Ausführungen allein auf die Auswirkungen der DIRL beziehen.

4. Vertragsrechtliche Aspekte des Datenschuldrechts

Zwar ist der Anwendungsbereich der §§ 327 ff. BGB eröffnet, sobald ein Verbrauchervertrag über digitale Produkte vorliegt. Allerdings finden sich keine speziellen Regelungen über den Vertragsabschluss in den entsprechenden Paragraphen, sodass die allgemeinen Regeln der §§ 145 ff. BGB einschlägig sind.

20 BT-Drs. 19/27653, S. 46.
21 *Spindler*, MMR 2021, 451 (452).

4.1 Vertragsschluss

Das Vorliegen eines Vertrages nach nationalem Recht ist Dreh- und Angelpunkt, wie auch ErwGr. 25 der DIRL klarstellt: „Diese Richtlinie sollte auch nicht in Fällen gelten, in denen der Unternehmer nur Metadaten wie Informationen zum Gerät des Verbrauchers oder zum Browserverlauf erhebt, es sei denn, der betreffende Sachverhalt gilt als Vertrag nach nationalem Recht." Ein Vertrag ist ein zweiseitiges Rechtsgeschäft, konkret die von mindestens zwei Vertragspartnern erklärte Einigung über die Begründung oder Änderung eines Schuldverhältnisses, § 311 BGB. Dies kann einseitig verpflichtend sein (wie im Falle eines Schenkungsversprechens gem. § 518 BGB, oder einer Bürgschaft gem. § 765 BGB) oder zweiseitig verpflichtend (synallagmatisch wie ein Kaufvertrag gem. § 433 BGB oder ein Mietvertrag gem. § 535 BGB). Digitale Produkte und die durch diverse Technologien erwachsenden Möglichkeiten eines digitalen Vertragsschlusses lassen die Äußerungen der korrespondierenden Willenserklärungen und damit den Vertragsschluss auf vielfältige Art und Weise zu. Der deutsche Gesetzgeber scheint in Anbetracht der Gesetzesbegründung sehr schnell bei der Annahme eines Vertrages im digitalen Kontext: „Für die Annahme eines Vertragsschlusses könnte beispielsweise sprechen, dass der Unternehmer den Dienst oder die Leistung erbringt, weil er den Verbraucher motivieren will, auf seiner Seite weitere Webseitenaufrufe zu tätigen oder Dienste oder Leistungen in Anspruch zu nehmen, weil er Einnahmen für auf seiner Seite dargestellte Werbung erzielen will, deren Höhe in aller Regel von den Zugriffszahlen abhängt, oder weil er mit dem Einsatz von Tracking-Technologien und der nachfolgenden Anzeige personalisierter Werbung wirtschaftliche Vorteile anstrebt."[22] Bei Cookies oder Tracking-Tools wäre dann immer schon von einem Vertragsschluss auszugehen.[23] Ob in diesem Falle aber tatsächlich ein Rechtsbindungswille beider Parteien anzunehmen ist, scheint mehr als fraglich.[24] Einmal mehr ist es daher ratsam, den Gedanken hinter der Rechtsprechung zur Cookie-Banner-Problematik[25] (Gestaltung des Einwilligungsprozesses) heranzuziehen und diesen vom Datenschutz- ins Schuldrecht zu übertragen. Alleine aus der vorgefundenen Situation (aktiviertes

22 BT-Drs. 19/27653, S. 40.
23 *Spindler*, MMR 2021, 451 (453).
24 *Schmitz/Buschuew*, MMR 2022, 171 (174).
25 EuGH, Urt. v. 01.10.2019, Az. C-673/17, NJW 2019, 3433; vgl. Besprechung u.a. von *Gesmann-Nuissl*, InTeR 2019, 190 (190 ff.).

Häkchen bzw. Webseitenaufruf) lässt sich noch keine rechtlich bindende Erklärung ableiten, die datenschutz- oder schuldrechtliche Folgen verursachen kann. Ein Rechtsbindungswille kann doch nur dann angenommen werden, wenn er zuvor auch gebildet wurde. Andererseits kann erst die Annahme eines Vertragsschlusses den Verbraucher unter den Schutzschirm der §§ 327 ff. BGB stellen, sodass schon in dessen Interesse die Hürden nicht allzu hoch angesetzt werden dürfen, was wohl auch die schnelle Annahme eines Vertrages im digitalen Kontext nach der Gesetzesbegründung erklärt. Am Rechtsbindungswillen des Unternehmers bestehen hingegen keine Zweifel. Gerade wenn auf Seiten des Unternehmers Daten verarbeitet werden, weil deren werbliche Nutzung für ihn Einkünfte verspricht, kann stets auf einen Rechtsbindungswillen des Unternehmers geschlossen werden.[26]

Die Feststellung des Rechtsbindungswillens auf Seiten des Verbrauchers als zentrale Voraussetzung für einen Vertragsschluss einschließlich der datenschuldrechtlichen Folgen ist daher ein Aspekt, der einer weiteren Untersuchung bedarf (vgl. Kap. 6.).

4.2 Vertragliche Pflichten

Ist die Hürde des Vertragsschlusses genommen, sind die jeweiligen Rechte und Pflichten zu betrachten. Auf Seiten des Unternehmers steht die Pflicht, das digitale Produkt (sprich: digitale Inhalte oder digitale Dienstleistungen) bereitzustellen. Dies kann wahlweise in Form einer einmaligen Bereitstellung (vergleichbar eines Kaufes) oder einer dauerhaften Bereitstellung (vergleichbar einer Miete) von digitalen Inhalten und Dienstleistungen erfolgen.[27] Bezogen auf die eingangs genannten Beispiele sind die Zugänge zu Servern von Computerspielen als dauerhafte Bereitstellung, das Verschaffen eines digitalen Schwertes als einmalige Bereitstellung zu verstehen. Demgegenüber steht – als Gegenleistung – die Pflicht zur Zahlung eines Preises in Form von Geld, digitaler Wertedarstellungen oder personenbezogener Daten.

Eine Schwierigkeit bei der Annahme eines Vertragsschlusses ebenso wie bei der Bestimmung der korrespondierenden Pflichten ist, dass damit zwar die Hauptleistungspflichten feststehen und somit theoretisch ein zweisei-

26 *Kramme*, RDi 2021, 20 (22).
27 *Riehm/Abold*, CR 2021, 530 (531).

tig verpflichtendes (synallagmatisches) Schuldverhältnis vorliegen sollte. Denn schließlich ist die Situation des Zahlens mit Daten doch mit der des Zahlens eines Geldbetrages im Rahmen eines klassischen Kaufvertrags gem. § 433 BGB vergleichbar und es scheint unlogisch, die Situation des Zahlens mittels Daten (also Daten für das digitale Schwert) nun anders zu bewerten. Gleichwohl wurde eine solche synallagmatische Einordnung durch den Gesetzgeber gerade nicht getroffen[28], weil er in der Bereitstellung von Daten gerade keine „Gegenleistung" festmachen wollte.[29] Dies wird zum einen damit begründet, dass der Begriff und Deutungsumfang der „Gegenleistung" bei Daten unklar sei.[30] Grob umrissen kann man den Begriff der Gegenleistung folgendermaßen definieren: Ein „transaktionsspezifisches, typischerweise […] vermögensmehrendes Äquivalent zur Leistung, welches […] ein Austauschverhältnis prägt und […] nicht vom Gegenleistungsbegriff ausgeschlossen wurde."[31] Im Kontext des Bezahlens mit personenbezogenen Daten sei – so der Europäische Datenschutzbeauftragte – der Begriff „Gegenleistung" irreführend, da ein Verbraucher stets wisse, dass er mit Geld bezahle – nicht aber, wenn er mit Daten bezahle.[32] Aus diesem Grund lasse sich die Parallele nur eingeschränkt ziehen und eine synallagmatische Gegenleistung sei ausgeschlossen. Da die Verknüpfung zur Leistung des Unternehmers aber nicht zwingend synallagmatisch, sondern auch konditional oder kausal sein könne[33], würden sich andere Möglichkeiten eröffnen. Nach Ansicht des Gesetzgebers und des Europäischen Datenschutzbeauftragten soll es im Falle der Bereitstellung von Daten also genügen, dass eine schuldrechtlich kausale Verknüpfung vorliegt – ein Synallagma ist nicht erforderlich.[34]

Tatsächlich stellt sich die Situation aber so dar, dass die reine Bereitstellung (d. h. das Zurverfügungstellen) von personenbezogenen Daten für die Geschäftszwecke des Unternehmers kaum ausreichend sein wird, weil die Daten allein so nicht ökonomisch eingesetzt werden können. „Daten" im Sinne des § 327 Abs. 3 BGB orientieren sich am Begriff der personenbe-

28 *Schmitz/Buschuew*, MMR 2022, 171 (174).
29 BT-Drs. 19/27653, S. 35; *EDPS*, Stellungnahme 4/2017, S. 11 ff.
30 *EDPS*, Stellungnahme 4/2017, S. 11 f.
31 *Hacker*, ZfPW 2019, 148 (158 ff.); zu den Situationen des Ausschlusses vom Gegenleistungsbegriff siehe ders. S. 169 ff.
32 *EDPS*, Stellungnahme 4/2017, S. 12.
33 *Hacker*, ZfPW 2019, 148 (150).
34 Grüneberg/*Grüneberg*, BGB, § 312 Rn. 3b; anders *Hacker*, der eine konditionale Verknüpfung annimmt: ZfPW 2019, 148 (196 f.).

zogenen Daten aus Art. 4 Nr. 1 DSGVO.[35] In den hier angesprochenen Fallkonstellationen (wie der Kauf eines virtuellen Items) werden dabei hauptsächlich Name, E-Mail-Adresse, Geburtsdatum, Standort und IP-Adressen übermittelt.[36] Allein das Zurverfügungstellen dieser Daten kann aber nicht ausreichend sein, um das Vertragsverhältnis auszufüllen, da deren Verarbeitung ohne vorherige Einwilligung unzulässig wäre. Im Mittelpunkt der vertraglichen Pflicht steht damit einmal mehr die Einwilligung in datenschutzrechtlicher Hinsicht als Voraussetzung für das Bereitstellen der Daten als solches.[37] Bewertet man die dargestellte vertragliche Konstellation, so lässt sich feststellen, dass die reine Bereitstellung der Daten eigentlich nur nachgeordneten Charakter besitzen kann; die datenschutzrechtliche Einwilligung ist jedenfalls wesentlicher Teil der Gegenleistung.

Weil eine datenschutzrechtliche Betrachtungsweise zu einem mit der schuldrechtlichen Betrachtung in Konflikt stehenden Ergebnis kommt, kommt § 327q BGB zum Tragen. Danach bleibt die Möglichkeit der Ausübung der Datenschutzrechte des Verbrauchers uneingeschränkt erhalten, indem klargestellt wird, dass die Abgabe datenschutzrechtlicher Erklärungen des Verbrauchers nach Vertragsschluss die Wirksamkeit des Vertrags unberührt lässt, § 327q Abs. 1 BGB.[38] Abs. 2 der Vorschrift bestimmt, dass dem Unternehmer im Falle eines Widerrufes der datenschutzrechtlichen Einwilligung des Verbrauchers (Art. 7 Abs. 3 DSGVO) ein außerordentliches Kündigungsrecht bei Dauerschuldverhältnissen zusteht. Schließlich bestimmt § 327q Abs. 3 BGB, dass der Unternehmer aus der Geltendmachung der datenschutzrechtlichen Ansprüche keine vertraglichen oder gesetzlichen Ersatzansprüche ableiten darf.[39] Nur wenn der Verbraucher keine Nachteile aus einem Widerruf erleidet, kann eine Einwilligung im Sinne des Art. 4 Nr. 11, Art. 7 Abs. 4 DSGVO freiwillig sein (vgl. ErwGr. 42 DSGVO). In der Praxis mag § 327q BGB das Verhältnis zwischen Datenschuld- und Datenschutzrecht gut klären – gerade in Situationen, in denen sich beide Konstellationen jedoch diffus und widersprechend gegenüberstehen (vgl. Kap. 5) muss dieses Problem jedoch durch eine weniger harte Trennung aufgelöst werden (vgl. Kap. 6.).

35 BT-Drs. 19/27653, S. 40.
36 *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (87).
37 *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (90).
38 *Blassl*, WM 2023, 1941 (1942); *Bittner*, VuR 2022, 9 (12); *Stierle*, IPRB 2021, 66 (68).
39 *Blassl*, WM 2023, 1941 (1942); *Bittner*, VuR 2022, 9 (12).

4.3 Gewährleistungspflichten

Davon losgelöst stehen den Verbrauchern, die einen solchen Vertrag über digitale Produkte schließen, die in den §§ 327 ff. BGB genannten Gewährleistungsrechte zu. Dabei bestehen die bekannten Rechte wie die Nacherfüllung, Kündigung, Minderung oder Schadensersatz – allerdings in angepasster Form. Es kommt den betroffenen Verbrauchern insbesondere eine Beweislastumkehr in § 327k BGB zugute. § 327d BGB (i.V.m. §§ 327e bis 327g BGB) erweitert zudem den Produktmangelbegriff; das digitale Produkt muss kumulativ den subjektiven und objektiven Anforderungen und den Anforderungen an die Integration entsprechen, § 327d Abs. 1 S. 1 BGB. Schließlich gelten gem. § 327f BGB besondere Aktualisierungspflichten – ein Unterlassen stellt einen Produktmangel dar. Für einen detaillierten Überblick über die einzelnen Regelungen, die im Verhältnis von Schuld- und Datenschutzrecht nur eine untergeordnete Rolle spielen, sei auf die einschlägige Literatur verwiesen.[40]

Im Verhältnis von Datenschutz- und Schuldrecht wird die Regelung des § 327o Abs. 2 S. 1 BGB zur Vertragsbeendigung bedeutsam (wobei sich die Beendigungsgründe als solche aus §§ 327c, 327m und 327r BGB ergeben). Im Fall der Vertragsbeendigung hat der Unternehmer dem Verbraucher die Zahlungen zu erstatten, die der Verbraucher zur Erfüllung des Vertrags geleistet hat. Dies ist eine Umsetzung der Art. 15 u. 16 DIRL. § 327p Abs. 2 BGB ergänzt, dass nicht personenbezogene Daten, die der Verbraucher bereitgestellt hat, nicht weiter genutzt werden dürfen, wenn keine Ausnahmen aus § 327p Abs. 2 S. 2 Nrn. 1-4 BGB vorliegen. Für personenbezogene Daten gelten die Regeln der DSGVO und die damit einhergehenden Löschpflichten aus Art. 17 DSGVO.[41] Es stellt sich die Frage, wie die Rückgewährverpflichtung aus § 327o Abs. 2 S. 1 BGB hinsichtlich personenbezogener Daten umzusetzen ist – eine Problematik, die auch der Europäische Datenschutzbeauftragte erkannt hat, als er verneinte, dass Bereitstellung von Daten und Bereitstellung eines digitalen Produktes im synallagmatischen

40 *Blassl*, WM 2023, 1907 (1907 ff.); *Blassl*, WM 2023, 1941 (1941 ff.); *Bittner*, VuR 2022, 9 (9 ff.); *Paal/Wais*, DStR 2022, 1164 (1164 ff.); *Mayer/Möllnitz*, RDi 2021, 333 (333 ff.); *Stierle*, IPRB 2021, 66 (66 ff.); *Riehm/Abold*, CR 2021, 530 (530 ff.); *Güster/Booke*, MMR 2022, 92 (92 ff.); *Schreier/Michels*, RDi 2022, 381 (381 ff.); *Felsch u.a.*, MMR 2022, 18 (18 ff.); *Gesmann-Nuissl u.a.*, in: BSI- Tagungsband zum 18. Deutschen IT-Sicherheitskongress, 2022, 35 (35 ff.); *Spindler*, MMR 2021, 451 (451 ff.).

41 *Spindler*, MMR 2021, 528 (529).

Gegenseitigkeitsverhältnis stehen dürfen.[42] Wie damit allerdings auch praxisgerecht verfahren werden kann, wird zu klären sein (vgl. Kap. 6.).[43]

5. Datenschutzrechtliche Anforderungen des Datenschuldrechts

Mit der Klarstellung in § 327q BGB sind und bleiben die datenschutzrechtlichen Erklärungen möglich, wirksam und lassen den Vertragsschluss unberührt. Datenschutz- und schuldrechtliche Rechte und Pflichten bestehen damit nebeneinander. Das funktioniert geräuschlos jedoch nur, wenn die beiden Rechtsgebiete nicht ineinandergreifen – was sie aber aufgrund der auch für den Vertragsschluss notwendigen Einwilligung in die Datenverarbeitung machen. Ohne eine wirksame Einwilligung ist die geschuldete „Bereitstellung" von Daten – wie bereits angedeutet (vgl. Kap. 4.2) weitestgehend nutzlos für den Unternehmer.

Auf den ersten Blick scheinen das BGB (bzw. die DIRL) und das Datenschutzrecht unterschiedliche Zielsetzungen zu haben: Das BGB ist bezogen auf die Privatautonomie der Bürger zueinander und das Datenschutzrecht ist auf den Persönlichkeitsschutz bezogen, d. h. auf individuelle Statusbeziehungen.[44] Dies gilt jedoch nicht absolut, da die Regelungsgehalte naturgemäß ineinandergreifen müssen. Beispielsweise wird der Einzelne in der Ausübung seiner Privatautonomie dergestalt eingeschränkt, als dass gewisse Vorschriften (u.a. insbesondere auch die §§ 327 ff. BGB) zum individuellen Schutz Grenzen setzen. Ebenso ist das Datenschutzrecht (und das damit verbundene Recht auf informationelle Selbstbestimmung, vgl. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 7 und 8 GRCh, respektive Art. 1 Abs. 2 DSGVO) nicht schrankenlos gewährleistet. Im Rahmen der Prüfung der Verhältnismäßigkeit muss gegen andere Grundrechte abgewogen werden, wie beispielsweise in Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO.

5.1 Rechtmäßige Datenverarbeitung – insbesondere Einwilligung

Da die gesamte DSGVO Anwendung findet, ist im Grundsatz die Einwilligung in die Datenverarbeitung nicht die einzige Möglichkeit, zulässiger-

42 *EDPS*, Stellungnahme 4/2017, S. 12.
43 Vgl. dazu: *Metzger* in: Münchner Kommentar zum BGB, § 327o Rn. 9.
44 *Schmidt-Kessel/Grimm*, ZfPW 2017, 84 (85).

weise die Daten für die gewünschten ökonomischen Zwecke zu nutzen. Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO stellt eine Rechtsgrundlage für die Verarbeitung von Daten dar, wenn dies für die Erfüllung eines Vertrages mit der betroffenen Person oder aber zur Durchführung vorvertraglicher Maßnahmen erforderlich ist. Allerdings muss hierfür ein Vertrag (vgl. Kap. 4.1) vorliegen oder eine Maßnahme für vorvertragliche Regelungen; insbesondere muss die Verarbeitung aber dem Zweck dienen, den Vertrag zu erfüllen. Dies ist insbesondere der Fall bei der Preisgabe der E-Mail-Adresse, um die digitalen Inhalte zu erhalten[45] – im Falle von Computerspielen auch durch die Verknüpfung mit den Account-Daten zur Freischaltung der erworbenen Features. Zu einem anderen Zweck dürften die so bekannt gewordenen Daten aber nicht verarbeitet werden. Entscheidender Punkt im Anwendungsfall des Bezahlens mit Daten im Sinne der §§ 327 ff. BGB ist aber, dass die Daten nicht zur Vertragserfüllung verarbeitet werden, sondern diese im Rahmen der datenökonomischen Einsatzmöglichkeiten zu bspw. Marketingzwecken verwendet werden. Dies ist nach allgemeiner Meinung auch nicht durch den Rechtfertigungsgrund des Art. 6 Abs. 1 UAbs. 1 lit. b) DSGVO gedeckt.[46] Da zudem auch Art. 6 Abs. 1 UAbs. 1 lit. f) DSGVO im Rahmen des dort vorausgesetzten „berechtigten Interesses des Verantwortlichen" bislang lediglich Betrugsprävention, Direktwerbung sowie Maßnahmen zur Verbesserung von IT-Systemen inkludiert,[47] und damit alle darüberhinausgehenden Aktivitäten ausnimmt, bleibt die vorherige Einwilligung im Sinne des Art. 6 Abs. 1 lit. a) DSGVO die zumeist einzige Möglichkeit, den datenschutzrechtlichen Anforderungen gerecht zu werden.[48]

Eine wirksame Einwilligung bedarf einiger Voraussetzungen, vgl. Art. 6 Abs. 1 UAbs. 1 lit. a), Art. 7 und Art. 4 Nr. 11 DSGVO. Die Einwilligung im Sinne des Art. 4 Nr. 11 DSGVO ist freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abzugeben; es muss eindeutig sein, dass die betroffene Person (der Verbraucher) mit der Datenverarbeitung zum angegebenen Zweck einverstanden ist. Da dies der Verantwortliche (hier der datenverarbeitende Unternehmer) gem. Art. 7 Abs. 1 DSGVO

45 *Schmitz/Buschuew*, MMR 2022, 171 (172).
46 Simitis/Hornung/Spiecker gen. Döhmann/*Schantz*, Datenschutzrecht, Art. 6 Rn. 33; *Sattler*, JZ 2017, 1036 (1040).
47 BeckOK DatenschutzR/*Albers/Veit*, 47. Ed. 1.2.2024, DS-GVO Art. 6 Rn. 68.
48 Simitis/Hornung/Spiecker gen. Döhmann/*Schantz*, Datenschutzrecht, Art. 6 Rn. 33: „Die Verarbeitung von *Daten als Entgelt* kann vielmehr nur auf die Einwilligung der betroffenen Person gestützt werden".

nachzuweisen hat, wird dies in der Regel auf elektronischem Wege geschehen.

Informiertheit nach Art. 4 Nr. 11 DSGVO bedeutet, dass die Einwilligung nur für den konkreten Fall und in Kenntnis der Sachlage abgegeben sein darf, vgl. ErwGr. 32 S. 1 DSGVO. Erforderlich ist eine Information durch den Unternehmer vor Abgabe der Einwilligung, die andernfalls nicht informiert sein kann. ErwGr. 42 S. 4 DSGVO sieht vor, dass mindestens über die Identität des Verantwortlichen und über die Zwecke der Verarbeitung informiert werden soll. Das EDPB hält es, angelehnt an Art. 13 Abs. 2 lit. c) DSGVO, für erforderlich, dass zumindest die Identität des Verantwortlichen, die Verarbeitungszwecke und die Art der Daten benannt werden, ein Hinweis auf das Widerrufsrecht und ggf. ein Hinweis auf automatisierte Entscheidungsfindung im Sinne des Art. 22 DSGVO erfolgt und auf mögliche Verarbeitungsrisiken bei Drittstaatentransfers (vgl. Art. 49 Abs. 1 lit. a) DSGVO) hingewiesen wird.[49] Sofern sich eine Einwilligung auf mehrere Verarbeitende erstrecken soll – und das ist im Falle der Datenwirtschaft ein durchaus denkbares Szenario – muss sich dies aus den Informationen ergeben. Fraglich ist, ob die Datenverarbeitung gerechtfertigt ist, wenn zwar eine Einwilligung in Datenflüsse zwischen verbundenen Unternehmen erteilt wurde, aber einzelne Konzernunternehmen erst nach der Einwilligung hinzukommen.[50] Allerdings wird es hier auf die Einwilligungserklärung und deren Wortlaut im Einzelfall ankommen.[51]

Im Falle des Bereitstellens von Daten als Preis für die Leistung eines digitalen Produkts ist insbesondere auch die Maßgabe des Art. 7 Abs. 2 DSGVO zu beachten. Erfolgt nämlich „die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung […] so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist". Schriftform in diesem Zusammenhang bedeutet nicht etwa ein Schriftstück mit entsprechender Unterschrift wie § 126 BGB dies versteht, sondern erfasst grundsätzlich jede eindeutige schriftliche oder elektronische Willensbekundung (vergleichbar zu § 126b BGB).[52] Im Falle der Bereitstellung von Daten erfolgt die Einwilligungserklärung in die Datenverarbeitung zumeist elektronisch – und vor allen Dingen im Zuge eines Vertragsschlusses, z. B. nach § 433 BGB. Zu be-

49 *EDPB*, Leitlinien 5/2020, Rn. 64.
50 Gola/Heckmann/*Schulz*, DS-GVO, Art. 7, Rn. 38.
51 Gola/Heckmann/*Schulz*, DS-GVO, Art. 7, Rn. 38.
52 Gola/Heckmann/*Schulz*, DS-GVO, Art. 7, Rn. 41; *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art.. 7 Rn. 76.

achten ist also, dass die Einwilligung zur Datenverarbeitung vom Angebot bzw. der Annahme zum Vertragsabschluss (§§ 145 ff. BGB) klar unterschieden werden kann, da sie andernfalls nicht verbindlich sind (Art. 7 Abs. 2 S. 2 DSGVO).

Dreh- und Angelpunkt der Einwilligung – insbesondere im Falle des Datenschuldrechts – ist die Freiwilligkeit der Einwilligung, vgl. Art. 4 Nr. 11, Art 7 Abs. 4 und ErwGr. 32, 42 und 43 DSGVO. Eine Einwilligung ist nur dann als freiwillig zu betrachten, wenn sie ohne jeden Druck oder Zwang abgegeben werden kann.[53] ErwGr. 42 fordert eine echte und freie Wahl, sodass die betroffene Person in der Lage sein muss, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Gerade im Rahmen des „Bezahlens" mit Daten werden Anreize wie die vermeintliche Kostenfreiheit geschaffen, aber auch sonstige verhaltensökonomische Methoden eingesetzt, um die Verbraucher gezielt zu steuern. Hierfür gibt es zulässige Methoden[54]; Grenzen bestehen jedoch da, wo Verbraucher gezielt getäuscht und manipuliert werden, wie in den Fällen der *Dark Pattern*.[55] ErwGr. 43 DSGVO greift schließlich das Ungleichgewicht zwischen den beteiligten Personen auf, das bei der Beurteilung der Freiwilligkeit eine große Rolle spielt. Beispielhaft werden hier Behörden als Verantwortliche genannt – es ist jedoch nicht ausgeschlossen, dass ein vergleichbares Ungleichgewicht auch anzunehmen ist, wenn es sich um das Verhältnis Unternehmer und Verbraucher handelt. Eine solche Machtasymmetrie wird von einigen Kritikern der DIRL und deren Umsetzung angenommen, weil keine andere Möglichkeit bestehe, als die Privatheit preiszugeben.[56] Dies lässt sich umso mehr diskutieren, wenn es sich um minderjährige oder ältere Verbraucher handelt (vulnerable Gruppen). Eine Besonderheit gilt für die Einwilligung Minderjähriger in Bezug auf Dienste der Informationsgesellschaft gem. Art. 8 DSGVO.

5.2 Datenschutzrechtliche Grundsätze - insbesondere Kopplungsverbot

Ein die Freiwilligkeit der Einwilligung beeinflussender Grundsatz der DSGVO ist das in Art. 7 Abs. 4 DSGVO normierte Kopplungsverbot. Es

53 Gola/Heckmann/*Schulz*, DS-GVO, Art. 7, Rn. 19.
54 Wie beispielsweise das Nudging, vgl. *Kollmar/Schirmbacher*, WRP 2020, 1015 (1017).
55 *Martini u.a.,* ZfDR 2021, 47 (49 ff.); Gola/Heckmann/*Schulz*, DS-GVO, Art. 7, Rn. 19.
56 *Schmitz/Buschuew*, MMR 2022, 171 (173).

handelt sich um ein allgemeines, nicht etwa um ein absolutes Kopplungsverbot.[57] Dies wird aus der Formulierung „in größtmöglichem Umfang" deutlich.[58] Das Kopplungsverbot findet wohl hauptsächlich Anwendung auf Kopplungen von Vertragsschluss und Einwilligung[59] – wie in den nun durch §§ 327 ff. BGB erlaubten Fällen des Bezahlens mit Daten. Allein schon deswegen muss dieser bestehende Konflikt aufgelöst werden (vgl. Kap. 6.).

Von Art. 7 Abs. 4 DSGVO werden zunächst – das liegt aufgrund der Einordnung nahe – nur zulässige Verarbeitungen umfasst.[60] Es genügt nicht, dass nur der Verbraucher subjektiv das Gefühl hat, dass er eine echte Wahl hat, sondern diese Wahl muss objektiv bestimmbar sein. Insbesondere in Konstellationen, in denen es im Einzelfall angebracht ist, für verschiedene Verarbeitungssituationen eine gesonderte Einwilligung einzuholen, dies aber nicht geschieht, oder in Fällen, in denen die Vertragserfüllung von der Einwilligung abhängig ist, diese aber objektiv nicht für die Erfüllung des Vertrages erforderlich ist, ist eine objektive Wahlfreiheit ausgeschlossen und damit eine Kopplung zu bejahen.[61] Oftmals trifft aber genau dies – um die Cookie-Problematik aufzugreifen – auf die Cookie-Banner zu. Dort werden Nutzer häufig die Einwilligung in die Verwendung von Tracking-Cookies abgeben, obwohl diese für die Erbringung der Dienstleistung (Anzeige der Webseite) nicht nötig wäre.[62]

Teilweise wird das (allgemeine) Kopplungsverbot als ein erheblicher Eingriff in die Privatautonomie betrachtet. Insbesondere in Bezug auf das Datenschuldrecht kommt gerade die Diskrepanz zwischen zum Privatautonomie und Datenschutz zum Tragen, weswegen es essentiell ist, dass das Kopplungsverbot eben nicht absolut, sondern nur in einem verhältnismäßig angemessenen Umfang angewendet wird.[63] Unverhältnismäßigkeit wäre allenfalls dann zu bejahen, wenn der Unternehmer eine herausgehobene (Monopol-)Stellung besäße und die Verbraucher auf die Leistungen ange-

57 *EDPB*, Leitlinien 05/2020, Rn. 34 u. 35; a.A.: *Dammann*, ZD 2016, 307 (311).
58 Gola/Heckmann/*Schulz*, DS-GVO, Art. 7, Rn. 23.
59 ÖOGH, Urt. v. 31.8.2018, Az. 6 Ob 140/18h, BeckRS 2018, 30960 Rn. 35.
60 Gola/Heckmann/*Schulz*, DS-GVO, Art. 7, Rn. 25.
61 *EDPS*, Stellungnahme 4/2017, S. 21.
62 *EDPS*, Stellungnahme 4/2017, S. 13.
63 Gola/Heckmann/*Schulz*, DS-GVO, Art. 7, Rn. 27.

wiesen wären.[64] Vorliegend kommt zudem die Maßgabe des ErwGr. 42 DSGVO zum Tragen, nach dem eine Person keine „Nachteile" erleiden darf, wenn die Einwilligung versagt wird. Handelt es sich bei den Nachteilen lediglich um Preisnachlässe, soll das nicht das Kopplungsverbot zur Anwendung bringen.[65] Auch das Ablehnen eines Vertrages kann kein Nachteil im Sinne des ErwGr. 42 DSGVO sein, da gerade dies Basis jedweder privatautonomen Handlung (z.B. eines Vertrages) ist. Zudem ist bei der Auslegung des Kopplungsverbotes in Bezug zum Datenschuldrecht die Intention des Richtlinien- und des Gesetzgebers zu berücksichtigen, die die Verknüpfung ja gerade gewollt haben.[66] Zusätzlich greift das Argument, dass seitens des Verbrauchers zumeist die Wahl des Preises (Entgelt, digitale Wertedarstellungen oder personenbezogene Daten) verbleibt – allein im Falle der alleinig möglichen Datenzahlung kommt das Argument erneut im Zuge der Freiwilligkeit zum Tragen, muss jedoch auch hier im Kontext der gesetzgeberisch gewollten privatautonomen Entscheidung betrachtet werden.

Unter Kap. 5.1 wurde bereits angesprochen, dass die Daten zu keinem anderen Zweck verwendet werden dürfen als zu dem, in den eingewilligt wurde. Dies folgt aus Art. 5 Abs. 1 lit. b) DSGVO. Diese Zweckbindung gilt vom Zeitpunkt der Erhebung bis zur Zweckerfüllung an.[67] Eine Zweckänderung ist grundsätzlich unzulässig. Ausnahmen hierzu finden sich in Art. 6 Abs. 4 DSGVO; dann aber ist der Betroffene hierüber zu informieren, Art. 13 Abs. 3 und Art. 14 Abs. 4 DSGVO.

5.3 Widerruf der Einwilligung und Löschpflichten

Ist der Zweck erreicht, sind die personenbezogenen Daten zu löschen, vgl. Art. 17 Abs. 1 lit. a) DSGVO. Das Gleiche gilt auch für diejenigen Fälle, in denen der Verbraucher gem. Art. 7 Abs. 3 DSGVO seine Einwilligung widerruft. Dazu hat er – worüber er entsprechend informiert werden muss (Kap. 5.2) – das jederzeitige Recht. Dies lässt, wie § 327q BGB regelt, die Wirksamkeit des Vertrags unberührt (Kap. 4.3). Damit bleibt die Datenver-

64 Gola/Heckmann/*Schulz*, DS-GVO, Art. 7, Rn. 27; unter Verweis u.a. auf: *Buchner*, DuD 2016, 155 (158); *Gierschmann*, ZD 2016, 51 (54); a.A.: *EDPB*, Leitlinien 05/2020, Rn. 38; BeckOK DatenschutzR/*Stemmer*, DS-GVO, Art. 7, Rn. 45.
65 *EDPB*, Leitlinien 05/2020, Rn. 50.
66 Gola/Heckmann/*Schulz*, DS-GVO, Art. 7, Rn. 30.
67 Gola/Heckmann/*Pötters*, DS-GVO, Art. 5, Rn. 18.

arbeitung bis zum Ausspruch des Widerrufs wirksam, es handelt sich um eine ex nunc-Wirkung. Allerdings hat der Unternehmer gem. § 327q Abs. 2 BGB in diesen Fällen das Recht, den Vertrag zu kündigen.

Wird der Widerruf nach Art. 7 Abs. 3 DSGVO ordnungsgemäß ausgeübt, sind die Daten zu löschen, wenn es an einer anderweitigen Rechtsgrundlage für die Verarbeitung fehlt (Art. 17 Abs. 1 lit. b) DSGVO). Insbesondere im Rahmen des ökonomischen Datenverkehrs, der durch das Datenschuldrecht etabliert wird, ist die Sicherstellung der Löschung ein großes praktisches Problem.

6. Konfliktpotenziale und -lösungen

Im Zuge der Untersuchung zu den rechtlichen Grundlagen des Datenschuldrechts wurden einige problematische Punkte aufgezeigt, die es in der Praxis – insbesondere auch im Vorgriff zur Einrichtung eines Datenwirtschaftsportals (vgl. Kap. 6.3) – zu lösen gilt; das Spektrum reicht von rein vertragsrechtlichen (wie den Rechtsbindungswillen und das Verhältnis von Leistung und Gegenleistung) über rein datenschutzrechtliche (Informiertheit und Freiwilligkeit der Einwilligung) bis hin zu verbindenden, „datenschuld-schutzrechtlichen" Fragestellungen (wie die Frage nach dem Kopplungsverbot und der Rückabwicklung des Vertrages).

6.1 Rechtliche Konfliktlösung

Rein rechtlich sind diese Problempunkte nur durch verbraucherfreundliche Auslegung und Anwendung der Normen zu lösen. Es sind jedoch die Wertungen, die der Gesetzgeber generell zur Anwendung bringen möchte, mitzudenken. Hinsichtlich der vertragsrechtlichen Problempunkte des Rechtsbindungswillens und des Vertragsschlusses gilt Folgendes: Im Falle eines Vertragsschlusses, bei dem ein Verbraucher aktiv die Wahl zwischen der Bezahlung eines Preises, Bezahlung mit digitalen Wertedarstellungen oder Bezahlung mit personenbezogenen Daten hat und sich für Letzteres entscheidet, ist die Annahme eines Rechtsbindungswillens unproblematisch. Fraglich ist vielmehr, ob – ähnlich wie bei der Cookie-Problematik – allein die vorgefundene Situation für die Annahme eines Vertrages ausreichen kann, da hier die Willensbildung mehr als problematisch ist. Allerdings ist

die Intention des Gesetzgebers wertend heranzuziehen: Der Verbraucher soll durch die §§ 327 ff. BGB besonders geschützt werden. Die weitgehende Ablehnung eines Rechtsbindungswillens würde ihm diese Schutzvorschriften vorenthalten und er wäre schutzloser gestellt.[68] Gerade wenn der Unternehmer ein Interesse an der ökonomischen Weiterverarbeitung der Daten hat und eine „Leistung" erhält, sollte der Verbraucher nicht schutzlos bleiben und ein Vertrag angenommen werden. Dies gilt umso mehr, als gerade in solchen digitalen (Kauf-)Situationen vulnerable Gruppen, wie Minderjährige oder Ältere, dazu neigen, besonders naiv zu agieren und daher besonderen Schutz bedürfen (insbesondere auch, weil Minderjährige von Gesetzes wegen gesteigert geschützt sind).[69]

Auch die Fragestellung nach dem Synallagma sollte der gesetzgeberischen Intention gerecht werden. Gegenleistungen müssen nicht notwendigerweise synallagmatisch verknüpft werden, sondern es ist ebenso eine kausale oder konditionale Verknüpfung denkbar.[70] Auch, wenn die Kaufsituation und die Zahlung eines Entgeltes intuitiv an ein Synallagma denken lässt, bleibt der Verbraucher bei einer kausalen oder konditionalen Verknüpfung nicht schutzlos (vgl. §§ 812 ff. BGB). Diese Problematik wurde im Vorfeld hinreichend diskutiert und der Wortlaut des Gesetzes entsprechend zurückhaltend formuliert.[71]

Bezüglich des datenschutzrechtlichen Grundsatzes des Kopplungsverbotes aus Art. 7 Abs. 4 DSGVO ist der gesetzgeberische Wille in die Beurteilung einzubeziehen. Lehnt man mit der wohl herrschenden Meinung ein absolutes Kopplungsverbot ab[72], bedeutet die Annahme eines allgemeinen Kopplungsverbotes, dass die Möglichkeit der Verbindung von vertraglichen Pflichten und „geschuldeter" bzw. vielmehr kausal verknüpfter Datenbereitstellung möglich ist – insbesondere eben auch, weil der Gesetzgeber diese Möglichkeit wollte. Dies wird insbesondere dann kein Problem darstellen, wenn der Verbraucher die Wahl zwischen Entgelt, digitalen Wertedarstellungen und personenbezogenen Daten hat. Es verbleibt jedoch die gleiche Problematik wie beim Vertragsschluss – wie ist im Falle von Datenerhebungen zu verfahren, die nicht wirklich nötig sind und hinsichtlich derer die Wahlfreiheit in gewisser Hinsicht wegfällt. Dies wird aber nicht auf rein

68 *Kramme*, RDi 2021, 20 (22).
69 Vgl. zur Gesamtproblematik im Kontext: *Gesmann-Nuissl/Meyer*, Robotics 2022, 11, 125.
70 *Hacker*, ZfPW 2019, 148 (150).
71 *EDPS*, Stellungnahme 4/2017, S. 12.
72 *EDPB*, Leitlinien 05/2020, Rn. 34 u. 35.

rechtlicher Ebene zu lösen sein. Hier bedarf es eines praktischen Umsetzungsansatzes, der die Informiertheit des Verbrauchers im Sinne des Art. 4 Nr. 11 und Art. 7 DSGVO in den Blick nimmt und über die Grundlagen und Rechtsfolgen in verständlicher Weise aufklärt (vgl. Kap. 6.2). Gerade die Informiertheit und Freiwilligkeit der Einwilligung muss sich im digitalen Umfeld stimmig an die technische Umgebung anpassen und nachvollziehbar bleiben.

In der Kombination Schuld- und Datenschutzrecht hat auch die Rückabwicklung des Vertrages seinen Raum. Für nicht personenbezogene Daten findet § 327o Abs. 2 S. 1 BGB Anwendung – „Zahlungen" sind zu erstatten. In Bezug auf personenbezogene Daten verweist Art. 16 Abs. 2 DIRL auf die DSGVO; einen entsprechenden Hinweis gibt es im BGB nicht, ist jedoch aufgrund der Regelung des § 327q BGB naheliegend. Die personenbezogenen Daten des Verbrauchers sind damit infolge eines Widerrufs der Einwilligung nach Art. 7 Abs. 3 DSGVO gem. Art. 17 Abs. 1 lit. b) DSGVO zu löschen. Darauf besteht bereits ein datenschutzrechtlicher Anspruch – ein Argument dafür, dass es schuldrechtlicher Löschungsansprüche als Folge eines Synallagmas im BGB nicht mehr bedarf. Für die Rückabwicklung innerhalb dieses Vertragsverhältnisses und für den Löschanspruch bestehen also keine anderen Anforderungen als bei jedem anderen Widerruf der Einwilligung.

6.2 Praktische Konfliktlösung

Die hinreichende Aufklärung hinsichtlich der Voraussetzungen und Folgen eines Vertragsschlusses, damit (1) ein Rechtsbindungswille gebildet werden kann und (2) die Einwilligung freiwillig und informiert erfolgen kann, bedarf eines praktischen, verbraucherfreundlichen und verständlichen Ansatzes. Die Reaktion auf die Cookie-Rechtsprechung des EuGHs[73] sowie auf die Umsetzung des Art. 5 Abs. 3 ePrivacyRL in § 25 TTDSGG hinsichtlich des vorangekreuzten Zustimmungskästchens war, dass nunmehr große (oftmals rechtswidrig gestaltete) Cookie-Banner auf der Webseite erscheinen und das Einwilligungskästchen zentral präsentiert wird, was dazu führt, dass Verbraucher den Banner wegklicken wollen und in die Erhebung von Tracking-Cookies einwilligen, ohne die Folgen zu reflektieren. Die-

73 EuGH, Urt. v. 01.10.2019, Az. C-673/17, NJW 2019, 3433.

se oder vergleichbare Cookie-Banner sind im Hinblick auf § 25 TTDSG rechtswidrig, da insoweit alternative, gleichartig präsentierte Formen der Zustimmung bzw. Ablehnung angeboten werden müssen.[74] Im Hinblick auf die Datenökonomie und dem Bezahlen mit Daten sind die Folgen aber noch weitreichender als beim bloßen Einsatz von Tracking-Cookies, da diese Daten, regelmäßig verbunden mit den personenbezogenen Daten usw., verwendet werden, um umfassende Profile zu bilden und Nutzer gezielt zu manipulieren.[75] Eine mit Cookie-Bannern vergleichbare – sich in der Praxis als nicht effektiv erweisende – Aufklärung sollte hier nun nicht angestrebt werden, weil dies dem Interesse des Verbraucherschutzes zuwiderläuft. Insbesondere, wenn es um die ökonomische Verwertung und Verarbeitung personenbezogener Daten geht, sollte auf eine konkrete und gezielte Aufklärung besonders Wert gelegt werden, damit die (auch wenig reflektierenden) Verbraucher genügend Informationen erhalten, um eine individuelle Abwägung treffen zu können.

Der praktische Ansatz sollte dabei die Idee des Bezahlens mit Daten und die damit einhergehenden Willenserklärungen besser aufzeigen. Die Tatsache, dass den Daten stärker denn je ein Wert zugeschrieben wird, muss bereits in der Information berücksichtigt werden und eine zentrale Rolle einnehmen.

6.3 Konkrete Ausgestaltung des Lösungsansatzes

Es bedarf eines intuitiv nutzbaren Werkzeugs, welches es den Nutzern ermöglicht, informiert und selbstbestimmt mit ihren personenbezogenen Daten im dynamischen und virulenten Marktumfeld zu agieren. Dieses Werkzeug benötigt zum einen ein Datenwertmanagement als wesentlichen Baustein. Es muss zum einen herausgefunden werden, welchen subjektiven Wert Daten für den Nutzer haben (können), um zum anderen einen objektiven Wert für die Daten bestimmen zu können. In Ansehung einer möglichst hohen Nutzerfreundlichkeit muss dieses Werkzeug in seiner Ausgestaltung und Anwendbarkeit einfach und leicht zugänglich sein. Es muss sichtbar werden, dass es die Interessenkonflikte von Verbrauchern und Unternehmen aufgreift und löst. Ziel sollte ein intuitives Portal zum Schutz der Datensouveränität in der Datenwirtschaft sein, das zu einer

74 Assion/*Schneider*, TTDSG, § 25 Rn. 30 f.
75 *Langhanke/Schmidt-Kessel*, EuCML 2015, 218 (219).

zentrale Anlaufstelle für Verbraucher wie auch Unternehmen wird, um personenbezogene Daten objektiv und fair zu bewerten bzw. bewerten zu können.

Die Einrichtung eines solchen Portals bedarf zunächst einiger Voruntersuchungen. Insbesondere müssen rechtskonforme Metriken entwickelt werden, die es ermöglichen, den Datenwert zu bestimmen. Da dieser Datenwert je nach Blickwinkel (ob aus Unternehmer- oder Nutzersicht) unterschiedlich ausfallen kann, ist vorab eine Untersuchung auf Basis eines quantitativen Marktforschungsansatzes angezeigt.[76] Bezogen auf konkrete Kaufentscheidungen könnte den Probanden (in der Rolle von Verbrauchern) hier aufgezeigt werden, ob sie den genannten Kaufpreis für ein digitales Produkt zahlen wollen oder personenbezogene Daten dafür preisgeben wollen. Indem die Preishöhe stetig angepasst wird, lässt sich hier die Schwelle Preis-personenbezogenes Datum bestimmen und in der Folge ein auf den Probanden bezogener subjektiver Wert des Datums. Nachdem den Probanden daraufhin unternehmerische Verarbeitungsmöglichkeiten aufgezeigt werden und sie über die Reichweite der Datenverarbeitung informiert werden (und damit dem Wert aus unternehmerischer Sicht), könnte der gleiche Test erneut stattfinden und so ein objektivierter Daten-Wert gebildet werden. Dies gibt zur Vorbereitung der Darstellung des Werkzeugs wertvolle Aufschlüsse hinsichtlich folgender Fragen: Welche Datenfreigaben sind dem Konsumenten mehr wert als andere? Gibt es unterschiedliche Präferenzen bezogen auf die Personengruppen? Gibt es Datenfreigaben, die nach erfolgter Aufklärung tabu sind? Daraus wiederum folgen wertvolle Hinweise (auch aus unternehmerischer Sicht) hinsichtlich der Frage, welche Wahlmöglichkeiten effektiv angeboten werden können oder nicht.

Die konkrete Umsetzung und Sichtbarmachung des Datenwertes kann beispielsweise in Form eines digitalen Daten-Zwillings geschehen, der auf einen Blick zeigt, welche Daten welchen Wert haben und wie sich dieser verändern könnte bzw. wird, wenn diese Daten in die Wirtschaft zur ökonomischen Verwertung gegeben werden. Letzteres lässt sich ohne weiteres auf einem Portal realisieren, auf das Unternehmer und Verbraucher gleichermaßen zugreifen können. Ein solches Portal ist auch hinreichend lebendig, so dass sich einerseits Preisschwankungen zu den Datenwerten abbilden lassen und andererseits der Tatsache Rechnung getragen werden

76 Beschrieben u.a. bei: Johnson, R. M., & Orme, B. K. (2007). *A new approach to adaptive CBC.* Sawtooth Software Inc. Sawtooth Software Research Papers Series.

kann, dass Daten – anders als Entgelt – mehrfach als Preis eingesetzt werden können, was ebenfalls deren Wert verändern würde.

Die vorgestellte Lösung (das „Datenwirtschaftsportal") muss zwingend als unabhängige und objektive Instanz funktionieren, wenn sie als wichtiges Element die Aufklärung während der vertragsrechtlichen Willensbildung unterstützen, und zur datenschutzrechtlichen Folgeabschätzung hinsichtlich der Konsequenzen der Einwilligung beitragen soll. Sie muss Vertrauen generieren. Die Dynamik, die in einer solchen Portallösung angelegt ist, kann fortlaufend weitere Entwicklungen aufnehmen und hierdurch das Konzept der datenschutz- und datenschuldrechtlichen Symbiose weiter ausgestalten. Das Nutzerverhalten wird dabei fortlaufend evaluiert werden müssen, um auf Basis neuer Erkenntnisse und Entwicklungen das Portal fortlaufend anzupassen. Ferner bleibt die Darstellung des Datenwertes hinreichend flexibel, der sich aufgrund der Häufigkeit des Datenbereitstellens, der Nutzerpräferenzen und aufgrund des Einsatzgebietes beim Bezahlen mit Daten verändern wird. Daten erhalten einen „Marktpreis", ähnlich wie Aktien oder Emissionswerte. Ferner können neu aufkommende, digitale Ökosysteme über das Portal stetig berücksichtigt und eingebunden werden. Hinzu kommt, dass die Erfahrenheit der Nutzer im Umgang mit ihren personenbezogenen Daten nicht nur in das Design des Portals einfließen, sondern durch das Nutzen des Portals wachsen wird. Selbst wenig reflektierende Gruppen, wie z. B. Minderjährige oder ältere Nutzer können (und werden) ein Gefühl für den Wert ihrer personenbezogenen Daten entwickeln. Eine stetige Evaluation stellt schließlich sicher, dass das Portal synergetisch mit Nutzern und Unternehmen (d. h. den Akteuren am Markt) zusammenspielt. Es soll kein regulierender Markt geschaffen werden (welcher weitere Fragen mit sich bringt), sondern es soll ausschließlich die Selbstbestimmung der Verbraucher gesteigert werden, sodass deren Teilhabe an datenbasierten, digitalen Geschäftsmodellen möglich wird und sich über die erlangten Erkenntnisse die Datenwirtschaft insgesamt weiter entwickeln lässt.

7. Ergebnis

Die vorangegangene Untersuchung hat gezeigt, wie das neue Datenschuldrecht auf Grundlage der DIRL in das deutsche Zivilrecht implementiert wurde. Es wurde festgestellt, dass die im Vorfeld und auch nach Inkrafttreten der DIRL und der §§ 327 ff. BGB geäußerten rechtlichen Bedenken

lösbar sind und dass ein Ausgleich von datenschuld- und datenschutzrechtlichen Vorgaben möglich ist. Die objektiv bestehenden Konflikte sind allesamt versöhnbar und können im Interesse des Verbraucherschutzes einer lebensnahen Lösung zugeführt werden.

Die noch verbleibenden Probleme zeigen sich auf subjektiver Seite, zum einen bei der Bildung des eindeutigen vertraglichen Rechtsbindungswillens und zum anderen bezogen auf die Informiertheit und Freiwilligkeit der Einwilligung bezüglich der Herausgabe von Daten in datenschutzrechtlicher Hinsicht. Um dennoch Privatautonomie und informelle Selbstbestimmung zur Entfaltung zu bringen, haben wir ein „Datenwirtschaftsportal" vorgeschlagen, welches dazu beitragen kann, die erkannten Defizite zu überwinden. Zum einen macht es den Preis für Daten und damit die Gegenleistung auch in Verträgen nach §§ 327 ff. BGB hinreichend transparent und nachvollziehbar. Zum anderen verhilft es den Verbrauchern zu bewussten, informierten und freiwilligen Entscheidungen im Sinne der DSGVO.

In der neu aufkommenden Datenwirtschaft kann sich die Plattform zu einem unverzichtbaren Werkzeug entwickeln, wenn alle Akteure im Markt, die Verbraucher und Unternehmen, dort synergetisch zusammenwirken. Dies würde zugleich die allgemeine Akzeptanz bezüglich der Datenwirtschaft sowohl auf Verbraucher- als auch auf Unternehmensseite befördern. Wenn es zudem gelingt, die Entwicklung eines solchen Portals nicht nur anzustoßen, sondern dynamisch weiterzuentwickeln, kann dieses jedenfalls den Zweispalt zwischen Datensouveränität der Verbraucher und monetären Interessen der Datenwirtschaft auflösen und auch als Beispiel für weitere Anwendungen dienen, wenn das Konstrukt des Bezahlens mit Daten nicht nur im digitalen Umfeld etabliert wird, sondern auch nicht-digitale Produkte einen alternativen Preis bekommen.

Literatur

Assion, Simon (Hrsg.) (2022): TTDSG. Baden-Baden: Nomos.

Bittner, Lydia (2022): Verträge über digitale Produkte – der Beginn des digitalen Zeitalters im BGB. *Verbraucher und Recht (VuR),* 1/22, S. 9-15.

Blassl, Johannes (2023): Neues digitales Vertragsrecht – Teil I. *Zeitschrift für Wirtschafts- und Bankrecht, Wertpapiermitteilungen (WM)*, 41/23, S. 1907-1912.

Blassl, Johannes (2023): Neues digitales Vertragsrecht – Teil II. *Zeitschrift für Wirtschafts- und Bankrecht, Wertpapiermitteilungen (WM)*, 42/23, S. 1941-1946.

Buchner, Benedikt (2016): Grundsätze und Rechtmäßigkeit der Datenverarbeitung unter der DS-GVO. *Datenschutz und Datensicherheit (DuD),* 40(3), S. 155-161. https://doi.org/10.1007/s11623-016-0567-0

Bundesregierung (2021). Entwurf eines Gesetzes zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen. BT-Drs. 19/27653. Berlin: Deutscher Bundestag.

Cameron, William Bruce (1963): *Informal Sociology, A Casual Introduction to Sociological Thinking*. New York: Random House.

Dammann, Ulrich (2016): Erfolge und Defizite der EU-Datenschutzgrundverordnung. Erwarteter Fortschritt, Schwächen und überraschende Innovationen. *Zeitschrift für Datenschutz (ZD),* 7/16, S. 307-314.

Do, Thomas (2021): Items, Waffen und Skins – 5 Spiele mit extrem teuren Inhalten. Esports.com vom 30.05.2021. https://www.esports.com/de/items-waffen-und-skins-5-spiele-mit-extrem-teuren-inhalten-215415 (abgerufen am 30.01.2024).

European Data Protection Board (EDPB) (04.05.2020): Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf (abgerufen am 07.02.2024).

European Data Protection Supervisor (EDPS) (14.03.2017): Stellungnahme 4/2017 zu dem Vorschlag für eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte. https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_de.pdf (abgerufen am 05.02.2024).

Felsch, Johannes Claudio, Kremer, Julian und Wagener, Jonas (2022). Handhabung der neuen Aktualisierungspflicht bei digitalen Produkten. Anwendungsbereich, Inhalt und Dauer anhand zweier konkreter Beispiele. *Multimedia und Recht (MMR)*, 1/22, S. 18-23.

Gesmann-Nuissl, Dagmar (2019): Rechtsprechungsreport. *Zeitschrift zum Innovations- und Technikrecht (InTeR*), 4/19, S. 190-195.

Gesmann-Nuissl, Dagmar, Kunitz, Stephan und Rätze, Michael (2022): Chefsache Aktualisierung – mehr Sicherheit durch Updatepflicht. In: *Cyber-Sicherheit ist Chefinnen- und Chefsache, Tagungsband zum 18. Deutschen IT-Sicherheitskongress, 2022*. Bonn: SecuMedia, 2022, S. 35 – 50.

Gesmann-Nuissl, Dagmar and Meyer, Stefanie (2023): From Self to Avatar as Likeness: Legal Barriers and Opportunities. In: *International Conference on Human-Agent Interaction (HAI '23), December 04-07, 2023, Gothenburg, Sweden*. ACM, New York, NY, USA. https://doi.org/10.1145/3623809.3623935

Gesmann-Nuissl, Dagmar and Meyer, Stefanie (2022): Siri 2.0 - Conversational Commerce of Social Bots and the New Law of Obligations of Data: Explorations for the Benefit of Consumer Protection. *Robotics,* 11(6), S. 125. https://doi.org/10.3390/robotics11060125

Gierschmann, Sibylle (2016): Was „bringt" deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber die Rechtsunsicherheit bleibt. *Zeitschrift für Datenschutz (ZD),* 2/16, S. 51-55.

Gola, Peter und Heckmann, Dirk (Hrsg.) (2022): *Kommentar Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*. 3. Aufl. München: C.H.Beck.

Grüneberg, Christian (Hrsg.) (2023): *Kommentar Bürgerliches Gesetzbuch*. 82. Aufl. München: C.H.Beck.

Guinessworldrecords: Most Valuable Virtual Object. https://www.guinnessworldrecords.com/world-records/92207-most-valuable-virtual-object (abgerufen am 18.04.2024).

Güster, Florian und Brooke, Christina (2022): Umsetzung der Warenkaufrichtlinie. Rechtssichere Implementierung von negativer Beschaffenheitsvereinbarung und Verjährungsverkürzung bei Gebrauchtwagen im Internet. *Multimedia und Recht (MMR)*, 2/22, S. 92-97.

Hacker, Philipp (2019): Daten als Gegenleistung: Rechtsgeschäfte im Spannungsfeld von DS-GVO und allgemeinem Vertragsrecht. *Zeitschrift für die gesamte Privatrechtswissenschaft (ZfPW)*, 2/19, S. 148-197.

Johnson, Richard M. und Orme, Bryan K. (2007). A New Approach to Adaptive CBC. Sawtooth Software Research Paper Series. https://sawtoothsoftware.com/resources/technical-papers/a-new-approach-to-adaptive-cbc.

Kirchhefer-Lauber, Anna (2021): Verbraucherverträge über digitale Produkte. Die deutsche Umsetzung der Digitale-Inhalte-Richtlinie im BGB. *Juristische Schulung (JuS),* 12/21, S. 1125-1129.

Kollmar, Frederika und Schirmbacher, Martin (2020): Kommentar zum Urt. d. BGH v. 28.05.2020, Az. I ZR 7/16. *Wettbewerb in Recht und Praxis (WRP),* 8/20, S. 1015-1017.

Kramme, Malte (2021): Vertragsrecht für digitale Produkte. Die Umsetzung der Digitale-Inhalte-Richtlinie im Schuldrecht AT. *Recht Digital (RDi),*1/21, S. 20-29.

Langhanke, Carmen und Schmidt-Kessel, Martin (2015): Consumer Data as Consideration. *Journal of European Consumer and Market Law (EuCML)*, 6/2015, S. 218-223.

Martini, Mario, Drews, Christian, Seeliger, Paul und Weinzierl, Quirin (2021): Dark Patterns. Phänomenologie und Antworten der Rechtsordnung. *Zeitschrift für Digitalisierung und Recht (ZfDR)*, 1/21, S. 47-74.

Mayer, Maximilian und Möllnitz, Christina (2021): Gewährleistung für „smarte" Produkte nach Umsetzung der Digitale Inhalte- und Warenkauf-Richtlinie. *Recht Digital (RDi),* 7/21, S. 333-340.

Meller-Hannich, Caroline (2021): Die Warenkaufrichtlinie und ihre Umsetzung. *Deutsches Autorecht (DAR),* 9/21, S. 493-497.

Norberg, Patricia A., Horne, Daniel R. und Horne, David A. (2007): The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs (JCA)*, 41(1), S. 100-126.

Paal, Boris P. und Wais, Niklas (2022): Ein Update für das BGB: Die Umsetzungen der Warenkauf- und Digitale-Inhalte-Richtlinie im Überblick. *Deutsches Steuerrecht (DStR)*, 23/22, S. 1164-1168.

Riehm, Thomas (2022): Verträge über digitale Dienstleistungen. *Recht Digital (RDi),* 5/22, S. 209-216.

Riehm, Thomas und Abold, Metawi Adrian (2021): Rechtsbehelfe von Verbrauchern bei Verträgen über digitale Produkte. Einführung in das neue Gewährleistungsrecht für die Digitalisierung. *Computer und Recht (CR),* 8/21, S. 530-540.

Säcker, Jürgen, Rixecker, Roland, Oetker, Hartmut und Limperg, Bettina (Hrsg.) (2022): Münchner Kommentar zum BGB, Band 3. 9. Auflage. München: C.H.Beck.

Sattler, Andreas (2017): Personenbezogene Daten als Leistungsgegenstand. *JuristenZeitung (JZ)* 72/21, S. 1036-1046.

Schmidt-Kessel, Martin und Grimm, Anna (2017): Unentgeltlich oder entgeltlich? – Der vertragliche Austausch von digitalen Inhalten gegen personenbezogene Daten. *Zeitschrift für die gesamte Privatrechtswissenschaft (ZfPW)*, 1/17, S. 84-108.

Schmitz, Barbara und Buschuew, Ellen (2022): (Be-)Zahlen mit Daten. Im Spannungsverhältnis zwischen Verbot mit Erlaubnisvorbehalt und Privatautonomie. *Multimedia und Recht (MMR)*, 3/22, S. 171-176.

Schreier, Hans-Georg und Michels, André (2022): Negative Beschaffenheitsvereinbarung im digitalen Vertragsrecht und bei Waren mit digitalen Elementen. Zum praktischen Umgang mit Mängellisten. *Recht Digital (RDi),* 9/22, S. 381-390.

Simitis, Spiros, Hornung, Gerrit und Spiecker gen. Döhmann, Indra (Hrsg.) (2019): *Datenschutzrecht*. 1. Auflage. Baden-Baden: Nomos.

Spindler, Gerald (2021): Umsetzung der Richtlinie über digitale Inhalte in das BGB. Schwerpunkt 1: Anwendungsbereich und Mangelbegriff. *Multimedia und Recht (MMR)*, 6/21, S. 451-457.

Spindler, Gerald (2021): Ausgewählte Rechtsfragen der Umsetzung der digitalen Inhalte-Richtlinie in das BGB. Schwerpunkt 2: Rechtsbehelfe, Beweislastregelungen und Regress zwischen Unternehmern. *Multimedia und Recht (MMR)*, 7/21, S. 528-533.

Stierle, Martin (2021): Der Regierungsentwurf zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen. *IP-Rechtsberater (IPRB)*, 3/21, S. 66-71.

Wolff, Heinrich Amadeus, Brink, Stefan und v. Ungern-Sternberg, Antje (Hrsg.) (2023): *BeckOK Datenschutzrecht*. 46. Aufl. (Stand 01.11.2023). München: C.H.Beck.

4 Der datensouveräne Bürger

„Dann drück ich auf's Mikro, wenn's hier mal um Dinge geht...": Kreative Privatisierung. Der Umgang mit Privatheitsansprüchen in der Smart Speaker-Nutzung

Lukas Schmitz

Zusammenfassung

Der vorliegende Beitrag erörtert den Umgang mit dem Datenkapitalismus im häuslichen Umfeld am Beispiel der Smart Speaker-Nutzung. Menschen nutzen Smart Speaker im Alltag aus Motiven der Erleichterung und produzieren dabei Daten, die von Unternehmen angeeignet werden; dabei bleibt zumeist unklar, wie diese Daten ausgewertet werden und welches Risiko für die Nutzer:innen damit verbunden ist. Mithilfe einer pragmatistischen Theorie des Attachments wird gezeigt, dass Menschen dieses Risiko unter Rückgriff auf Formen des Vertrauens sowie Strategien der Analogisierung bearbeiten. Auf diese Weise wird ein tiefergehendes Verständnis der kreativen Auseinandersetzung von Nutzer:innen mit antizipierten Privatheitsbedrohungen erarbeitet, das ermöglicht, den je spezifischen Umgang nicht als paradox – im Sinne eines Widerspruchs zwischen Sensibilität in Privatheitsfragen und ergriffenen Maßnahmen – , sondern als erfahrungsgeleitete Auseinandersetzung zu beschreiben.

1. Einleitung

Privatheitsfragen gehören zu den drängendsten Herausforderungen in Zeiten der fortschreitenden Digitalisierung jedweder Lebensbereiche. Mit dem steigenden Zugriff privatwirtschaftlicher Akteure auf Datensätze, die Eigenschaften und Verhalten von Nutzer:innen verschiedener Dienstleistungen sammeln und prognostizieren, gewinnen diese Fragen an Brisanz. Sie verlangen nach einer Antwort, die den Ansprüchen eines sich digitalisierenden Gemeinwesens (in staatlicher und wirtschaftlicher Hinsicht) einerseits und einer demokratisch integrierten und selbstbestimmten Bürger:in andererseits Rechnung trägt. Dass die Sammlung von Daten Voraussetzung von Gesellschaft ist und eine Lösung nicht darin bestehen kann, diese *nicht* zu erheben, ist mittlerweile ein Gemeinplatz der Privatheitsforschung gewor-

den. Jedoch ist insbesondere der Umgang mit der Kapitalisierung ebenjener Daten eine besondere Herausforderung – zu unklar ist das Ausmaß der Sammlung sowie die Art der Verwertung, zumal die Möglichkeiten der Bürger:innen, Handlungsmacht in dieser Frage zu gewinnen, beschränkt sind (Lamla 2019). Seien es Unkenntnis über technische Möglichkeiten der Kontrolle der eigenen Daten, der bewusste Verzicht auf Kontrolle zugunsten sozialer Teilhabe oder schlicht Unlust, sich mit den häufig komplizierten Zusammenhängen zu beschäftigen – potenzielle Gefahren des Datenkapitalismus sind offenbar und dennoch scheint im alltäglichen Umgang das stille Einvernehmen, Daten für Bequemlichkeit der Nutzung digitaler Dienstleistungen preiszugeben, etabliert.

Die Diskussion ebendieser Fragen ist währenddessen in verschiedenen Diskursen verortet, sei es in der Medienberichterstattung, der akademischen Sphäre, parlamentarischer Diskussion und Gesetzgebung, Verlautbarungen zivilgesellschaftlicher Akteure oder in den individuellen Reflexionen der Staatsbürger, in denen Auswirkungen der um sich greifenden Datensammlung behandelt werden.

Allerdings hinkt der Diskurs dabei der Wirklichkeit hinterher. Daten werden fortlaufend gesammelt und der Begleitdiskurs erörtert allzu häufig eine Perspektive ex post – als nachträgliche Korrektur von Fehlentwicklungen oder einer verspäteten Einsicht in kritische Potenziale technischer Neuerungen. Ganz unabhängig von bestehenden, möglichen und künftigen Regelungsverfahren, die den Einzelnen vor Übergriffen (gleich welcher Art: sei es in personalisierter Werbung oder im potenziellen Angriff auf Persönlichkeitsrechte) schützen, sehen sich Menschen gegenwärtig der Frage ausgesetzt, wie sie dem Datenkapitalismus im Alltag begegnen. Die Antworten dafür können verschieden ausfallen: Plädieren die einen für eine systemische Lösung, da es schwerfällt, durchgehend Aufmerksamkeit für potenziell bedrohlichen Datenfluss aufzubringen, verorten andere die Kontrollgewalt über den Datenkapitalismus in einem selbstbestimmten Akteur, der – vermeintlich gut informiert und privatheitssensibel – selbst alles Nötige aufbringt, um seine Privatheit (worin auch immer sie besteht) zu schützen.

Dieser Aufsatz erörtert den Umgang von Menschen mit Fragen der Privatheit am Beispiel der Smart Speaker-Nutzung im häuslichen Bereich:[1]

1 Als Smart Speaker werden hier Sprachassistenten wie Amazon Echo, Google Nest oder Apple Home Pod verstanden, also Lautsprecher mit integrierten Mikrophonen, die auf Sprachbefehle hin verschiedene Funktionen ausführen können, so etwa Internet-

Wie begegnen Menschen dem Umstand, dass sie in ihrem häuslichen Bereich potenziell Daten produzieren, die über den Smart Speaker von einer dritten Partei nutzbar gemacht werden können? Nach welchen Kriterien werden in der Smart Speaker-Nutzung Privatheitsansprüche formuliert, wo sind die Grenzen der Umsetzung dieser Privatheitsansprüche und auf welche Art stellen Nutzer:innen ihre persönliche, gefühlte Privatheit wieder her? Insbesondere das Bild des selbstbestimmten, rationalen Akteurs, der eine informierte Entscheidung über seine Privatheit trifft, soll dabei kritisch hinterfragt werden. Es bestehen bereits einige Ansätze dazu, das sogenannte Privacy Paradox (Barnes 2006),[2] also die Beobachtung, dass Personen im Gespräch ihre Privatheit als zentralen Wert adressieren, aber im konkreten Handeln diese Sensibilität missen lassen, zu dekonstruieren (Trepte u. a. 2020; Solove 2021; Agi/Jullien 2018). Daran anknüpfend verfolgt dieser Aufsatz einen Ansatz, der unter Rückgriff auf eine pragmatistische Theorietradition eine Perspektive eröffnet, die das Handeln von Personen nicht als Ergebnis von objektiv gebotenen (und entsprechend subjektiv ausgedeuteten), rationalen Kriterien behandelt, sondern als individuelle Auseinandersetzung und Aushandlung, die vor dem Hintergrund persönlicher Erfahrung vorgenommen wird.

Für die Auseinandersetzung mit diesen Fragestellungen greife ich zurück auf Interviewmaterial aus zehn Besuchen in Haushalten, die mit Smart Speakern ausgestattet sind. Im Ergebnis zeigt sich, dass die Auseinandersetzung mit Privatheitsfragen in der Smart-Speaker-Nutzung als kreative Aushandlung begriffen werden muss, die in spezifischen, scheinbar teils widersprüchlichen oder inkonsistenten, Formen der Privatisierung mündet. Nach einer soziologischen Begriffsbestimmung der Privatheit (2.1) wird ein Überblick über den Forschungsstand zu Smart Speakern und Privatheit bereitgestellt (2.2). Anschließend wird eine pragmatistische Theoriegrundlage erarbeitet (3) sowie das methodische Vorgehen vorgestellt (4); daraus resultieren empirische Ergebnisse zur „Kreativen Privatisierung" (5), die abschließend in einem Fazit zusammengefasst werden (6).

recherche, Koordinierungsleistungen (Terminplanung, Steuerung von IoT-Vernetzungen) oder Unterhaltungsfeatures.

2 Eine frühe Beobachtung dieses Phänomens findet sich auch bei: Acquisti, Grossklags (2005): Privacy and Rationality.

2. Forschungsstand

2.1 Privatheit als soziologischer Begriff

Bevor der Umgang von Personen mit Fragen der Privatheit in Bezug auf Smart Speaker behandelt wird, wird hier zunächst ein soziologischer Begriff der Privatheit erarbeitet. Zu berücksichtigen ist, dass der Diskurs um den Begriff der Privatheit überaus differenziert ist, sodass keine umfassende Zusammenfassung der vielfältigen Ausprägungen gegeben werden kann, die sich auch nach wissenschaftlicher Disziplin massiv unterscheiden.[3] Auch die Ansprüche an einen Privatheitsbegriff differieren je nach disziplinärer Verortung stark: Während in der Informatik etwa der Schwerpunkt häufig auf technischen Möglichkeiten zu Datenkontrolle liegt, ist die Sozialwissenschaft eher an einer theoretischen Bestimmung und insbesondere im Falle der Sozialphilosophie auch der normativen Dimension des Begriffs interessiert.

Häufig beschreiben theoretische Perspektiven auf Privatheit ein spezifisches Verhältnis des Subjekts zu einer übergeordneten Struktur, zumeist einem bestimmten Begriff der Öffentlichkeit. In klassischen soziologischen Ansätzen steht dabei mal das Private, mal das Öffentliche im Fokus, etwa indem das Private als Vorbereitungsraum für öffentliches, politisches Wirken und also als Grundlage für eine funktionierende Demokratie beschrieben wird (Arendt 2002) oder indem ein Idealbild von Öffentlichkeit gezeichnet wird, in dem Privatleute bar jeden Eigeninteresses einen Diskurs um die objektiv bestmögliche Organisation des Staates führen (Habermas 1990).

Mittlerweile besteht jedoch Konsens darin, dass Öffentlichkeit und Privatheit keinen Gegensatz bilden, sondern ein komplementäres Antithesenpaar im Wandel. Laut Armin Nassehi muss etwa die systematische Datensammlung im 19. Jh., nicht allein als Übergreifen staatlicher Gewalt auf private Lebenswelten verstanden werden, sondern Staatlichkeit – und damit auch eine spezifische Arena der Öffentlichkeit – lässt sich vielmehr nur auf Grundlage systematischer Datensammlung herstellen. Die staatliche Datensammlung wiederum bringt auf diese Art eine Blaupause für Normalität in der individuellen Lebensführung hervor. Bürgerliche Vorstellungen von Privatheit sind entsprechend als Ergebnis von Selbsttechniken zu verstehen,

3 Für eine ausführliche Darstellung des soziologischen Privatheitsdiskurses siehe: Lamla u.a. (2022): Privatheit und Digitalität.

die sich als Reaktion auf äußere Erwartung und Datensammlung herausbilden (Nassehi 2019, S. 307f.). Die vermeintlichen Gegensätze Privatheit und Öffentlichkeit bringen sich also wechselseitig hervor und sind nur in dieser Verwobenheit zu denken.

Privatheit zeichnet sich, um diese Verwobenheit weiterhin zu unterstreichen, zudem auch durch bestimmte Praktiken der Offenbarung aus – wenn man etwa an ein geteiltes Geheimnis in einer privaten Beziehung denkt. Anderseits funktioniert Öffentlichkeit nur über spezifische Praktiken der Privatisierung: Höflichkeit als gesellschaftliche Umgangsform, und damit in der Sphäre des Öffentlichen verortet, beispielsweise ist häufig dadurch gekennzeichnet, dass bestimmte Dinge nicht zur Sprache kommen; auch dass man sich an öffentlichen Orten i. d. R. bemüht, seine Umgebung nicht durch lautes Sprechen zu stören, verdeutlicht die enge Verzahnung der Sphären (Roessler/Mokrosinska 2013).

Neuere Ansätze konzentrieren sich daher auch weniger auf das grundsätzliche Verhältnis von Privatheit und Öffentlichkeit als Gegensatzpaar, sondern erarbeiten differenziertere Kartierungen, indem sie etwa den Begriff der Privatheit theoretisch in verschiedenen Dimensionen bestimmen oder sich den Praktiken der Privatisierung – häufig unter den Vorzeichen der Digitalisierung – widmen. Der Begriff der Privatheit spielt verschiedene Rollen und wird in höchst unterschiedlichen Zusammenhängen in Anschlag gebracht. Die aktuelleren Ausarbeitungen versuchen entsprechend, dieser Vielfalt gerecht zu werden, indem sie den Begriff theoretisch dynamisieren.

So entwirft Beate Roessler einen multidimensionalen Zugang zum Privatheitsbegriff, indem sie drei Ausrichtungen des Privaten beschreibt. Sie differenziert zwischen dezisionaler, informationeller sowie lokaler Privatheit: Während dezisionale Privatheit die Freiheit zur selbstbestimmten Entscheidung beschreibt, umfasst informationelle Privatheit die Art und Weise, selbstbezogene Aufschlüsse in sozialen Beziehungen zu moderieren. Lokale Privatheit schließlich zielt auf eine spezifische Räumlichkeit ab, die dem Menschen als Schutzraum die Möglichkeit zur freien Entfaltung bietet (Roessler 2001).

Helen Nissenbaum dagegen versteht Privatheit nicht als Kontrollbegriff ausgehend vom Individuum, sondern, nicht zuletzt vor dem Hintergrund fortschreitender Digitalisierung, als kontextabhängig. So beschreibe Privatheit nicht das Recht, persönliche Informationen zu kontrollieren, sondern jenes „to live in a world in which our expectations about the flow of personal information are, for the most part, met" (Nissenbaum 2010, S. 231).

Eine Privatheitsverletzung liege nicht vor, wenn eine Person keine absolute Kontrollgewalt über diese Informationen hat, sondern wenn die impliziten Normen der jeweiligen Kontexte verletzt werden. Privatheit besteht so verstanden in *Contextual Integrity*.

Auch für Christina Nippert-Eng (2010) ist Privatheit kein holistischer Begriff, sondern Gegenstand der Aushandlung in Praktiken des Teilens oder Verbergens. Absolute Privatheit als solche gebe es nicht, vielmehr versuchten Menschen, sich gewissermaßen situativ private Inseln zu schaffen, in denen sie Kontrollgewalt über zu teilendes oder nicht zu teilendes besitzen.

Den Praktiken des Teilens und Verbergens wenden sich auch Alice Marwick und danah boyd zu. In ihrer Arbeit zum Verhalten von Teenagern in sozialen Medien zeigen sie, dass diese ihre Privatheit auf kreative Weise in Auseinandersetzung mit der Technik herstellen. Insbesondere soziale Netzwerke arbeiten mit einem solch hohen Maß an Sichtbarkeit, dass eine absolute Kontrolle kaum möglich ist. Entsprechend bilden Teenager kreative Weisen des Umgangs heraus, mit denen sie einerseits ihre Privatheit schützen und andererseits nicht auf soziale Teilhabe verzichten müssen; dabei argumentieren Marwick/boyd, dass soziale Medien grundsätzlich die Art und Weise verändern, wie Privatheit verhandelt wird (Marwick/boyd 2014).

Eine umfassende Bestimmung des Begriffs der Privatheit, der in einem spezifischen Verhältnis der Verwobenheit von Privatheit und Öffentlichkeit besteht, bietet Carsten Ochs. Dafür nähert er sich dem Begriff aus zwei Richtungen. Einerseits beschreibe das Private vom Individuum ausgehend gedacht sogenannte Erfahrungsspielräume: Durch bestimmte Praktiken der Beschränkung oder Öffnung dieser Spielräume mache sich das Individuum bestimmte Erfahrungen zugänglich oder schließe diese aus. Andererseits werde über den Begriff der Privatheit auch markiert, in welchem Maße eine Öffentlichkeit im Sinne von dem Individuum distanten Akteuren wie Staaten oder Unternehmen, an diesem teilhaben können: Das Maß, in dem das Individuum diesen Zugriff zulasse, bestimme Privatheit als Teilhabebeschränkung (Ochs 2022).

Der soziologische Privatheitsbegriff kann also verschiedene Ausprägungen haben – gemein ist insbesondere aktuelleren Arbeiten aber der Fokus auf Aushandlungsprozesse sozialer Teilhabe in Auseinandersetzung mit kontextbestimmenden Faktoren. Insbesondere das konkrete Tun, also die situative, kontextgebundene Herstellung von Sicherheit, steht dabei im Vordergrund.

Hintergründe, die Smart Speaker als problematisch in Privatheitsfragen kennzeichnen, liegen freilich in der engen Verzahnung von Fragen der Privatheit mit Prozessen der Digitalisierung. Der Smart Speaker sammelt und speichert Daten – entsprechend gilt er auch als Projektionsfläche für Diskurse um Privatheit in Zeiten fortschreitender Digitalisierung.

Häufig liegt in diesen ein Fokus darauf, wie sich die soziale Welt mit der digitalen Transformation verändert: Insbesondere Datenerfassungs- und -verwertungspraktiken stehen dabei im Vordergrund (Palen/Dourish 2003; Gstrein/Beaulieu 2022). Problematisiert wird dabei der – von Shoshanna Zuboff benannte – *Überwachungskapitalismus*, indem argumentiert wird, dass gegenwärtig einem System Vorschub geleistet werde, das in der Sammlung und Kapitalisierung personenbezogener Daten totalitäre Züge trage (Zuboff 2018). Überhaupt ist die fortschreitende Digitalisierung bereits länger ein kritisches Thema für die Privatheitsforschung. Rief Reg Whitaker bereits 1999 das Ende der Privatheit aus (Whitaker 1999), kam sie als paradoxes Phänomen einige Jahre später doch wieder zu unverhoffter Prominenz: Susan Barnes' bereits oben erwähntes *Privacy Paradox* ist mittlerweile nachgerade ein geflügeltes Wort geworden und beschreibt die Beobachtung, dass Personen sich i. d. R. selbst als privatheitssensibel beschreiben, jedoch in der Interaktion diese scheinbare Sensibilität nicht an den Tag legten (Barnes 2006). Aus soziologischer Perspektive ist mit der Zuschreibung paradoxen Verhaltens unter Verweis auf eine objektive Rationalität jedoch nicht viel gewonnen. Entsprechend nähern sich viele sozialwissenschaftliche Perspektiven dem Begriff der Privatheit aus praxeologischer Perspektive, die akzeptiert, dass Handlungen von Subjekten nicht als intentional vorauszusetzen sind; vielmehr wirken Habitualisierungen und Routinisierungen handlungsleitend und je nach Medium, Sozialisation und Lebensphase entstehen neue Erfordernisse und Praktiken. (Roessler/Mokrosinska 2013; Marwyck/boyd 2014; Steijn/Vedder 2015; Suh/Hargittai 2015).

2.2 Smart Speaker und Privatheit

Bevor in der Folge das theoretische Programm dieses Aufsatzes näher ausgeführt wird und der konkrete Umgang mit antizipierten Privatheitsbedrohungen durch Smart Speaker im häuslichen Umfeld eingegangen wird, stellt der folgende Abschnitt einen Überblick zu bestehender Forschung zu Smart Speakern bereit. Gerade in Bezug auf Privatheitsfragen existiert eine

große Bandbreite an Forschungen, die im Folgenden skizziert wird.
Einige Publikationen widmen sich der Frage, was Menschen zur Nutzung von Smart Speakern bewegt. Dabei sind es insbesondere Motive der Erleichterung, die herausstechen, etwa in Bezug auf die Optimierung alltäglicher Aufgaben wie dem Schreiben von Einkaufslisten, Unterhaltung oder Bequemlichkeit (Rzepka 2019; Malodia 2024). Gleichwohl stellen Privatheitsbedenken ein Hindernis dar: Je ausgeprägter diese sind, desto weniger werden Smart Speaker genutzt (Buteau/Lee 2021).

Dabei herrscht Konsens, dass Nutzer:innen sich des Ausmaßes der Datensammlung nicht bewusst sind (Gautam 2022; Kröger u. a. 2022; Malkin u. a. 2019). Zudem verfügten sie nicht über die technischen Kompetenzen, dies einzuschätzen (Zeng u. a. 2017; Lau u. a. 2018a). Und auch, wenn Sensibilität in Bezug auf Privatheitsfragen vorhanden ist, ist es unwahrscheinlich, dass weitreichende Schutzmaßnahmen getroffen werden – ein Umstand, der in der Forschung als Privacy Pragmatism bzw. Privacy Cynicism beschrieben wird (Hoffmann u. a. 2016; Lutz/Newlands 2021). Was jedoch die Maßnahmen angeht, die Menschen zum Schutz ihrer Privatheit ergreifen, ist die Forschungslage nicht eindeutig: So geben Nutzer:innen auch bei geringer Kenntnis der tatsächlichen Bedrohung vorsorglich etwa bestimmte Informationen nicht an ihren Smart Speaker weiter (Brause 2020). Andererseits herrsche insgesamt wohl eine geringe Motivation, die eigene Privatheit zu schützen – weil Nutzer:innen sich keine Sorgen machen oder sich schlichtweg nicht damit auseinandersetzen. Dabei verfügen sie über elaborierte Begründungsfiguren, warum sich Schutzmaßnahmen nicht lohnen, etwa, weil sie den Wert der preisgegebenen Informationen als gering einschätzen oder argumentieren, dass ihre Informationen ohnehin schon an anderer Stelle erhoben werden (Lau u. a. 2018a). Auch die bewusste Aufgabe von Privatheit, um bestimmte Funktionen nutzen zu können, spielt dabei eine Rolle (Lau u. a. 2018b).

Die folgenden Abschnitte haben zum Ziel, genau diese Perspektiven auf Privatheit systematisch in den Blick zu nehmen: Was bewegt Menschen dazu, in ganz unterschiedlicher Art und Weise mit Privatheitsbedrohungen umzugehen? Im Kontext der Nutzung von Smart Speakern werden, um Beate Rössler erneut aufzugreifen, verschiedene Dimensionen von Privatheit angesprochen und potenziell bedroht; sei es in Bezug auf die räumliche Integrität des häuslichen Umfelds oder in der Entscheidungsgewalt darüber, welche Daten gesammelt und ausgewertet werden. Zu welchen Schritten greifen Nutzer:innen, um diesem Umstand zu begegnen? Dafür

wird zunächst eine theoretische Grundlage bereitgestellt, bevor diese Fragen in der Analyse empirischen Materials beantwortet werden.

3. Eine pragmatistische Theorieperspektive

Nutzer:innen weisen i. d. R. Sensibilität in Bezug auf Privatheit auf, handeln in der konkreten Nutzung das potenzielle Risiko aber in ganz individueller Weise aus. In diesem Abschnitt wird diese Aushandlung unter Rückgriff auf eine pragmatistische Theorietradition als erfahrungsgeleiteter Umgang mit einer neuartigen Technologie beschrieben. Es wird herausgestellt, dass menschliches Handeln nicht in einer Umsetzung von intentional und objektiv-rational geleiteten Motiven besteht, sondern in einer individuellen Auseinandersetzung mit der Umwelt auf Grundlage persönlicher Erfahrungswerte. Mit dem Begriff des Attachments wird verdeutlicht, dass diese Erfahrungen die Person konstituieren und somit den jeweiligen Umgang mit der Umwelt prägen.

Der Pragmatismus setzt sich seit seinen Anfängen im 19. Jahrhundert kritisch mit dem Begriff der ‚objektiven Wahrheit', der bis dahin große Teile der damals zeitgenössischen Philosophie prägte, auseinander. Diese Perspektive scheint daher geeignet, auch einen monolithischen Begriff der Privatheit, wie er im ‚Privacy-Paradox' zum Ausdruck kommt, zu dekonstruieren. Für William James (1842-1910), einen Gründervater des Pragmatismus, bedeutet ebendieser die „Herrschaft der empirischen Stimmung und ehrliches Aufgeben des rationalistischen Temperamentes" (James 1994, S. 22). Nicht mehr an einer objektiven Ratio soll das Handeln von Menschen gemessen werden, sondern durch ein Ernstnehmen der Empirie in einer gleichsam unendlichen Differenzierung aufgehen. Entsprechend schreibt James: „Der Pragmatismus fühlt sich nicht wohl, wenn er weit weg ist von Tatsachen. Der Rationalist fühlt sich nur in der Nähe von Abstraktionen behaglich" (ebd., S.35). Insoweit beschreibt der Pragmatismus zunächst eine Methode, die „aus jedem […] Wort seinen praktischen Kassenwert heraus[zu]bringen" (ebd. S.23) bestrebt ist – um soziale Zusammenhänge zu verstehen, plädiert James für einen „radikalen Empirismus". Nicht in der begrifflichen Abstraktion der Phänomene liege entsprechend der Erkenntnisgewinn, sondern vielmehr in der empirischen Ausdifferenzierung.

Ähnlich skeptisch ist der Pragmatismus in Bezug auf Intentionalität, die menschliches Handeln stets als geplant und zweckgerichtet beschreibt; Hans Joas versteht die pragmatistische Perspektive als „einen Bruch mit

einem teleologisch verengten Verständnis von Intentionalität“ (Joas 1996, S. 366). So seien Handlungsverläufe „auch bei individuellem Handeln nie auf einzelne Intentionen zurückzuführen“ (ebd., S. 228). Vielmehr stelle sich die Wirklichkeit der Person als widerständig dar: Personen begegnen Phänomenen stets vor dem Hintergrund in Routinen geronnener Erfahrung – nur passen diese häufig nicht zu den etablierten Weisen, der Welt zu begegnen. Daher sei es ein stetiges Ausprobieren und Testen, ein „kreative[s] Verarbeiten von Widerfahrnissen“, welches das Handeln charakterisiere (ebd., S.366).

Unter Rückgriff auf einen weiteren Autor in pragmatistischer Tradition, Antoine Hennion, wird deutlich, dass Personen ihre Privatheit in Bezug auf die Smart-Speaker-Nutzung stets vor dem Hintergrund eines spezifischen *Attachments* vornehmen. Das Attachment – als die Erfahrungen, die der jeweiligen Person zu eigen sind und diese entsprechend konstituieren – prägt die Art und Weise, wie Menschen mit der Umwelt interagieren. Handlungen sind daher nicht allein als Ergebnis von Intentionalität zu verstehen, sondern als Ergebnis eines Wechselspiels mit dem jeweiligen Attachment (Hennion 2017, S. 74). Dieses bezieht sich auf eine individuelle Verhaftung in materiellen Konstellationen, persönlichen Beziehungen, Ideen und Diskurse, die performativ aktualisiert werden; auf diese Weise modelliert und reflektiert sich die Person auf eine Weise, die ihre eigene ist. Das Attachment ist gleichsam „die Rechnung, welche die Vergangenheit der Gegenwart präsentiert” (Hennion 2011, S. 94). Personen bilden in ihrer individuellen Gewordenheit einen Nexus aus Erfahrungen, Wissensbeständen und Praktiken, der vorprägt, wie neue Erfahrungen bearbeitet werden. Dieser Nexus symbolisiert gewissermaßen den Werkzeugkoffer (im Sinne von zur Verfügung stehenden Mitteln), mit dem Personen ihre Umwelt bearbeiten; gleichzeitig beschränkt er die Person in ihren Handlungsmöglichkeiten insofern, als die geronnene Erfahrung auch die Grenzen des Zugriffs definiert. Personen wechseln entsprechend zwischen ‘aktiv’ und ‘passiv’: Aktiv in der bewussten Bearbeitung der Umwelt unter Rückgriff auf etablierte Praktiken, passiv im Ausgesetzt-Sein dieser spezifischen Gewordenheit (Hennion/Gomart 1999, S. 243).

Das Attachment beschreibt also eine je individuelle Verhaftung in materiellen Settings, Praktiken und Diskursen, die den Menschen als solchen hervorbringen und die ihm in besonderer Weise gewohnt sind. Soziales Tun besteht in dieser Perspektive aus einem Wechselspiel aus Sich-hervorbringen und Hervorgebracht-werden, das zwischen der Person und ihrer Umwelt besteht. Der Begriff des Attachments erklärt, warum sich die Zu-

gänge, die technischen Kompetenzen und auch die Antizipation von Gefährdungspotential in Bezug auf Privatheit in der Smart-Speaker-Nutzung so unterschiedlich darstellen. Anstatt diese nach Konsistenz zu bewerten, müssen diese vielmehr als Ausdruck eines individuellen Weltzugriffs perspektiviert werden. Für eine verstehende Auseinandersetzung des Umgangs von Personen mit Privatheitsbedrohungen in der Smart Speaker-Nutzung muss also, um dem pragmatistischen Imperativ nachzukommen, zunächst die Komplexität empirischer Vielfalt ernst genommen werden, die sich am deutlichsten in einer materialnahen Analyse zeigt; der Begriff des Attachments hilft dann dabei, diese Komplexität theoretisch einzuordnen.

In Bezug auf die Datensammlung von Smart Speakern lautet die leitende Hypothese, dass der Umgang mit Privatheitsfragen durch Kenntnis potenzieller Risiken und technischer Zusammenhänge grundiert ist, die von Person zu Person differieren. Dies bedeutet zunächst: Wer über kein entsprechendes Attachment verfügt, hat auch kaum eine Vorstellung davon 1) was Daten überhaupt sind 2) wie sie angeeignet werden können und von wem das auf welche Weise technisch bewerkstelligt wird sowie 3) was mit den Daten anschließend passiert, etwa wie und zu welchem Zweck sie ausgewertet werden. Privatheit als relevantes Thema wird in den Interviews durchaus reflektiert adressiert – der jeweilige Umgang macht jedoch deutlich, dass die Bearbeitung der Thematik stets vor einem spezifischen Attachment vorgenommen wird. Wie also handeln Personen in Bezug auf Smart Speaker, und worin besteht die Kreativität der Auseinandersetzung? Was sind die Attachments, gleichsam die Blaupausen der Erfahrung, die mit dem neuen technischen Artefakt in Einklang gebracht werden müssen, wo die Bruchlinien? Im folgenden Abschnitt wird zunächst der methodische Zugang dargestellt, bevor anschließend verschiedene Dimensionen (im pragmatistischen Sinne:) kreativer Privatisierung als Ausdruck des personenspezifischen Attachments erarbeitet werden.

4. Methodischer Zugang

Der Datenkorpus, der die Grundlage der folgenden Auswertung bildet, umfasst Material aus ethnografischen Besuchen in zehn Haushalten. Die Datenerhebung fand also im häuslichen Umfeld der Studienteilnehmer:innen statt. Für die Rekrutierung der Studienteilnehmer:innen wurde zunächst eine Zeitungsannonce geschaltet; anschließend wurde das Sample nach einem Schneeballsystem ergänzt, um eine höhere Heterogenität zu

erreichen. Hatten sich auf die Annonce zunächst überzeugte Nutzer:innen von Smart Speakern gemeldet, wurde in der Folge insbesondere darauf geachtet, auch kritischere Stimmen einzufangen, etwa von Personen, die den Smart Speaker kaum benutzen oder wieder abgeschafft hatten. Die Haushalte befanden sich im städtischen wie im ländlichen Bereich und waren unterschiedlich mit smarter Technik ausgestattet; es wurden häusliche Umgebungen sogenannter ‚early adopter' ebenso erhoben wie Haushalte, die lediglich über einen einzigen Smart Speaker verfügten – in einem Falle wurde der Smart Speaker sogar ‚aus Versehen' angeschafft, nämlich in eine Lautsprecherbox integriert. Die Gesprächspartner:innen lebten entweder alleine oder in Partnerschaft. In letzterem Fall wurde entweder mit beiden Partner:innen gesprochen oder mit einer Person, wobei darauf geachtet wurde, nicht nur mit jenen Interviews zu führen, welche die Anschaffung der Smart Speaker ursprünglich initiiert hatten. Das Alter der befragten Personen variierte ebenso wie der Bildungsgrad (im Studium; abgeschlossene Ausbildung; Hochschulabschluss). Bis auf eine Ausnahme lebten in den erhobenen Haushalten keine Kinder.

In der Erhebungssituation wurde zunächst eine Techniksichtung vorgenommen, in der sämtliche smarten Geräte, insbesondere Smart Speaker, in Augenschein genommen wurden: Wo stehen diese und wie fügen sie sich in das häusliche Arrangement ein? Wie sind sie miteinander vernetzt und wie werden sie gesteuert? Wofür werden sie benutzt? Im Fokus standen dabei insbesondere die individuellen Motive der Nutzer:innen für die jeweilige Smart Speaker-Nutzung (Hine 2019). Für eine umfassende Rekonstruktion der Forschungsumgebung wurde der gesamte Besuch mit einem Sprachrekorder aufgenommen sowie Feldnotizen für ergänzende Beobachtungen angelegt; außerdem wurde das Gezeigte über Fotomaterial dokumentiert. Anschließend wurde mit den Studienteilnehmern ethnografische Interviews geführt, in denen diese die Smart-Speaker-Nutzung ausführlich reflektierten (Spradley 2016). Der Hausbesuch wurde schließlich in einem Protokoll festgehalten, um den Charakter der Forschungssituation zu konservieren.

In der Auswertung nach den Maßgaben der Grounded Theory wurde das Interviewmaterial transkribiert und anschließend mitsamt der Feldnotizen offen kodiert; im Analyseprozess wurden dabei stetig Memos angelegt. So ergaben sich sukzessive übergeordnete Muster aus dem Material, die anschließend theoretisch perspektiviert wurden (Pentzold u. a. 2018).

5. Kreative Privatisierung

In den Interviews wurde durchgehend das Bewusstsein artikuliert, dass Smart Speaker Daten sammeln. Gleichwohl bestanden graduelle Unterschiede abhängig von der technischen Kompetenz der Gesprächspartner:innen. Es war bekannt, dass Smart Speaker, um reagieren zu können, Sprachdaten verarbeiten und zu diesem Zwecke diese zumindest temporär speichern müssen. Ebenso wurde reflektiert, dass Unternehmen auf diese Daten zurückgreifen, um ihr jeweiliges Angebot zu verbessern, etwa in Bezug auf personalisierte Werbeanzeigen auf Grundlage der jeweiligen Nutzung – dass, abgesehen von den Herstellern wie Google oder Amazon, je nach Anwendung, eine ganze Reihe an Unternehmen auf die erhobenen Daten zugreifen, kam allerdings nicht zur Sprache. Welche Daten dabei konkret gesammelt werden, wie diese ausgewertet werden und welche Konsequenzen das potenziell haben kann, blieb für die Nutzer:innen unklar. Den Umgang von Personen mit diesen Unwägbarkeiten in Bezug auf Privatheit in der Smart-Speaker-Nutzung bezeichne ich im Anschluss an Hans Joas als „kreative Privatisierung". Kreativ meint – wie oben – ein je individuelles Vernetzen von Erfahrungsbeständen, Kompetenzen, Routinen und Bewertungen, das vor dem Hintergrund des jeweiligen Attachments vorgenommen wird.

Im Folgenden werden zwei verschiedene Arten des in diesem Sinne kreativen Umgangs mit dem diffusen Gefühl potenziell bedrohter Privatheit vorgestellt:

- Vertrauen: Aufgrund der Komplexität technischer Zusammenhänge, der Unmöglichkeit, das konkrete Vorgehen der datenerhebenden Unternehmen zu eruieren und der Schwierigkeit, das in der Zukunft liegende Risiko einzuschätzen, rekurrieren Befragte auf eine Praxis des Vertrauens im Sinne einer Schließung kontingenter Zusammenhänge.
- Analogisierung: Die Unsicherheit in Bezug auf das Maß der Privatheitsbedrohung führt zu einem Rückgriff auf Strategien der Analogisierung, die Sicherheit versprechen, indem sie einen scheinbar vordigitalen Zustand herbeiführen.

5.1 Blindes Vertrauen?

Für Niklas Luhmann ist Vertrauen ein Schließungsmechanismus für kontingente Zusammenhänge – die Welt habe sich „zu unkontrollierbarer

Komplexität auseinandergezogen" (Luhmann 2000, S. 27) und die Entscheidung, zu vertrauen, mache ein Handeln im „hier und jetzt" möglich (ebd., S. 28). Außerdem gehe „Vertrauen stufenlos in Kontinuitätserwartungen über" (ebd., S. 29). Damit ist gemeint, dass in der Entscheidung, zu vertrauen, zugleich die Erwartung angelegt ist, dass sich die Dinge nicht unvorhergesehen entwickeln – der schlimmste anzunehmende Fall ist nicht maßgeblich für diese Entscheidung. Damit erschließe Vertrauen „Handlungsmöglichkeiten, die ohne [es] unwahrscheinlich und unattraktiv geblieben, also nicht zum Zuge gekommen wären" (ebd., S. 30). Insofern mische sich im Terminus des Vertrauens „Wissen und Nicht-Wissen" (ebd., S.31). Dies bezieht sich auf Situationen, in denen Unsicherheit herrscht und etwas auf dem Spiel steht; die Art des Vertrauens beschreibt den spezifischen Umgang mit diesen. Insofern ist Vertrauen als „Lösung für spezifische Risikoprobleme" zu verstehen (Luhmann 2001, S. 144).

Den Studienteilnehmer:innen ist bewusst, dass sie häufig zum einen nicht über die nötigen Informationen oder Fertigkeiten verfügen, die sie bräuchten, um potenzielle Gefährdungen für sie abzuschätzen, und zum anderen die Motivation derer, die Daten sammeln, nicht grundsätzlich bewerten können, ohne eine komplizierte systemkritische Perspektive einzunehmen. Sie fangen entsprechend an, auf verschiedene Weise zu vertrauen. Anhand empirischer Beispiele zeige ich im Folgenden, in welcher Form dieses Vertrauen vor dem Hintergrund spezifischer Attachments an Gestalt gewinnt und sich etwa als Vertrauen in 1) Bezug auf Staatlichkeit, 2) die beteiligten Unternehmen, oder 3) als ‚Trade-Off' zeigt.

Zunächst berichte ich dafür aus einem Videointerview mit einer Personalerin, wohnhaft im ländlichen Bereich Sachsens. Sie wohnt mit ihrem Partner in einem Neubau, der von Grund auf ‚smart' gestaltet ist. Entsprechend besitzen sie auch mehrere Smart Speaker in verschiedenen Ausführungen. Im Gespräch über potenzielle Bedrohungen von Privatheit durch Alexa, schildert sie mir, wieso sie sich dahingehend eigentlich keine Sorgen mache:

> „Da ist man ja in Deutschland, glaub ich, gut aufgehoben (lacht) was das Thema angeht, aber ich glaube, da macht man sich, wenn man [woanders] wohnen würde, anders Gedanken drüber, ja, durchaus, aber ich glaub, in Deutschland muss man sich da keine Gedanken machen und deswegen hab' ich mir da ehrlich gesagt auch noch nicht so viele Gedanken drüber gemacht, dass das da irgendwelche persönlichen Nachteile haben könnte…" (Ausschnitt Transkript 4)

Die angerufene Instanz, der Vertrauen geschenkt wird, ist hier also der deutsche Staat. Zunächst wird darauf verwiesen, dass Deutschland in Privatheitsfragen im internationalen Vergleich eine Sonderstellung habe. Dies könnte sich auf spezifische gesetzliche Regelungen beziehen oder ganz allgemein auf den rechtstaatlichen Charakter; vermutlich ist (so ließe das Lachen schließen) aber auch insgesamt eine gewisse Regelungswut, die als ‚typisch deutsch' markiert wird, angesprochen. Anschließend verweist sie darauf, dass sie sich damit grundsätzlich nicht viel beschäftigt habe. Hier kommt ein spezifisches Attachment zum Ausdruck, das in der Gewohnheit besteht, innerhalb eines gesetzlich verfassten Rahmens bislang keine Willkür erfahren zu haben. Dies bildet den Erfahrungshintergrund der Person, von dem aus sie die Entscheidung, zu vertrauen, reflektiert. Hier kommt idealtypisch zum Ausdruck, was Luhmann mit Kontinuitätserwartung des Vertrauens beschrieben hat – da sich diese Einstellung bisher bewährt habe, bestehe keine Notwendigkeit für eine kritischere Reflexion.

Im nächsten Beispiel ist nicht die Staatlichkeit Adressat des Vertrauens, sondern die Unternehmen, die Smart Speaker im Portfolio haben. Ich unterhalte mich mit einem jungen Familienvater, der als Ingenieur eine gewisse technische Grundaffinität aufweist. In Privatheitsfragen macht er sich ebenso keine Gedanken und begründet dies so:

> „Jaaa, ein gewisses Vertrauen muss man sowieso in die Hersteller haben, weil, natürlich ist da Missbrauch, na was heißt Tür und Tor geöffnet, die Frage ist, was können die denn damit anfangen? Das müsste ja dann irgendein Hacker sein, der einen dann damit erpresst oder so. [....] Das ist halt das Risiko, das wir eingehen, aber ich hab jetzt nicht irgendwie Bedenken, dass also Google oder Amazon oder Apple jetzt irgendwie die Daten gegen einen verwenden. Also, die werden sicher Target-Werbung machen oder so, ok. [...] Es ist mir bewusst, ja, es ist halt Aufwand und Nutzen. Oder: Nutzen und Gegenwert. Sozusagen." (Ausschnitt Transkript 8)

Hier wird direkt ein Vertrauen in die Hersteller angesprochen: Zunächst wird ein kritisches Bewusstsein markiert: Die Tatsache, dass Daten gesammelt werden, sei grundsätzlich problematisch. Sogleich wird aber differenziert: Im Grunde bestehe nur ein Problem, wenn Dritte auf die Daten zugreifen könnten, von den Unternehmen an sich gehe keine Gefahr aus (freilich ließe sich einwenden, dass auch Unternehmen als Dritte gelten müssten, ein Umstand, der vom Gesprächspartner aber nicht angeführt wird). Dahingehend präzisiert der Studienteilnehmer an anderer Stelle im

Interview, dass die Unternehmen ja in staatliche Regelungszusammenhänge eingebunden seien und insofern bei Zuwiderhandlung verklagt würden – über Umwege ist also auch hier die Staatlichkeit Adressat des Vertrauens. Dass Unternehmen die Daten allerdings kapitalisieren, wird nicht kritisch gesehen, sondern vielmehr als ‚Trade-Off' markiert. Gleichwohl wird in der kurzen Passage deutlich, dass das ‚Risiko' nicht vollends überschaut werden kann; dennoch werden Begründungsfiguren in Anschlag gebracht, die als Ausdruck eines spezifischen Attachments gelesen werden können: Die Verbindung von Problembewusstsein, technischer Argumentation und Zustimmung zum Geschäftsmodell als individueller Perspektive meines Gesprächspartners kennzeichnen diese konkrete Form des Vertrauens.

Das Motiv des ‚Trade-Offs', das bereits im vorangegangenen Beispiel zutage trat, findet sich differenzierter im nächsten Interviewausschnitt. Im Gespräch mit einer jungen Akademikerin kommen wir ebenso auf Privatheitsfragen zu sprechen und sie äußert eine dezidierte Meinung:

> „Es ist ja eigentlich scheißegal, ob du jetzt Alexa hast oder nicht, deine Daten werden so oder so abgezogen, es sei denn wahrscheinlich, du hast noch ein altes Nokia und keinerlei Social Media Account, aber auch dann nimmst du dich ja quasi aus dem gesellschaftlichen Leben raus. Grad in [meinem] Alter jetzt, das ist halt…ja, im Endeffekt kann man zwar immer sagen, wir haben eine freie Wahl, aber im Endeffekt, wenn du auch partizipieren willst, hast du keine ganz freie Wahl, würde ich sagen, ist es nicht. Weil du…im Endeffekt hast du einfach nur die Entscheidung zwischen: Ich gebe vielleicht auch nur einen Teil meiner Daten ab oder ich exkludier mich halt sozial total. Das hat jetzt nichts mit Alexa zu tun, weil Alexa braucht man nicht, um sozial teilhaben zu müssen, aber ich glaub, dass da die Hemmschwelle auch einfach ist, ja, jetzt hast du deine Daten…also wie gesagt es haben schon zwei Großkonzerne meine Daten, tut dann wirklich weh, wenn die ein dritter auch noch hat?" (Ausschnitt Transkript 7)

In diesem Exzerpt wird eine Fülle an Begründungen in Anschlag gebracht, die alle in ein Motiv sozialen Anschlusses münden; die Befragte abstrahiert vom Thema Smart Speaker und macht generell zum Thema, dass der Verzicht auf Teilhabe an (technischer) Innovation in die soziale Isolation führe. Sie habe dahingehend nicht einmal „freie Wahl" – sie tauscht also imaginär das Risiko potenziellen Datenmissbrauchs gegen die Möglichkeit, an Gesellschaft teilzunehmen. Diese Risikobereitschaft charakterisiert die Haltung der Gesprächspartner:in als Vertrauen in Abgrenzung zu reiner

Zuversicht. Die komplexe Struktur der Gegenwart, in der die Differenzierung sozialer Sphären durch die übergreifende Datensammlung gleichsam technisch aufgehoben wird, führt weiterhin zu der Argumentation, dass ein selektives kritisches Bewusstsein ohnehin nicht zielführend sei. Entsprechend führt sie an, dass ihre Daten ohnehin in der Welt seien und sich also in dieser Sache eine Sensibilität in Privatheitsfragen schlicht nicht lohne. Hier kommt das Attachment in doppelter Hinsicht zum Tragen: Einerseits bildet die – auch generationstypische – selbstverständliche Einbindung in gesellschaftlichen Fortschritt (Smartphone, Social Media) den Hintergrund der Entscheidung, an einen lohnenden Trade-Off als Grundlage des Vertrauens zu glauben. Andererseits ist auch hier, wie bereits oben ausgeführt, die Kontinuitätserwartung Teil der Erwägung – man sei das Risiko ja in der Vergangenheit bereits eingegangen, da könne ein weiteres Mal ja nicht schaden. Das Vertrauen als Schließungsmechanismus wird dabei argumentativ von einer fatalistischen Perspektive grundiert, die man durchaus als zynisch verstehen kann (Hoffmann u. a. 2016; Lutz/Newman 2021). Während sich in den vorangegangenen Beispielen das Vertrauen also auf konkrete Akteure, nämlich den Staat oder Unternehmen bezieht, wird hier darin vertraut, dass sich der Trade-off auszahlt: Einerseits durch soziale Teilhabe, die durch die freiwillige Abgabe von Daten durch Nutzung spezieller Technologien ermöglicht werde, anderseits, indem sich potenzielle Bedrohungen schlichtweg nicht realisieren.

Vertrauen darauf, dass die Smart Speaker-Nutzung über den Abfluss von Daten nicht zum eigenen Nachteil wird, ist ein zentrales Motiv in der Antwort auf die Frage, wie Menschen mit der potenziellen Bedrohung ihrer Privatheit umgehen. Dabei hat dieser Abschnitt verdeutlicht, welch unterschiedliche Gestalt dieses Vertrauen vor dem Hintergrund verschiedener Attachments annehmen kann. Diesem Vertrauen gehen, wie von Luhmann ausgeführt, verschiedene Reflexionen voran, die dem jeweiligen Vertrauen ihren individuellen Charakter verleihen und sind gewissermaßen als Rückversicherungen zu verstehen, die dem jeweiligen Umgang mit Privatheitsbedrohungen durch Smart Speaker begleiten. Welche Reflexionen vorgenommen werden, ist dabei von Person zu Person verschieden und gründet in der jeweiligen Verhaftung in Gewohnheiten, Diskursen und Überzeugungen. Die Reflexionen sind dabei durchaus widersprüchlich strukturiert und nur bedingt geeignet, das Vertrauen angemessen zu begründen, etwa wenn in Zeiten globaler Informationsflüsse die Hoffnung auf den Staat als Kontrollgewalt angeführt wird. Die angeführten Begründungen für das Vertrauen spiegeln entsprechend eher die individuelle dis-

kursive Verhaftung der Person wider als eine objektiv-rationale Abwägung. Insofern ist Vertrauen aus pragmatistischer Perspektive als Teil einer individuellen Praxis im Sinne einer erfahrungsgeleiteten Auseinandersetzung zu verstehen, die in ganz verschiedenen und meist widersprüchlichen – weil eben das persönliche Attachment und nicht eine objektiv-rationale Auseinandersetzung widerspiegelnden – Begründungsfiguren mündet.

5.2 Analogisierung

Ebenso wie das Vertrauen eine Möglichkeit darstellt, Unsicherheit und Nicht-Wissen bearbeiten zu können und Handlungsfähigkeit zu ermöglichen, gilt dies auch für die im Folgenden beschriebenen Strategien der Analogisierung. Helen Nissenbaum hat bereits herausgearbeitet, dass Privatheit keinen statischen Wert darstellt, sondern je nach Kontext eigene Erfordernisse des Abschlusses oder der Öffnung nötig sind (Nissenbaum 2010). Ebenso ist auch das Zuhause als Privatraum nicht durchgehend gleich strukturiert. Vielmehr können auch innerhalb eines Haushaltes verschiedene Kontexte nebeneinander existieren, die unterschiedlichen Umgang mit potenziellen Privatheitsbedrohungen nötig machen. Um dem Umstand zu begegnen, dass Smart Speaker potenziell auch ungewollt sowie trotz etwaiger Einstellungen Daten aufzeichnen, berichten Befragte, dass sie in besonderen Fällen einen räumlichen Kontext zu schaffen bestrebt sind, der ihnen sicher erscheint. Entsprechend berichten zahlreiche Gesprächspartner:innen umgekehrt, dass sie ungern einen Smart Speaker im Bade- oder Schlafzimmer aufstellen. So berichtet meine Gesprächspartnerin:

> „Naja, die zeichnet ja auch auf, die speichert, was machst du in deinem Schlafzimmer? Wie gesagt, ich hab da tatsächlich auch öfter nachgedacht, ich hab das dann alles ausgestellt, die speichert ja nichts, aber da ist auch wieder die Frage, wie sehr glaubst du dem…aber dann ist auch wieder die Frage, gut, was hörst du da? [Im Zweifel] schieb ich's einfach auf meine Schwester (lacht) die klingt genauso wie ich (lacht) […] es ist ja auch noch was anderes, wenn's deine Küche ist oder dein Schlafzimmer. Das ist ja doch nochmal vielleicht ne andere Ebene." (Ausschnitt Transkript 7)

Auch hier wird also darauf verwiesen, dass das Zuhause in Bezug auf die Anforderungen an Privatheit unterschiedlich kartiert ist. In diesem Fall hat

sich die Person für eine Alexa im Schlafzimmer entschieden, aber offenbar ausführlich reflektiert, wie sie im Falle eines Datenmissbrauchs reagieren würde, wenngleich sie die Aussage in einen Scherz kleidet; es bleibt dennoch zu bezweifeln, dass eine akustische Ähnlichkeit der Stimmen zu einer tatsächlichen ‚Obfuscation'[4] führt, also der Unmöglichkeit einer Personalisierung durch Verschleierung. Welche konkreten Folgen ein Abhören des Schlafzimmers haben könnte, wird nicht ausgeführt, jedoch scheint hier Scham eine Rolle zu spielen. Diese Scham speist sich aus Erfahrungen im Analogen – der Smart Speaker wird gewissermaßen vermenschlicht, indem er behandelt wird wie ein potenzieller Stalker. Dies sagt wenig aus über die tatsächliche potenzielle Verwendung von Sprachdaten, verdeutlicht aber, dass das Analoge als Blaupause der Erfahrung die Referenz für die Einschätzung von Privatheitsbedrohungen bildet.

Analogisierung ist ein häufig gewähltes Mittel für die Bearbeitung von potenziellen Privatheitsbedrohungen. Die Grundlage dafür kann freilich stark differieren. So berichtet mir im nächsten Interviewausschnitt ein Gesprächspartner, dass er gelegentlich Themen bespreche, die sich am Rande der Legalität bewegten:

> „Aber…nee, z. B. Kontonummern et cetera, ne? Sowas ist dort nicht hinterlegt und sowas kriegen die dort auch nicht raus, und sowas nenn ich auch nicht, indem ich sage, Alexa hier ist meine Kontonummer, ne? […] In diesem Raum ist das völlig ok, da kann man frei sprechen. Wenn, dann drück ich auf's Mikro, wenn's hier mal um Dinge geht, die…das mach ich auch." (Ausschnitt Transkript 5)

Zunächst definiert mein Gesprächspartner Informationen, die er nicht teilen würde; dies betrifft – wenig überraschend – Finanzdaten. Dabei ist aufschlussreich, dass er es laut Aussage vermeidet, seine Kontonummer in der Nähe der Smart Speaker laut auszusprechen; er behandelt den Smart Speaker entsprechend wie eine dritte Partei und sensible Daten in seinem Wohnraum wie ein Geheimnis. Zwar ist nicht klar, ob die Informationen zum eigenen Nachteil eingesetzt werden können, aber die bewährte Praxis

4 Der Begriff der *Obfuscation* bezeichnet eine Verschleierungstaktik, die sich die Eigenheiten digitaler Technik zu eigen macht. In ihrem gleichnamigen Buch geben die Autor:innen Nutzer:innen eine Handreichung, ihre digitalen Spuren durch bestimmte Praktiken vor Missbrauch zu schützen (Nissenbaum/Brunton 2016). Die Verschleierung der eigenen Informationen als spezifischen Umgang mit Fragen der informationellen Selbstbestimmung als Subjektivierungsangebot des 21. Jahrhunderts beschreibt Carsten Ochs als *blurry self* (Ochs 2022, S. 435f.).

des Verheimlichens wird nichtsdestotrotz angewandt. Anschließend kommt er auf Situationen zu sprechen, in denen er den Smart Speaker ausschalten würde: „[W]enn's hier mal um Dinge geht" bezieht sich auf, so wird an anderer Stelle deutlich, Gespräche über Drogenkonsum. Hier öffnet sich also ein Graben, der mit Vertrauen nicht überbrückt werden kann und der eine Handlung nötig macht, die dieses Unsicherheitsgefühl bearbeitet. Dabei bleibt unklar, ob den Mikrofonschalter zu drücken geeignet ist, die räumliche Integrität wiederherzustellen. Ein anderer Gesprächspartner bemerkt auf meine Frage hin, ob er ab und an das Mikrofon stumm schalte, entsprechend: „Wenn ich [mit dem Abhören in bestimmten Situationen] ein Problem hätte, dann würde ich wahrscheinlich eher den WLAN-Stecker, also den Rooterstecker ziehen." (Ausschnitt Transkript 7). Hier zeigt sich also eine weitergehende Praxis der Analogisierung. Man könnte konstatieren, dass im ersten Fall ein Vertrauen in das Versprechen der Anbieter, die Aufzeichnung über die Mikrofontaste kontrollieren zu können, besteht, das im zweiten Fall als Teil des Risikos minimiert werden soll. Dennoch ist das Ziel, nämlich das Herstellen eines analogen Zustandes identisch; die Wahl der Mittel differiert mit unterschiedlichem Attachment, das sich hier in einer spezifischen Risikoabwägung äußert.

Abschließend berichte ich von einem Gesprächspartner, der ebenfalls in einer ländlichen Region beheimatet ist. Er ist Pendler und daher unter der Woche viel unterwegs; in Bezug auf Smart Speaker ist er äußerst bewandert und programmiert sogar eigene ‚Skills', also Anwendungen für den Smart Speaker; so beispielsweise auch ein elektronisches Türschloss, das sich auf einen Sprachbefehl hin öffnet. Gefragt, ob das für ihn nicht ein Risiko darstelle, kontert er mit dieser launigen Erklärung:

> „Ich wohn hier [...] im Dorf, und es sind so viele alte Leute hier bei mir rundrum – wir sind, glaube ich, mit die Jüngsten – die sind den ganzen Tag daheim. Also, ich brauch eigentlich auch gar keine Alarmanlage. Weil, wenn ich Besuch bekomme, dann wissen die das auf jeden Fall, und wenn meine Partnerin nicht da ist, dann weiß auf jeden Fall meine Partnerin spätestens einen halben Tag später, dass hier Besuch da war. Und so ist's auch andersrum. Wenn für sie Besuch da ist, und ich bin nicht da, und ich komm das Wochenende heim, dann hab' ich garantiert einen halben Tag später die Information, wer hier in der Woche alles ein- und ausgegangen ist. Das funktioniert ganz gut bei uns (lacht)." (Ausschnitt Transkript 1)

Auf ein potenzielles Risiko durch die Programmierung des Türschlosses über den Smart Speaker wird hier gar nicht dezidiert eingegangen. Vielmehr wird mit der Eigenheit des Sozialraumes eines kleinen Dorfes argumentiert: Die nachgerade panoptischen Zustände machen einen Missbrauch der Technologie unwahrscheinlich. Es wird auf einen Raum verwiesen, der übersichtlich und vorhersehbar strukturiert ist. Daher ist auch nachrangig, ob diese Beschreibung tatsächlich den Hintergrund für die Risikoeinschätzung bildet. Vielmehr ist der Verweis auf analoge Prinzipien, die das Sozialleben in diesem Dorf kennzeichnen, zentral. Die Potenzialität eines Missbrauchs der Smart Speaker-Technologie wird verhandelt, aber entkräftet durch den Verweis auf etablierte analoge Praktiken der Beobachtung und mündlichen Kommunikation. Bemerkenswerterweise wird hier, in humoristischer Weise und provokanter Zuspitzung, die Bereitschaft angezeigt, sich überwachen zu lassen. Wenn sie der eigenen Sicherheit zuträglich ist, sei eine – hier beinahe fürsorgliche – Überwachung durchaus wünschenswert.

Das Analoge bildet also einerseits den Ausgangspunkt der Einschätzung der Privatheitsbedrohung durch den Smart Speaker wie den Fluchtpunkt der Versicherung. Im Analogen haben Menschen gelernt, Privatheitsbedrohungen zu moderieren; durchgehend muss in verschiedenen Kontexten und sozialen Konstellationen das Verhältnis von Offenbarung und Verheimlichung austariert werden. Im Kontakt mit dem Smart Speaker löst sich diese Gewissheit auf, weil die Kriterien der Einschätzung verschwimmen; es bedeutet einen immensen Aufwand, eine gewissenhafte Prüfung der tatsächlichen Bedrohung vorzunehmen, und zugleich verbleibt vieles im Unklaren und kann nicht abschließend eingeschätzt werden.[5] Es zeigt sich außerdem in diesem Zusammenhang, dass Dimensionen der Privatheit , wie von Beate Rössler erarbeitet (lokal, informationell, dezisional) zwar theoretisch unterscheidbar, allerdings empirisch miteineinander verzahnt sind – die Entscheidung über den Informationsfluss etwa ist stets

5 So macht beispielsweise das BSI (Bundesamt für Sicherheit in der Informationstechnik) acht Empfehlungen, um die eigene Privatsphäre vor potenziellen Übergriffen via Smart Speaker zu schützen: 1. Separates WLAN einrichten; 2. Smart Speaker mit Bedacht platzieren; 3. Personalisierte Sprachprofile; 4. Passwortsicherung; 5. Datenschutzeinstellungen anpassen; 6. Gespeicherte Daten kontrollieren; 7. Nur vertrauenswürdige (sic!) Erweiterungen installieren; 8. Smart Speaker abschalten, vgl.: https://social.bund.de/@bsi/112002894812746815 (zuletzt aufgerufen am 28.2.2024). Diese Maßnahmen benötigen einigen Aufwand oder Technikkompetenz; bemerkenswerterweise werden auch hier Techniken der Analogisierung empfohlen (Nr. 2 und 8).

lokal gebunden und macht eine Umsetzung in einem konkreten materiellen Arrangement nötig.

Das Analoge, als primäre Referenz persönlicher Erfahrung – kondensiert im Attachment – bildet den Hintergrund der Einschätzung unüberschaubarer Zusammenhänge. Zugleich ist die Überführung in das Analoge, etwa durch das Ziehen des Steckers, eine Strategie, einen kontrollierbaren Raum zu schaffen, und mithin das Mittel, Sicherheit zu schaffen in Situationen, in denen Vertrauen keine Option ist. Dabei wirkt die Analogisierung auf eine denkwürdige Weise unzeitgemäß und spiegelt gewissermaßen eine Überforderung angesichts der rasanten digitalen Transformation. Kreativ sind diese Formen der Privatisierung in pragmatistischem Sinne allemal, als sie eine individuelle und erfahrungsgeleitete Auseinandersetzung beschreiben; dem Anspruch, tatsächlichen Privatheitsbedrohungen angemessen zu begegnen, werden sie dabei jedoch nicht gerecht. Das Attachment als Theorieangebot ist geeignet, zu erklären, wieso Personen auf diese Strategien zurückgreifen – in der Empirie tritt die Verhaftung der Gesprächspartner:innen in analogen Zusammenhängen deutlich zu Tage und bildet den Hintergrund der jeweiligen Formen der Privatisierung. Dies verweist jedoch zugleich auf eine übergeordnete Problematik: Die Komplexität der datenökonomischen Infrastrukturen im Kontext der digitalen Transformation führt zu einer Hilflosigkeit, die entweder nur durch Vertrauen – begleitet von spezifischen Rationalisierungen und gelegentlich garniert mit Fatalismus und Zynismus – oder durch gleichsam antiquierte Strategien der Analogisierung, die höchstens situativ Sicherheit verschaffen, aufgelöst werden kann.

6. Fazit

Dieser Beitrag hat gezeigt, dass Menschen potenzielle Privatheitsbedrohungen durch Smart Speaker vor dem Hintergrund eines spezifischen Attachments vornehmen. Wie Menschen sich dieser Bedrohungen bewusst sind, wie sie ein potenzielles Risiko bewerten und welche Schritte sie zur Wahrung ihrer Privatheit unternehmen, ist dabei von Person zu Person verschieden und als erfahrungsgeleitete Auseinandersetzung zu verstehen. Das Attachment prägt dabei einen bestimmten Umgang mit Privatheitheitsansprüchen vor; das betrifft Routinen der Selbstinformation zur Bearbeitung von Unsicherheit oder die Verarbeitung von potenziellem Risiko ebenso wie konkrete Schritte der Privatisierung. Menschen behandeln Fragen der

Privatheit in der Smart Speaker-Nutzung mit den Mitteln, die sie für geeignet halten und die ihnen als Bearbeitungsmodi vertraut sind. Dabei wurde gezeigt, dass diese Bearbeitungen in bestimmten Formen des Vertrauens sowie der Analogisierung münden; diese weisen insofern Ähnlichkeit auf, indem sie in unterschiedlicher Intensität Risiko bearbeiten. Freilich sind sie i. d. R. nicht geeignet, ein Risiko tatsächlich aufzulösen: Ob Vertrauen sich gelohnt hat, ist allein im Nachhinein zu beurteilen, und auch, ob Analogisierung zum Schutz der Privatheit geeignet ist, bleibt zumindest fraglich. Dass Menschen trotz ausgestellter Sensibilität keine umfassenden Maßnahmen zum Schutz ihrer Privatheit ergreifen oder diese sich nicht eignen, das Risiko auszuschließen, ist, soviel ist deutlich geworden, zwar als widersprüchliches, allerdings nicht zielführend als paradoxes Verhalten zu bezeichnen. Die jeweilige Form des Vertrauens oder der Analogisierung und die entsprechende argumentative Manifestation gründet vielmehr in einem spezifischen Attachment, das Ausdruck der jeweiligen Erfahrungsbestände der Person ist.

Eine pragmatistische Perspektive legt nahe, dass sich mögliche Inkonsistenzen nicht zuletzt aus der fehlenden Widerständigkeit des digitalisierten Umfelds ergeben – abgesehen etwa von personalisierter Werbung bleibt das Potential vollkommen unbestimmt, in welchem Maße Datensammlung auf die Lebenswirklichkeit der Nutzer:innen zurückwirkt. Das Risiko ist schlichtweg nicht greifbar, da mögliche Konsequenzen nur in den seltensten Fällen auftreten, sondern i. d. R. Gegenstand fiktiver Gedankenspiele bleiben. Es besteht daher kaum eine Veranlassung, Privatisierung als Anspruch ernstzunehmen und entschiedene Maßnahmen zur Privatisierung im Alltag zu ergreifen. Insofern verweist das vermeintliche Paradoxon eines nachlässigen Umgangs mit Privatheitsbedrohungen durch den Smart Speaker, bei gleichzeitigem Bewusstsein über die Datenaneignung durch privatwirtschaftliche Akteure, auf konkrete Defizite: Die unzureichende Kenntnis in Bezug auf technische Zusammenhänge und die Verwertungsketten in einer globalen Datenökonomie und damit einhergehenden Risiken. Diese Umstände machen deutlich, dass die digitale Transformation in einem Tempo von Statten geht, das es schwerlich möglich macht, in Privatheitsfragen aufgrund eigener Erfahrungsbestände angemessen zu agieren; insofern stellen Konzepte wie informationelle Selbstbestimmung Nutzer:innen häufig vor kaum zu lösende Aufgaben – eine Erkenntnis, die als Aufforderung für systemische Lösungen dieser Fragen auf rechtlicher Ebene ebenso wie für verstärkte, institutionell verankerte und gesamtgesellschaftlich angelegte Aufklärungsarbeit verstanden werden muss.

Literaturverzeichnis

Agi, Benjamin und Jullien, Nicolas (2018): Is the Privacy Paradox in Fact Rational? doi: http://dx.doi.org/10.2139/ssrn.3109695.

Acquisti, Alessandro und Grossklags, Jens (2005): Privacy and Rationality in Individual Decision Making. *IEEE Security & Privacy,* 3(1). doi: http://doi.org/10.1109/MSP.2005.22.

Arendt, Hannah (2002): *Vita activa oder Vom tätigem Leben*. München: Piper.

Barnes, Susan (2006): A privacy paradox: Social networking in the United States. *First Monday* 1. URL: https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312.

Bhatt, Jiten Jwalant (2019): I Think I Can Trust Alexa, But How Much? *Intersect* 13 (1). URL: https://ojs.stanford.edu/ojs/index.php/intersect/article/view/1410.

Brause, Saba R. und Blank, Grant (2020): Externalized Domestication: Smart Speaker Assistants, Networks and Domestication Theory. *Information, Communication & Society,* 23 (5), S. 751–63. doi: https://doi.org/10.1080/1369118X.2020.1713845.

Brause, Saba R. und Blank, Grant (2024): 'There Are Some Things That I Would Never Ask Alexa' – Privacy Work, Contextual Integrity, and Smart Speaker Assistants. *Information, Communication & Society,* 27 (1), S. 182–97. doi: https://doi.org/10.1080/1369118X.2023.2193241.

Buteau, Emily und Lee, Joonghwa (2021): Hey Alexa, Why Do We Use Voice Assistants? The Driving Factors of Voice Assistant Technology Use. *Communication Research Reports,* 38 (5), S. 336–45. doi: https://doi.org/10.1080/08824096.2021.1980380.

Cho, Eugene, S. Shyam Sundar, Saeed Abdullah, und Nasim Motalebi. 2020. „Will Deleting History Make Alexa More Trustworthy? Effects of Privacy and Content Customization on User Experience of Smart Speakers". *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, S. 1–13. doi: https://doi.org/10.1145/3313831.3376551.

Endress, Martin (2003): *Vertrauen*. Bielefeld: transcript.

Gautam, Sanjana (2022): In Alexa, We Trust. Or Do We?: An Analysis of People's Perception of Privacy Policies. arXiv. URL: http://arxiv.org/abs/2209.00086.

Gomart, Emilie und Hennion, Antoine (1999): A Sociology of Attachment: Music Amateurs, Drug Users. *The Sociological Review,* 47(1), S. 220-247. doi: https://doi.org/10.1111/j.1467-954X.1999.tb03490.

Habermas, Jürgen (1990): *Strukturwandel der Öffentlichkeit*. Frankfurt: Suhrkamp.

Hennion, Antoine (2011): „Offene Objekte, Offene Subjekte? Körper und Dinge im Geflecht von Anhänglichkeit, Zuneigung und Verbundenheit." *Zeitschrift für Medien- und Kulturforschung,* 2 (1), S. 93–110.

Hennion, Antoine (2017): From Valuation to Instauration: On the Double Pluralism of Values. *Valuation Studies*, 5 (1), S. 69–81.

Hine, Christine (2020): Strategies for Reflexive Ethnography in the Smart Home: Autoethnography of Silence and Emotion. *Sociology,* 54 (1), S. 22-36. doi: https://doi.org/10.1177/0038038519855325

Hoffmann, Christian Pieter; Lutz, Christoph und Ranzini, Giulia (2016): Privacy Cynicism: A New Approach to the Privacy Paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4). doi: http://dx.doi.org/10.2139/ssrn.3319830.

James, William (1994): *Was ist Pragmatismus?* Weinheim: Beltz.

James, William (2006): *Pragmatismus und radikaler Empirismus*. Frankfurt: Suhrkamp.

Joas, Hans (1996): *Die Kreativität des Handelns*. Frankfurt: Suhrkamp.

Kang, Hyunjin und Oh, Jeeyun (2023): Communication Privacy Management for Smart Speaker Use: Integrating the Role of Privacy Self-Efficacy and the Multidimensional View. *New Media & Society* 25 (5), S. 1153–75. doi: https://doi.org/10.1177/14614448211026611.

Kröger, Jacob Leon; Gellrich, Leon; Pape, Sebastian; Brause, Saba R. und Stefan Ullrich (2022): Personal Information Inference from Voice Recordings: User Awareness and Privacy Concerns. *Proceedings on Privacy Enhancing Technologies,* 2022 (1), S. 6–27. doi: https://doi.org/10.2478/popets-2022-0002.

Lamla, Jörn (2019): Selbstbestimmung und Verbraucherschutz in der Datenökonomie. *Aus Politik und Zeitgeschichte,* 69 (24-26).

Lamla, Jörn; Büttner, Barbara; Ochs, Carsten; Pittroff, Fabian; Uhlmann, Markus (2022): Privatheit und Digitalität. Zur soziotechnischen Transformation des selbstbestimmten Lebens. In: Roßnagel, Alexander und Friedewald, Michael (Hrsg.): *Die Zukunft von Privatheit und Selbstbestimmung*. Wiesbaden: Springer, S.125-158.

Lau, Josephine; Zimmermann, Benjamin und Schaub, Florian (2018a): Alexa, Stop Recording: Mismatches between Smart Speaker Privacy Controls and User Needs. Poster presented at the *14th Symposium on Usable Privacy and Security (SOUPS 2018)*. URL: https://www.usenix.org/sites/default/files/soups2018posters-lau.pdf.

Lau, Josephine; Zimmermann, Benjamin und Schaub, Florian (2018b): Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-Seeking Behaviors with Smart Speakers. *Proceedings of the ACM on Human-Computer Interaction* 2 (CSCW), S. 1–31. doi: https://doi.org/10.1145/3274371.

Luhmann, Niklas (2000): *Vertrauen*. Stuttgart: Lucius&Lucius.

Luhmann, Niklas (2001): Vertrautheit, Zuversicht, Vertrauen. Probleme und Alternativen. In: Hartmann, Martin und Offe, Claus (Hrsg.): *Vertrauen. Die Grundlage sozialen Zusammenhalts*. Frankfurt: Campus.

Lutz, Christoph und Newlands, Gemma (2021): Privacy and smart speakers: A multi-dimensional approach. *The Information Society,* 37(3), S. 147-162. doi: 10.1080/01972243.2021.1897914.

Malodia, Suresh; Islam, Nazrul; Kaur, Puneet und Dhir, Amandeep (2024): Why Do People Use Artificial Intelligence (AI)-Enabled Voice Assistants? *IEEE Transactions on Engineering Management 71*, S. 491–505. doi: https://doi.org/10.1109/TEM.2021.3117884.

Malkin, Nathan; Deatrick, Joe; Tong, Allen; Wijesekera, Primal; Egelman, Serge und Wagner, David (2019): Privacy Attitudes of Smart Speaker Users. *Proceedings on Privacy Enhancing Technologies,* 2019 (4), S. 250–71. doi: https://doi.org/10.2478/popets-2019-0068.

Mittal, Mehak und Manocha, Sanjay (2022): Alexa! Examine Privacy Perception and Acceptance of Voice-Based Artificial Intelligence among Digital Natives. *Journal of Information and Optimization Sciences,* 43 (7), S. 1679–92. doi: https://doi.org/10.1080/02522667.2022.2134367.

Mols, Anouk; Wang, Yijing und Pridmore, Jason (2022): Household Intelligent Personal Assistants in the Netherlands: Exploring Privacy Concerns around Surveillance, Security, and Platforms. *Convergence: The International Journal of Research into New Media Technologies,* 28 (6), S. 1841–60. doi: https://doi.org/10.1177/13548565211042234.

Nassehi, Armin (2019): *Muster. Theorie der digitalen Gesellschaft*. München: C.H. Beck.

Nissenbaum, Helen (2010): *Privacy in Context*. Stanford: Stanford University Press.

Nissenbaum Helen und Brunton, Finn (2016): *Obfuscation*. Cambridge: MIT Press

Ochs, Carsten (2022): *Soziologie der Privatheit. Informationelle Teilhabebeschränkung vom Reputation Management bis zum Recht auf Unberechenbarkeit*. Weilerswist: Velbrück.

Pentzold, Christian; Bischof, Andreas und Heise, Nele (Hrsg.): *Praxis Grounded Theory: theoriegenerierendes empirisches Forschen in medienbezogenen Lebenswelten: ein Lehr- und Arbeitsbuch. Lehrbuch*. Wiesbaden: Springer VS 2018.

Pridmore, Jason und Mols, Anouk (2020): Personal Choices and Situated Data: Privacy Negotiations and the Acceptance of Household Intelligent Personal Assistants. *Big Data & Society,* 7 (1). doi: https://doi.org/10.1177/2053951719891748.

Roessler, Beate und Mokrosinska, Dorota (2013): Privacy and Social Interaction. *Philosophy and Social Criticism,* 39 (8), S. 771-791.

Rzepka, Christine (2019): Examining the Use of Voice Assistants: A Value-Focused Thinking Approach. *Twenty-fifth Americas Conference on Information Systems*. URL: https://aisel.aisnet.org/amcis2019/human_computer_interact/human_computer_interact/20.

Sennett, Richard (1993): *Verfall und Ende des öffentlichen Lebens. Die Tyrannei der Intimität*. Frankfurt: Fischer.

Solove, Daniel J. (2021): The Myth of the Privacy Paradox. *Washington Law Review,* 1/2021. URL: https://scholarship.law.gwu.edu/faculty_publications/1482/.

Spradley, James (2016): *The Ethnographic Interview*. Long Grove: Waveland.

Trepte, Sabine; Scharkow, Michael und Dienlin, Tobias (2020): The privacy calculus contextualized: The influence of affordances. *Computers in Human Behavior*, 104. doi: https://doi.org/10.1016/j.chb.20.

Whitaker, Reg (1999): *Das Ende der Privatheit. Überwachung, Macht und Kontrolle im Informationszeitalter*. München: Kunstmann.

Zeng, Eric; Mare, Shrirang und Roesner, Franziska (2017): End User Security & Privacy Concerns with Smart Homes. *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. URL: https://www.usenix.org/system/files/conference/soups2017/soups2017-zeng.pdf.

Zuboff, Shoshanna (2018): *Das Zeitalter des Überwachungskapitalismus*. Frankfurt/New York: Campus.

Datenautonomie im Smart Home: eine praktische/prototypische Umsetzung

Christopher Ruff, Alexander Orlowski, Andrea Horch

Zusammenfassung

In diesem Paper stellen wir einen Meta-Assistenten - Transparenter Datenautonomie Meta-Assistent (DAMA) - vor, der die informationelle Selbstbestimmung der Nutzer:innen von Smart Home-Systemen erhöht, indem er über Verdatung informiert und (semi-)automatische Kontrollmöglichkeiten gibt.

1. Das Home wird Smart

Smart Home-Geräte ermöglichen die Automatisierung und Fernsteuerung von Haushaltsfunktionen wie Beleuchtung, Heizung und Sicherheitssystemen über vernetzte Technologie. Die Nutzung und Verbreitung von Smart Home-Geräten ist in den letzten Jahren deutlich gestiegen. Nach einer BITKOM-Studie (Moltrecht/Schnaack 2022) ist die Nutzung von Smart Home-Anwendungen in deutschen Haushalten von 26 % im Jahr 2018 stetig auf 43 % im Jahr 2022 angestiegen. Hierbei wird das Smart Home zumeist per Smartphone (85 %) gesteuert. 55 % nutzen jedoch auch Sprachsteuerung, wobei bei 87 % ein stationärer Sprachassistent, wie z. B. Amazon Echo oder Google Home, eingesetzt wird. Die Studie hat zudem ermittelt, dass Smart Home-Geräte in Zimmern mit erhöhtem Bedarf an Privatsphäre, wie z. B. Wohnzimmer (79 %), Schlafzimmer (69 %), Badezimmer (57 %), Arbeitszimmer (49 %) oder Kinderzimmer (24 %), verwendet werden. Dies deckt sich mit einer Studie zur Nutzung von Smart Speakern (Brandt 2020), die von 67 % im Wohnzimmer, von 44 % im Arbeitszimmer, von 43 % im Schlafzimmer und von 35 % im Badezimmer genutzt werden. Daraus ergeben sich hohe Anforderungen an Privatheit und Datenschutz, insbesondere bei der Erhebung und Verarbeitung personenbezogener Daten (Feldmeier u.a. 2022). Diese Anforderungen sind in Deutschland gesetzlich geregelt (Feldmeier u.a. 2022). Bei der Speicherung und Verarbeitung der Daten im Ausland kann sich die rechtliche Lage verkomplizieren. Nach der BIT-

KOM-Studie sind Hemmnisse für den Einsatz von Smart Home-Geräten vor allem die Angst vor Hacker-Angriffen (47 %), die Befürchtung des Missbrauchs der persönlichen Daten (37 %) sowie die Angst um die eigene Privatsphäre (29 %) (Moltrecht/Schnaack 2022). Verstärkt werden diese Bedenken durch Medienberichte über den Zugriff auf Bilder der eigenen Sicherheitskamera durch Dritte (Breithut 2020) oder das Erscheinen von Bildern von Privatpersonen im Internet, die von ihrem Saugroboter erstellt wurden (Hensen 2022).

Betrachtet man die von den aufgeführten Studien ermittelten Hemmnisse für die Nutzung von smarten Geräten, wird klar, dass diese auf fehlende Transparenz der Anbieter bezüglich der Datenerhebung, Datenverarbeitung und Datenspeicherung basieren. Es existieren zwar Ansätze zur Erhöhung der Sicherheit in smarten Umgebungen (BSI 2022), aber keine ausreichenden Regulierungssysteme. Die Erfassung und die Verarbeitung sind daher nicht vollständig unter Kontrolle der Menschen, die Smart Home-Systeme nutzen oder die sich in smarten Umgebungen befinden.

In diesem Kapitel arbeiten wir die Relevanz von Datenautonomie im Smart Home-Kontext heraus und präsentieren eine Möglichkeit für Nutzer:innen, diese zu verbessern. Dazu stellen wir die Ergebnisse des Projekts »Transparenter Datenautonomie Meta-Assistent (DAMA)« vor. DAMA wirkt den o.g. Hemmnissen mit einem Meta-Assistenten für smarte Umgebungen entgegen und will diese möglichst beseitigen. Hierfür reguliert der Meta-Assistent die smarten Geräte oder gar einzelnen Sensoren der Geräte kontextbasiert. Zudem schafft er Transparenz, indem er den Benutzer:innen und auch den Gästen von smarten Umgebungen angeschaltete Geräte, die Sensoren für die Datenerfassung besitzen, anzeigt. Zusätzliche Transparenz schafft der Meta-Assistent durch die Anzeige von Veränderungen, wenn sich beispielsweise der Kontext der smarten Umgebung ändert (z. B. eine Person ist allein in der Umgebung vs. mehrere Personen sind anwesend) und deswegen einzelne Geräte oder Sensoren an- bzw. abgeschaltet werden. Nach der Darstellung der Funktionen und ihrer technischen Umsetzung gehen wir auf verschiedene Szenarien ein, in denen der Meta-Assistent Anwendung finden kann. Darüber hinaus skizzieren wir Ergebnisse aus der Evaluation mit potenziellen Nutzer:innen.

2. Smart Home-Geräte als Herausforderung für die Datenautonomie

Die Wohnung als typischer Nutzungskontext von Smart Home-Geräten genießt eigentlich besonderen Schutz vor Überwachung. So ist in Art. 13 GG verankert, dass „die Wohnung […] unverletzlich" ist. Durch die Nutzung von Smart Home-Geräten werden nun in diesem Bereich eine Vielzahl an Sensoren eingebaut, die verschiedenste, möglicherweise sensible Daten erheben. So verfügen beispielsweise Sprachassistenten über Mikrofone oder smarte Kühlschränke und Türklingeln über Kameras. Dadurch werden bei der Nutzung Daten und Informationen aufgezeichnet, aber auch viele weitere Meta-Informationen gesammelt, die bei der allgemeinen Nutzung dieser Geräte anfallen (Lutz/Newlands 2021).

Dies erzeugt in mehrerlei Hinsicht Konflikte, denn generell sollte Datenerhebung nur erfolgen, wenn die Nutzer:innen dieser aktiv zustimmen. Nur dann ist die informationelle Selbstbestimmung (Jandt 2016) gegeben, wie sie auch im Volkszählungurteil (BVerfG 1983) festgelegt wurde. Dabei bedeutet informationelle Selbstbestimmung, dass eine Person bewusst und informiert dem Teilen ihrer Daten zustimmen muss. Informiert heißt, dass der Umfang und die Konsequenzen des Datensammelns bekannt sind, und die Nutzer:innen sich auf Basis dieses Wissens explizit dafür entscheiden, diese Daten zweckgebunden zu teilen. Insbesondere das eigene Zuhause sollte dabei als Rückzugsort gelten, in dem ein freies und unbeobachtete Leben garantiert ist. Das untergraben Smart Home-Gegenstände jedoch aus mehreren Gründen, die im Folgenden näher dargestellt werden.

2.1 Allgegenwärtige und kontinuierliche Datenerfassung

Die Erfassung von Daten durch Smart Home-Geräte findet kontinuierlich und unauffällig statt. Insbesondere da die Geräte so gestaltet sind, dass sie mit der Umgebung verschmelzen (Rajkumar u.a, 2010) und eben nicht im Alltag auffallen, unterlaufen sie die bewusste Zustimmung. So kann ein Sprachassistent, wie ein Amazon Echo Dot, in einem Bücherregal stehen und so gerade von Gästen übersehen werden (Marky u.a. 2020). Das Mikrofon darin kann jedoch jederzeit angehen. Dies kann auch passieren, wenn es gar nicht intendiert ist, beispielsweise wenn das Wakeword aus Versehen ausgesprochen wird oder ein ähnliches Wort als Wakeword missinterpretiert wird und zu einer Aktivierung des Mikrofons führt. Doch selbst wenn bekannt ist, dass diese Geräte im Raum sind, ist für die Nut-

zer:innen meist nicht transparent, wann die Geräte Daten erheben und für welche Zwecke (Guhr u.a. 2020; Hern 2019).

2.2 Prädiktive Privatheit

Der Begriff „prädiktive Privatheit" (Mühlhoff 2020) beschreibt das Phänomen, wenn ursprünglich nicht personenbezogene Daten so mit anderen Daten in Kontext gesetzt werden oder vorhergesagt werden können, dass daraus sensible Informationen abgeleitet werden können. Denn selbst wenn bekannt ist, welche Daten übermittelt werden, reicht das nicht unbedingt aus, um eine informierte Entscheidung für eine Zustimmung zu treffen. Zwar ist es offensichtlich, dass Daten, wie zum Beispiel aufgenommene Unterhaltungen, personenbezogen sind. Es gibt jedoch eine Vielzahl an Informationen, die von Smart Home-Geräten gesammelt werden, bei denen dies nicht auf den ersten Blick klar ist, beziehungswiese das Ausmaß der Zustimmung nicht bekannt ist. Dabei können scheinbar unverdächtige Daten detaillierte Rückschlüsse über Personen zulassen, obwohl sie von Sensoren stammen, die auf den ersten Blick harmlos wirken (Kröger 2019). Beispielsweise lassen die Daten von einem CO_2-Sensor mit entsprechenden Vergleichswerten Rückschlüsse zu, ob gerade eine oder mehrere Personen in einem Raum anwesenden sind (ebd.). Dadurch kann ggf. gefolgert werden, dass zu einem bestimmten Zeitpunkt Besucher:innen anwesend waren. Ein weiterer Fall wäre, dass es durch den entsprechenden Abgleich mit Vergleichsgruppen möglich ist, aus den Sehgewohnheiten von Fernsehzuschauer:innen abzuleiten, welcher sozialen Gruppe diese angehören (Ghiglieri u.a. 2016). Welche Daten welche Rückschlüsse zulassen, beziehungsweise in Zukunft zulassen könnten, ist also nicht vorherzusagen.

Der Prozess des Ableitens wird als *inferencing* (Wachter 2018) bezeichnet. Durch gestiegene Rechenleistungen und insbesondere Fortschritte im Bereich künstlicher Intelligenz werden immer mehr Inferenzen möglich. Dementsprechend ist es nicht möglich, zu einem bestimmten Zeitpunkt zu sagen, welche Rückschlüsse aus bestimmten Daten in Zukunft möglich sein werden. Deshalb können Informationen, die zum Zeitpunkt der Zustimmung nicht personenbezogen sind, in Zukunft durch Inferenz zu personenbezogenen Daten werden.

2.3 Deanonymisierung

Die zunehmende Rechenleistung macht es nicht nur möglich, dass aus den Daten Rückschlüsse über Personen gezogen werden, sondern ermöglicht auch, eigentlich anonymisierte Daten wieder so in Kontext zu setzen, dass sie wieder einer Person zugeordnet werden können (Wachter 2018). Selbst wenn also zu einem bestimmten Zeitpunkt Daten anonymisiert weiterverarbeitet werden dürfen, ist es möglich, dass sie zu einem späteren Zeitpunkt doch wieder deanonymisiert werden können.

Durch die in diesem Kapitel beschrieben Faktoren wird das Recht auf informierte Selbstbestimmung mehrfach unterlaufen, sodass eine informierte Einwilligung im Smart Home wiederholt unterlaufen wird, weder für die Bewohner:innen der Wohnung, aber erst recht nicht für mögliche Besucher:innen ist es möglich, informierte Entscheidungen zu treffen. Deshalb ist es notwendig, andere Wege zu finden, zu kontrollieren, wann welche Daten erhoben werden.

3. Meta-Assistent

Aufgrund dieser vielfältigen Problematik haben wir einen Meta-Assistenten entwickelt, der es Smart Home-Nutzer:innen ermöglichen soll, ihre informationelle Selbstbestimmung zu verbessern. Der *transparente Datenautonomie Meta-Assistent* (DAMA) soll die im vorherigen Kapitel beschriebenen Probleme adressieren und eine Hands-on-Lösung bieten, die eine bewusstere Nutzung der Geräte zulässt. Das System ist dabei als Überbrückung gedacht, bis notwendige juristische und technische Regulierung eingreift. Im Nachfolgenden skizzieren wir die Ziele von DAMA und wie wir diese umsetzen.

3.1 Ziele von DAMA

Transparenz

Benutzer:innen von intelligenten Assistenten und Geräten wissen oft nicht genau, ob und wann ihre Daten aufgezeichnet und übertragen werden. Darüber hinaus haben die Hersteller solcher Geräte oft Gründe, dies zu verschleiern, da sie die Daten z. B. für Diagnose- und Werbe-Zwecke

nutzen möchten und um das Benutzer:innen-Verhalten zu studieren. Der Meta-Assistent schafft hier Transparenz für die Benutzer:innen, indem auf verschiedenen Kommunikationskanälen, je nach Wunsch der Benutzer:innen, (z. B. Sprachdurchsage und/oder Anzeige auf einem Smart-TV, Smartphone oder Tablet) darüber aufgeklärt wird, welche smarten Geräte sich in der Umgebung befinden, über welche Sensoren diese verfügen und ob diese an- oder ausgeschaltet sind. Dadurch wird zum einen Aufmerksamkeit darauf gelenkt und der Tendenz smarter Geräte entgegengewirkt, im Raum zu verschwinden. Zum anderen wird allgemein Bewusstsein geschaffen, wie oft Daten im Smart Home erhoben werden.

Kontext-basierte, automatische Regulierung von Geräten

Ein weiteres Ziel des Datenautonomie-Assistenten ist die möglichst automatisierte Regulierung der smarten Geräte anhand der Datenschutzpräferenzen der Benutzer:innen in spezifischen Situationen. In den meisten Fällen sollten die Funktionen der Geräte nutzbar sein und ihren Zweck erfüllen. In einigen, von den Benutzer:innen festgelegten Situationen, überwiegt aber das Bedürfnis nach Datenschutz. Im Zuge des DAMA-Projektes wurden mehrere empirische Studien durchgeführt, um das Bedürfnis nach Datenschutz in unterschiedlichen Situationen zu ermitteln und welche Geräte, bzw. Sensoren dabei besonders heikel sind. Durch die Automatisierung bleibt der grundsätzliche Mehrwert der Convenience von Smart Home Systemen erhalten. Denn häufig werden Lösungen die datenschutzsensibel sind, eben nicht verwendet, weil sie einen höheren Aufwand mit sich bringen (Sheridan 2019).

In DAMA wird die Sicherung des Datenschutzes im Smart Home auf drei grundlegende Arten gesichert:

- Sicherstellung der Privatsphäre der Hausbesitzenden durch Verhinderung von Datenlecks in die Cloud, beispielsweise durch Gerätehersteller, Hacker:innen oder Nachrichtendienste.
- Gewährleistung der Privatsphäre von Gästen durch Verhinderung von Datenabflüssen in die Cloud.
- Schutz der Privatsphäre der Hausbesitzenden vor Datenlecks durch Personen mit temporärem Zugang zur smarten Umgebung.

3.2 Technische Umsetzung

Um diese Ziele zu erreichen, muss das System zum einen in der Lage sein, Informationen über die aktuelle Situation im Smart-Home zu erlangen und zum anderen, diese Informationen zu verarbeiten und daraufhin eine *Steuerung* der Geräte vorzunehmen. Um mehr *Transparenz* zu erreichen, sind sog. Aktoren – also Geräte, die eine Aktion ausführen können, wie z. B. den Benutzer:innen aktuelle Informationen über die Smart Home-Geräte und das System selbst zu geben – integriert.

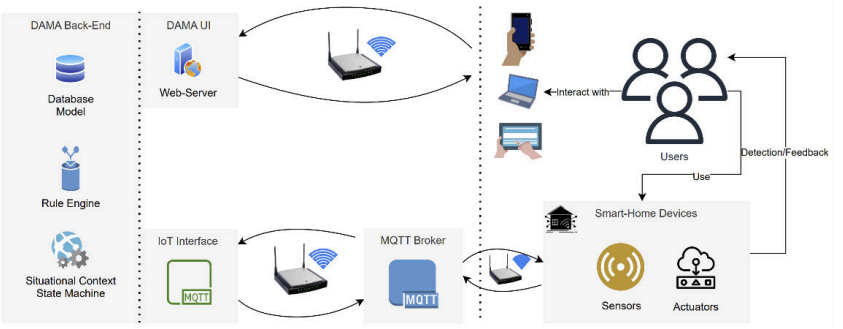

Abbildung 1: Architektur des Datenautonomie-Assistenten

Abbildung 1 zeigt den schematischen Aufbau der Architektur von DAMA. Auf der linken Seite befindet sich das sog. „Back-End". Dieses kommuniziert über die Kommunikations-Ebene (Mitte) mit den Benutzer:innen über die Präsentations-Ebene (rechts). Die smarten Geräte mit diversen Sensoren und Aktoren werden genutzt, um die nötigen Kontextinformationen zu bekommen und auch um die Regulierung dieser Geräte selbst zu verändern. Im Folgenden werden die einzelnen Ebenen näher erläutert.

Back-End

Im „Back-End" werden die von verschiedenen Sensoren und Geräten erfassten Daten und Informationen gesammelt und verarbeitet. Basierend auf der Benutzerkonfiguration, einschließlich der Einstellung verschiedener Situations-Modi, ist die Business-Logik des Datenautonomie-Assistenten für die Verarbeitung und Steuerung der Geräte im Smart Home durch Geräte- (Device-) Ebene verantwortlich.

Persistenz (Database Model)

In einer relationalen Datenbank werden die Informationen über smarte Geräte und Komponenten, sowie die Informationen über Situationsmodi und automatisierte Regeln dauerhaft gespeichert.

In das System ist eine *Regel-Engine* integriert, welche die Nutzer:innen in der Oberfläche einfach konfigurieren können. So können die automatisierten Regulierungen der Geräte ausgelöst werden. Die Regeln müssen persistent abgelegt werden, um jederzeit abrufbar zu sein.

Des Weiteren ist hier die Logik zum Wechsel der Situations-Modi hinterlegt, die die Informationen der Sensoren verarbeitet, mittels der Regel-Engine Entscheidungen trifft und dann über entsprechende Schnittstellen die Regulierung der Geräte veranlasst.

Kommunikations-Ebene

DAMA kann mit verschiedenen Aktoren und Sensoren kommunizieren, um die gewünschte Regulierung und Transparenz für die Benutzer:innen herzustellen. Es wird das MQTT-Protokoll eingesetzt (falls unterstützt), um zwischen dem Back-End und den Geräten zu Informationen zu übermitteln. Das System ist erweiterbar, sodass verschiedene weitere Geräte unterstützt werden können.

Präsentations-Ebene

Diese Ebene ist durch eine webbasierte Benutzeroberfläche bedienbar, die auf mobilen Endgeräten wie Tablets und Smartphones, sowie anderen Geräten (z. B. Smart-TV) angezeigt werden kann. In der endgültigen Version wird die Datenverbindung zwischen Geräten und dem Controller TLS-Verschlüsselung verwenden, um Manipulation der gesendeten Informationen vorzubeugen. Die Benutzer:innen können sich hier einen Account anlegen, der durch ein Passwort geschützt wird. In einem Haushalt mit mehreren Personen sind mehrere Benutzer:innen mit verschiedenen Situations-Modi möglich.

3.3 Situationserkennung

Die Situationserkennung umfasst Komponenten, die Informationen über sensorische Systeme sammeln, wie Mikrofone in Sprachassistenten, Umweltsensoren, aber auch KI-gestützte Algorithmen in Verbindung mit Kameraaufnahmen. In unseren empirischen Studien zeigt sich, dass für das Bedürfnis nach Privatheit mitentscheidend ist, wie viele, bzw. welche Menschen sich im Smart-Home aufhalten. Deshalb versucht das System, zu erkennen, wer und wie viele Personen sich in der aktuellen Smart Home- (oder Büro-) Umgebung aufhalten, auf die der DAMA-Assistent Zugriff hat. Da DAMA darauf ausgelegt ist, die Privatsphäre zu maximieren, verwendet das System minimalinvasive Detektionstechnologie und vermeidet biometrische Erkennung, wie Gesichts-, Sprach- oder Iriserkennung. Kameras befinden sich in weniger privaten Bereichen, wie dem Eingang, konzentrieren sich nur auf einen kleinen Bereich und nur von oben. Die KI versucht lediglich, Personen beim Betreten oder Verlassen zu erkennen, und zeichnet keine biometrischen Informationen auf. Die Datenverarbeitung erfolgt ausschließlich lokal.

Weitere Komponenten und Sensoren können an das System angeschlossen werden, um noch weitere Situationen zu erkennen und darauf reagieren zu können. Im aktuellen System ist ein digitaler Kalender angeschlossen, womit sich – je nach geplantem Ereignis, Änderungen an den smarten Geräten anstoßen lassen. So kann beispielsweise der Besuch einer bestimmten Person im Kalender vermerkt werden, worauf das System schon im Vorfeld die gewünschten Privatsphäre-Einstellungen vornimmt.

Benutzeroberfläche

Es wurde eine Web-basierte Benutzeroberfläche implementiert, über die alle Funktionen von DAMA genutzt und gesteuert werden können.

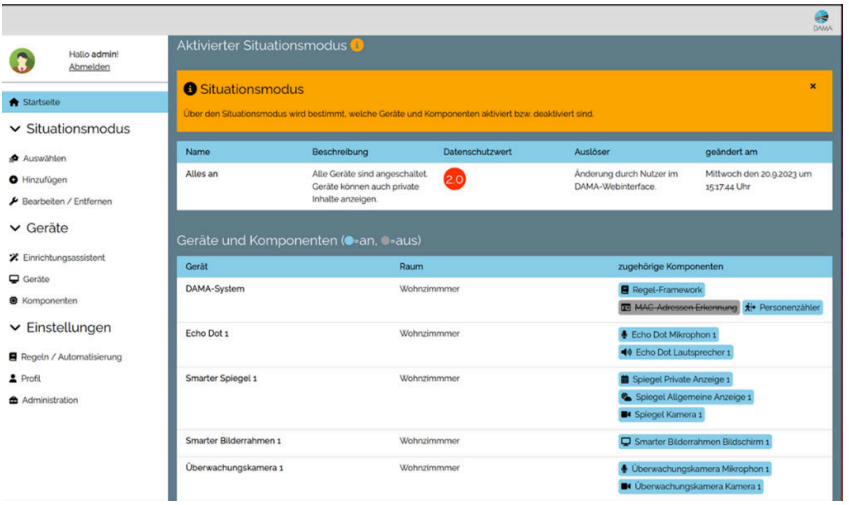

Abbildung 2: Bedienoberfläche

Die Oberfläche umfasst die folgenden Funktionen:

- *Startseite:* Übersicht über den aktuellen Situationsmodus samt allen dazu eingeschalteten smarten Geräten und Komponenten. Ein daraus errechneter Datenschutzwert wird einfach sichtbar und farblich hervorgehoben dargestellt, um die Benutzer:innen zu informieren.
- *Situationsmodus bearbeiten:* Hier können die Benutzer:innen den aktuell eingestellten Modus manuell ändern, neue Situationsmodi erstellen oder diese anpassen.
- *Einrichtungsassistent:* Über einen leicht zu bedienenden Assistenten wird der Nutzer durch die Einrichtung der smarten Geräte geführt. Dies muss nur bei der Einrichtung des Systems oder beim Hinzufügen eines neuen Geräts geschehen. Ziel ist es, die technischen Hürden bei der Nutzung so niedrig wie möglich zu halten.
- *Regeln/Automatisierung:* Hier können Benutzer:innen verschachtelte Regeln anlegen, wie das System auf Ereignisse reagieren und damit die Situationsmodi ändern soll. Als Beispiel könnte eine Regel angelegt werden, anhand derer bei Eintritt einer bestimmten Person in das Smart-Home der Sprachassistent und die Anzeige eines Privaten Kalenders abgeschaltet wird, bis die Person das Smart-Home wieder verlässt.
- *Geräte/Komponenten:* Hier können die Geräte und Komponenten, die bereits im System eingerichtet sind, verwaltet werden. Namen und Da-

ten, wie beispielsweise für die Berechnung des Datenschutzwertes, können hier ebenfalls modifiziert werden.
- *Administration:* Hier können bestimmte Benutzer:innen die Profile der anderen Benutzer:innen und grundlegende Einstellungen des Systems verwalten.

Integration und Test-Aufbau

Abbildung 3: Grundriss des Smart Home bzw. Smart Office Bereichs

Das DAMA-System wurde in das Smart Home / Smart Office Labor im Bürogebäude des Fraunhofer IAO in Stuttgart integriert. Das Labor ist in einen Smart Home-Bereich (links) und einen Smart Office-Bereich (rechts) unterteilt, wie in Abbildung 3 dargestellt. In der Evaluations-Phase des Projektes wurde der Smart-Home Bereich genutzt. Der Smart Home-Bereich umfasst Geräte wie einen intelligenten Kühlschrank, ein intelligentes Sofa, einen intelligenten Couchtisch, einen intelligenten Spiegel und einen intelligenten Fernseher. Außerdem sind zwei Tablets, verschiedene smarte Steckdosen, mehrere Sprach-Assistenten (Amazon Alexa), Web-Cams und der Smart-Home Hub „Homey“ integriert. Kern der Applikation ist ein Kleinst-Rechner, auf dem das System selbst läuft.

4. Szenarien

Durch verschiedene Szenarien adressieren wir die unterschiedlichen Herausforderungen für den Datenschutz im Smart Home und berücksichtigen typische Konstellationen an Geräten und Akteuren. Die Szenarien sind auch Grundlage für die Evaluation, anhand derer überprüft wird, ob der von uns entwickelte Prototyp wirklich zu einer Verbesserung für Nutzer:innen geführt hat. Dazu haben wir fünf Szenarien erarbeitet, in denen sich typische Anwendungsfälle konkret widerspiegeln. Sie sind stark an die Nutzungsrealität angelehnt, um eben genau für diese eine Verbesserung zu erzielen. Die von uns entwickelten Szenarien decken dabei eine Bandbreite von Situationen und Akteurskonstellationen ab, wie sie in der alltäglichen Nutzung vorkommen, aber abstrakt genug sind, um für die Entwicklung verallgemeinerbare Prinzipien und Ziele anlegen zu können. Es können dabei jedoch nicht alle Datenschutz-Aspekte im Smart Home erfasst werden. Wir sind jedoch der Überzeugung, dass diese Szenarien eine gute Basis für die Entwicklung sind und die Nutzungsrealität gut abbilden. Das System selbst lässt sich auch für anderweitige Szenarien flexibel anpassen.

4.1 Szenario 1: Bewohner:in kommt nach Hause (DAMA aktiviert alle Smarten Geräte)

Das erste Szenario ist eine Basisversion und spiegelt die häufigste Ausgangsposition bei der Nutzung wider: eine Person, die in einem Smart Home lebt. Wir gehen davon aus, dass eine Person die eigenen Smart Home-Gegenstände in ihrem normalen Alltag ihre Smart Home Gegenstände auch nutzen will, sonst hätte sie diese nicht angeschafft. Deshalb werden die Geräte angeschaltet, sobald die Person alleine nach Hause kommt. Durch einen Sensor des Systems wird erkannt, dass jemand das Haus oder die Wohnung betritt. Dass es sich dabei um den bzw. die Bewohner:in handelt, wird über einen Mac-Adressen-Scanner festgestellt, der die Person über ihr Smartphone als Besitzer:in des Smart Home identifiziert. Daraufhin werden alle smarten Gegenstände durch DAMA freigegeben und aktiviert. Dieses Basisszenario erweitern wir Schritt für Schritt und adaptieren es entsprechend.

4.2 Szenario 2: Bekannte Personen kommen zu Besuch

Eine erste Abweichung, die eine Abschaltung von Geräten erfordern könnte, ist die Anwesenheit einer anderen Person, also von Besuch. Wenn diese Person nicht darüber informiert ist, dass Smart Home-Geräte Daten aufzeichnen, liegt keine informierte Einwilligung vor. Dementsprechend sollten die Smart Home-Geräte, die Daten über die Besucher aufzeichnen können, deaktiviert sein. So sollen beispielsweise persönliche Gespräche nicht zufällig durch aktive Mikrofone mitgeschnitten werden, insbesondere, wenn sehr private Dinge besprochen werden.

Wenn die Person dem oder der Bewohner:in bekannt ist, kann es sein, dass diese über die Geräte bereits Bescheid weiß, aber trotzdem bestimmte Sensoren nicht aktiviert haben möchte. Um die Person von einer nicht bekannten Person zu unterscheiden, kann diese ebenfalls durch den Mac-Adressen-Scanner erkannt werden[1], und der Meta-Assistent schaltet dann automatisch um auf das für die jeweilige Besucher:in festgelegten Situationsmodus. Für den Besuch können aber auch die Besitzer:innen ihre eigenen Einstellungen festlegen, so können beispielsweise private Anzeigen wie Kalender deaktiviert werden.

4.3 Szenario 3: Unbekannte Person kommt ins Smart Home

Es können unterschiedliche Gruppen und Konstellationen im Smart Home anwesend sein. So macht es einen großen Unterschied, wenn es sich nicht um eine bekannte Person handelt, die das Haus betritt, sondern eine bisher unbekannte Person, beispielsweise ein:e Handwerker:in.

In diesem Fall ist es nicht mehr möglich, diese Person durch den Mac-Adressen-Scanner zu identifizieren, sondern sie muss alternativ erkannt werden (z. B. durch einen Personenzähler), und es kann durch das Fehlen eines freundschaftlichen Verhältnisses nicht davon ausgegangen werden, dass die Person davor über das Vorhandensein von Smart Home Geräten informiert ist. Neben dem Aspekt, dass diese Person nicht ohne Informierung Daten abgibt, möchte man als Bewohner:in möglicherweise nicht,

1 Dafür müsste die bekannte Person mit ihrem Smartphone in das WLAN eingewählt sein. Dies passiert in den meisten Fällen, in denen privater Besuch vorbei kommt automatisch. Zusätzlich braucht es dann die Einwilligung der Person, dass die MAC-Adresse des Smartphones von DAMA erkannt werden darf.

dass private Daten, zum Beispiel auf Anzeigen, für diese fremden Personen sichtbar sind.

4.4 Szenario 4: Home-Office

Wenn eine Person allein zu Hause ist, kann dennoch nicht gewollt sein, dass bestimmte Sensoren etwas aufzeichnen können. Sollten die Bedürfnisse der Bewohner:in in einer Situation von der Basiseinstellung abweichen, kann sie über DAMA den Situationsmodus jederzeit unkompliziert anpassen, sodass Geräte und Sensoren gemäß den Wünschen deaktiviert werden. Hierdurch sollen die Daten der Person geschützt werden. Es muss jederzeit eine Abwägung zwischen Nützlichkeit der Geräte und Risiko der Datenweitergabe erfolgen. Basierend auf dieser Abwägung stellt sich also die Frage, in welchen Situationen die Geräte dann abgeschaltet werden sollen. Dies spiegelt sich im Szenario Home-Office wider.

So sollte eine Telefonkonferenz, die im Smart Home geführt wird, nicht durch ein Smart Home-Geräte mitaufgezeichnet werden. Hinzu kommt aber auch ein zweiter Aspekt, es sollten auch keine privaten Informationen aus Versehen veröffentlicht werden. Zum Beispiel, wenn ein Gerät etwas durchsagt oder Anzeigen im Hintergrund zu sehen sind. Deshalb ist es sinnvoll, gewisse Geräte abzuschalten. Dies kann auch automatisch passieren durch eine Verbindung mit dem eigenen Kalender, sodass während eines Meetings Sprachassistenten oder digitale Anzeigen automatisch deaktiviert werden.

4.4 Szenario 5: Mehrere Personen wohnen im Smart Home

Die bisherigen Szenarien waren dadurch gekennzeichnet, dass es eine klare Unterscheidung/Hierarchie gab zwischen Bewohner:in und Besucher:innen. Wenn es mehrere Bewohner:innen gibt, ist dies nicht mehr der Fall. Die Herausforderung dabei ist es, abzuwägen, was zu tun ist, wenn diese verschiedene Interessen haben. Eine Erkennung der verschiedenen Personen wäre grundsätzlich ebenfalls durch den Mac-Adressen-Scanner möglich.

Wenn beispielsweise eine Person Home-Office macht und im Schlafzimmer sitzt, wo auch der gemeinsame Schreibtisch steht. Dort hat sie gerade eine wichtige Besprechung mit einem Kunden per Telefon. Deswegen hat

sie alle anderen Kameras und Mikrofone durch DAMA im Schlafzimmer deaktivieren lassen. Während ihres Calls kommt die zweite Person von der Arbeit nach Hause. DAMA weiß, dass diese, um sich vom Arbeitstag zu erholen, gerne Musik hört und aktiviert deshalb die Smart Speaker, als diese heimkommt.

Hier zu entscheiden, welche Präferenz bevorzugt werden soll, ist deutlich schwieriger und war Teil der dritten Umfrage unserer Evaluation.

5. Evaluation

Um sicherzustellen, dass die Funktionen des Prototyps die oben beschrieben Ziele erfüllen und um während der Entwicklung Perspektiven von Nutzer:innen einzubeziehen, haben wir im Projekt zu verschiedenen Zeitpunkten Nutzerbefragungen durchgeführt. Eine erste Umfrage zielte dabei darauf ab, generelle Präferenzen der Benutzer:innen zu identifizieren – also deren Vorwissen zu Privatsphäre abzuschätzen und einzuschätzen, ob geplante Funktionen angenommen werden. In der zweiten Umfrage ging es darum für die Automatisierung des Meta-Assistenten nützliche Gruppierungen der Geräte- und Komponentengruppen zu finden, die für eine sinnvolle Vorbelegung von Situations-Modi nützlich wären. In den abschließenden Experimenten haben wir anhand der Szenarien getestet, ob die Bedienung des Prototyps selbsterklärend ist und Nutzer:innen dadurch mehr Transparenz erfahren und Kontrolle über den Abfluss ihrer Daten ausüben können. Grundsätzlich lassen die Studien dabei auch Rückschlüsse auf die Nutzung smarter Geräte im Allgemeinen und die Präferenzen zur Privatsphäre zu.

5.1 Umfrage 1

Die erste Umfrage wurde als quantitative Erhebung mittels eines standardisierten Fragebogens durchgeführt. Sie bestand hauptsächlich aus Fragen mit einer 6-stufigen Likert-Skala, sowie einigen offenen Fragen und wurde mit dem Umfragetool Lime-Survey erstellt. Am Ende lagen von 607 Teilnehmenden auswertbare Fragebögen vor, die mittels deskriptiver und Inferenzstatistik mit dem Programm SPSS analysiert wurden. Die Ergebnisse sind:

- Die Befragten finden die Erhebung mit Kameras und Mikrofonen deutlich problematischer als die Erhebung von Meta-Daten (wie z. B. Nutzungsdaten von Steckdosen oder MAC-Scannern). Das zeigt, dass für Risiken durch die Übertragung solcher Daten ein zu niedriges Bewusstsein herrscht, trotz der in Kapitel 2 dargestellten Probleme.
- Insgesamt wünschen sich die Befragten, über Sensoren von Smart Home-Gegenständen informiert zu werden (bspw. ist für 94,05 % der Befragten eine Informierung über das Vorhandensein von Kameras wichtig).
- Kontrolle über die Sensoren auszuüben, ist den Befragten ebenfalls wichtig (83,89 % der Befragten ist die Möglichkeit zur Deaktivierung von Kameras wichtig).
- Je früher über Kameras, Mikrofone und weiteres informiert wird, desto besser wird dies bewertet (83,44 % der Befragten finden eine Informierung beim Betreten eines Smart-Homes für „eher gut" bis „sehr gut").
- Sie präferieren dabei, über Anzeigen informiert zu werden oder aber durch das eigene Smartphone, gegenüber Durchsagen. (84,55 % der Befragten befinden die Informierung via Displayanzeige „eher gut" bis „sehr gut", 69,03 % via Smartphone und nur 41,90 % per Durchsage).
- 85,38 % der Smart-Home Nutzer:innen halten einen Privacy-Meta-Assistenten für teilweise nützlich bis essenziell. Personen, die bereits Smart Home-Geräte benutzen, sind auch als Besucher:innen in der Tendenz eher bereit, gewisse Daten für DAMA bereitzustellen und Funktionen des Meta-Assistenten benutzen. Personen, die bisher keine Geräte benutzen, sind tendenziell eher skeptisch gegenüber dem Meta-Assistenten und ihre Daten stärker schützen zu wollen. Auch sehen sie die Automatisierung kritischer.
- Sowohl der Meta-Assistent als auch Smart Home-Geräte im Allgemeinen erzeugen bei einigen Befragten Skepsis. Hier muss es durch Transparenz und Optionalität der Funktionen gelingen, diese Bedenken auszuräumen. Deswegen ist es umso wichtiger zu reflektieren, wie Funktionen dargestellt werden und dass die grundlegende Funktion von DAMA auch ohne Automatisierung, sondern nur durch eine manuelle Bedienung funktionieren muss (Datensparsamkeit).

5.2 Umfrage 2

In einer weiteren Online-Umfrage standen Präferenzen von Nutzern bezüglich der Abschaltung bestimmter Komponenten und Geräte in bestimmten Situationen im Fokus. Hier wurden qualitative und quantitative Daten erfasst und ausgewertet. Durch Clustering-Verfahren sollte erforscht werden, ob es gewisse Patterns bei der Bewertung von Situationen in Zusammenhang mit Smart-Home Geräten und Komponenten gibt.

Die Ergebnisse unserer Online-Umfrage mit insgesamt 495 vollständig und sorgfältig (Bearbeitungszeit > 3 Minuten) ausgefüllten Fragebögen bestätigten die Relevanz von Situationsmodi bei Entscheidungen zur Deaktivierung von Gerätekomponenten.

Eine Gemeinsamkeit lag im Wunsch der Teilnehmenden, bestimmte Komponenten gemeinsam zu deaktivieren, insbesondere, wenn sie ähnliche Funktionen hatten, wie Mikrofon, Kamera oder Lautsprecher. Die Funktion ist dabei ausschlaggebender als das Gerät, in dem sie realisiert ist. Komponenten, die Bild und/oder Ton aufzeichnen, wurden dabei als potenziell größte Gefahr für die Privatsphäre eingeschätzt.

Ein Beispiel verdeutlicht diese Ergebnisse: Wenn Personen allein zu Hause waren, wollten 51,5 % in bestimmten Situationen mindestens die Sensoren (Mikrofone) des Smart-TV und des Sprachassistenten gemeinsam deaktivieren, weitere Funktionen aber gerne behalten.

Es zeigte sich zudem, dass mit zunehmender Ungewissheit der Situation der Wunsch nach Deaktivierung von Komponenten stärker ausgeprägt war, wie beispielsweise, wenn die Situation schwieriger zu bewerten ist, z. B. durch die Anwesenheit unbekannter Personen. Dies äußerte sich in einer Reduktion der Anzahl von Clustern und einer verbesserten Qualität des Clusterings. Der Wunsch, Sensor-Komponenten gemeinsam zu deaktivieren, war dann besonders ausgeprägt. Hier wäre eine granulare Steuerung von Gerätekomponenten gewünscht (z. B. nur die Mikrophone verschiedener Geräte temporär zu deaktivieren), was die meisten Hersteller solcher Geräte jedoch nicht unterstützen. Eine interessante Ausnahme bildete die Situation »Fremde zu Besuch im eigenen Smart-Home«, wo der Sicherheitswunsch überwog, und deshalb die im Smart-Home-Szenario vorhandene Kamera nicht deaktiviert werden sollte.

Insgesamt verdeutlichten diese Ergebnisse die Vielschichtigkeit der Entscheidungsprozesse im Zusammenhang mit der Deaktivierung von Gerätekomponenten und die Bedeutung einer differenzierten Betrachtung des Kontextes.

5.3 Umfrage 3

Bei der dritten Erhebung wurden User-Tests im Smart-Home Labor des Fraunhofer IAO durchgeführt, um die implementierten Funktionalitäten, Konzepte und Anwendungspotenzial von DAMA zu evaluieren. Dabei wurde stärker auf qualitative Methoden gesetzt. Insgesamt haben 13 Proband:innen an den Experimenten teilgenommen. Die Tests setzten sich dabei sowohl aus einem theoretischen Part als auch aus einem praktischen, interaktiven Part zusammen. Im interaktiven Part sollten die Versuchspersonen das System ohne vorherige Einweisung nutzen. Der Versuch an sich wurde mit der Thinking Aloud-Methode durchgeführt und mit Interviews und kurzen Fragebögen abgerundet.

Das Ergebnis der Versuche war, dass die Versuchspersonen durch DAMA besser informiert sind und beispielsweise Gefahren für den Datenschutz erkennen, die ihnen davor nicht bewusst waren. Die Bedingung des Meta-Assistenten gelang ihnen dabei meist intuitiv, und sie konnten für vorgegebene Situationen die vorhandenen Smart Home-Gegenstände und deren Sensoren so steuern, dass sie sich in der Umgebung wohlfühlten und ihre Privatheit verbessert war.

Im Rahmen der Experimente haben wir die Versuchspersonen befragt, wie sie sich in Konfliktsituationen entscheiden würden. Also Situationen, in denen sich mehrere Personen im Smart Home befinden und nicht übereinstimmen, welche Geräte und Sensoren deaktiviert werden sollen. In den vorgestellten Szenarien haben sich die Versuchspersonen überwiegend für die Option entschieden, die datenschutzsensibler ist, also dafür Geräte abzuschalten, auch wenn deren Verwendung von Personen in der Situation gewünscht wurde. Wenn zum Beispiel ein Gast sie als Bewohner:in bitten würde, Smart Home Geräte abzuschalten, würden dies 92 % der Versuchspersonen tun. Jedoch sind die Versuchspersonen dabei immer darum bemüht einen Kompromiss zu finden oder die andere Seite zu überzeugen, statt ihren Willen einfach durchzusetzen. Das heißt, hierfür ist eine technische Lösung nicht unbedingt die optimale Variante. Was der Assistent jedoch leisten kann, ist 1.) Die Personen erstmalig auf die Geräte hinzuweisen. 2.) Alle notwendigen Informationen für die Entscheidung geben. Auch wenn die letztendliche Kompromissfindung bei den Personen liegt, können diese durch DAMA die Basis für ihre informationelle Selbstbestimmung in solchen Situationen verbessern.

6. Schluss

Smarte Geräte und KI-basierte Assistenten werden in privaten sowie professionellen Umgebungen aktuellen Trends nach in Zukunft noch stärker als heute zum Einsatz kommen. Da Geräte- und Ökosystemhersteller wenig Transparenz und Kontrolle über die Sammlung der Daten ermöglichen und meist entgegengesetzte Interessen und Motive haben, wird so die Datenautonomie und Transparenz für die Benutzer:innen abnehmen und weitestgehend unkontrollierbar.

In diesem Paper stellten wir den Smart-Home Privacy-Assistenten »DAMA« in seiner aktuellen Ausprägung vor. Das System kann durch situative Erkennung des Kontextes und das Konzept der Situations-Modi semi-automatisch Sensoren und Aktoren in smarten Umgebungen dahingehend regulieren, dass eine erhöhte Transparenz für die Benutzer:innen erreicht wird, als auch eine Stärkung der Privatsphäre und Datenautonomie möglich wird. Es wurde ein funktionsfähiger Prototyp implementiert und seine Architektur und Funktionsweise dargestellt. Darüber hinaus wurde das System anhand der Ergebnisse mehrerer Nutzerstudien weiterentwickelt und evaluiert. Das System liefert so einen praktischen und Beitrag zur Stärkung der Datenautonomie in Umgebungen mit smarten Geräten und KI-basierten Assistenten. Die Nutzung der Geräte und Funktionen bleibt weiterhin gegeben und wird nur in vom Benutzer gewünschten Situationen temporär, feingranular und automatisch reguliert. Benutzer:innen, aber auch Gäste in smarten Umgebungen werden dabei durchgehend über die im Einsatz befindlichen Geräte und deren Satus aufgeklärt und können so wohlinformierte Entscheidungen treffen.

Danksagung

Wir danken ausdrücklich der Baden-Württemberg Stiftung für die finanzielle Unterstützung unserer Forschungsarbeit. Ihre fachliche und finanzielle Unterstützung war für den Erfolg des Projektes entscheidend.

Literatur

Brandt Mathias (7. Januar 2020): Wo Alexa und Co. im Einsatz sind. URL: https://de.statista.com/infografik/20414/orte-an-denen-smart-speaker-genutzt-werden/ (besucht am 19.6.2020).

Breithut Jörg (3. Januar 2020): Kamerabesitzer konnte in fremde Wohnungen schauen. *SPIEGEL Online* URL: https://www.spiegel.de/netzwelt/gadgets/xiaomi-kamera besitzer-sah-in-fremde-wohnungen-google-reagiert-a-1303518.html (besucht am 19.6.2020).

Bundesamt für Sicherheit in der Informationstechnik BSI (06 Mai 2022): IT-Sicherheitskennzeichen jetzt auch für smarte Verbraucherprodukte. Pressemitteilung. URL: https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220504_IT-SiK-Erweiterung.html (besucht am 8.8.2022).

BVerfGE 65, 1 - 71 - 1 BvR 209/83 -, Rn. 1-215.

Feldmeier Felix; Hermann, Maximilian; Kohou, Lukas; Lauenroth, Kim; Salomon, Gabriela; Thiel, Christian und Westermeier, Michael (2022): Neue Mehrwerte im Smart Home durch Daten. Berlin: BITKOM. URL: https://www.bitkom.org/sites/main/files/2022-09/220909_LF_Neue-Mehrwerte-im-Smart-Home-durch-Daten.pdf (besucht am 8.8.2022).

Ghiglieri, Marco; Hansen, Marit; Nebel, Maxi; Pörschke, Julia Victoria und Simo Fhom, Hervais (2016): Smart-TV und Privatheit: Bedrohungspotenziale und Handlungsmöglichkeiten. Forschungsbericht. Karlsruhe: Forum Privatheit und selbstbestimmtes Leben in der digitalen Welt. URL: https://plattform-privatheit.de/p-prv-wAssets/wp-content/uploads/Forschungsbericht-Smart-TV-und-Privatheit_Druckfassung-1.pdf (besucht am 11. Juni 2024)

Guhr, Nadine; Werth, Oliver; Blacha, Philip Peter Hermann und Breitner, Michael H. (2020): Privacy concerns in the smart home context. *SN Applied Sciences*, 2(2). doi: 10.1007/s42452-020-2025-8.

Hensen, Christian (2022): Saugroboter mit Kamera reinigte ihr Bad – danach landeten Bilder einer Frau auf der Toilette im Netz. *STERN.De*. URL: https://www.stern.de/digital/online/saugroboter-mit-kamera--bilder-einer-frau-auf-der-toilette-landeten-im-netz-33027364.html (besucht am 19.6.2020).

Hern, Alex (2019): 'Amazon staff listen to customers' Alexa recordings, report says: Staff review audio in effort to help AI-powered voice assistant respond to commands. *The Guardian*. URL: https://www.theguardian.com/technology/2019/apr/11/amazon-staff-listen-to-customers-alexa-recordings-report-says (besucht am 19.6.2020).

Jandt, Silke (2016): Informationelle Selbstbestimmung. In: Heesen, Jessica (Hrsg.): *Handbuch Medien- und Informationsethik*. Stuttgart: J.B.Metzler, S. 195-201. doi: 10.1007/978-3-476-05394-7_26.

Kröger, Jacob (2019): Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things. In: Strous, Leon und Cerf, Vinton (Hrsg.): *Internet of Things. Information Processing in an Increasingly Connected World. IFIPIoT 2018*. Cham: Springer, S. 147–159. doi: 10.1007/978-3-030-15651-0_13.

Lutz, Christoph und Newlands, Gemma (2021): Privacy and smart speakers: A multi-dimensional approach. *The Information Society,* 37(3), S. 147–162. doi: 10.1080/01972243.2021.1897914.

Marky, Karola; Prange, Sarah; Krell, Florian; Mühlhäuser, Max und Alt, Florian (2020): "You just can't know about everything": Privacy Perceptions of Smart Home Visitors. In: Cauchard, Jessica und Löchtefeld, Markus (Hrsg.): *MUM 2020: Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia*. New York: ACM Press, S. 83–95. doi: 10.1145/3428361.3428464.

Moltrecht, Klaas und Schnaack, Greta (2022): Das intelligente Zuhause: Smart Home 2022. Ein Bitkom-Studienbericht. Berlin: BITKOM. URL: https://www.bitkom.org/sites/main/files/2022-09/220912_Bitkom_Smart_Home_Chartbericht_2022_final.pdf (besucht am 19.6.2020).

Mühlhoff, Rainer (2020): Prädiktive Privatheit: Warum wir alle „etwas zu verbergen haben". In: *KI als Laboratorium? Ethik als Aufgabe!* Berlin: Berlin-Brandenburgische Akademie der Wissenschaften, S. 38–45. URL: https://www.bbaw.de/files-bbaw/user_upload/publikationen/BBAW_Verantwortung-KI-3-2020_PDF-A-1b.pdf (besucht am 19.6.2020).

Rajkumar, Ragunathan; Lee, Insup; Sha, Lui and Stankovic, John (2010): Cyber Physical Systems: The Next Computing Revolution. In: *DAC '10: Proceedings of the 47th Design Automation Conference*. New York: ACM Press, S. 731-736. doi: 10.1145/1837274.1837461.

Sheridan, Kelly (2019): Consumers Care About Privacy, but Not Enough to Act on It. *DarkReading*. URL: https://www.darkreading.com/threat-intelligence/consumers-care-about-privacy-but-not-enough-to-act-on-it (besucht am 01.02.2024).

Wachter, Sandra (2018): Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR. *Computer Law & Security Review*, 34 (3), S. 436-449. doi: 10.2139/ssrn.3083554.

Standard Health Consent – Ein partizipativer Einwilligungsmanagment-Ansatz für die Nutzung von Gesundheitsdaten aus Apps und Wearables

Stefanie Brückner, F. Gerrik Verhees, Peter Schwarz, Andrea Pfennig, Stephen Gilbert

Zusammenfassung

Gesundheits-Apps und Wearables erfreuen sich immer größerer Beliebtheit. Über Sensorenmessungen und manuelle Einträge können Menschen so einfach eine Vielzahl gesundheitsrelevanter Parameter in ihrem Alltag aufzeichnen. In diesen Daten stecken wichtige Informationen nicht nur für die eigene Gesundheitsversorgung, sondern auch für die Sekundärnutzung wie beispielsweise für die medizinische Forschung. Das Potenzial ist erkannt und Initiativen zu einer gemeinsamen Nutzung von Gesundheitsdaten, wie der Europäische Gesundheitsdatenraum, sollen neben den klassischen klinischen Gesundheitsdaten auch die aus Apps und Wearables berücksichtigen. Der bisherige Entwurf lässt jedoch offen, wie Bürger:innen die Kontrolle über die Weitergabe ihrer Daten ausüben können. Wir beschreiben einen neuen, standardisierten Ansatz für die Einholung und Verwaltung von Einwilligungen für das Teilen von Gesundheitsdaten aus Apps und Wearables, den Standard Health Consent. Die digitale Standard Health Consent-Plattform könnte Bürger:innen die Kontrolle über die Verwendung ihrer Gesundheitsdaten geben und zu der Entwicklung eines fairen und vertrauenswürdigen Gesundheitsdatenökosystems beitragen. In einer ersten Pilotumfrage mit Ärzt:innen werden die Meinungen dieser Fachgruppe zu von Patient:innen digital selbst erfassten Gesundheitsdaten sowie digitalem Einwilligungsmanagement erfasst.

1. Die digitale Vermessung der Gesundheit

Die Gesundheitssysteme der OECD-Staaten stehen unter einem hohen Druck, der sich aus der Kombination einer immer älter werdenden Bevölkerung, dem starken Anstieg an lebensstil- und umweltbedingten chro-

nischen Erkrankungen sowie einem wachsenden Fachkräftemangel in Gesundheits- und Sozialberufen ergibt.[1] Die Komplexität dieser Problemlage erfordert vielfältige Lösungsansätze, wobei besonders hohe Erwartungen in die Digitalisierung der Gesundheitsversorgung gesetzt werden. Mit dem Einsatz von Informationstechnologie und innovativen Tools wie Gesundheits-Apps, Telemedizinservices oder Künstlicher Intelligenz soll eine zeitgemäße und datenbasierte Gesundheitsversorgung etabliert werden. In einem digitalisierten Gesundheitssystem nehmen Daten eine Schlüsselrolle ein.

Bisher waren Gesundheitsdaten auf klinische Informationen beschränkt, die in den Praxen, Krankenhäusern und Laboren erhoben und dokumentiert wurden, wie z. B. Laborergebnisse, medizinische Diagnosen und Medikamentenverordnungen. Mit dem Aufkommen und der rasanten Verbreitung von Smartphones und Wearables können Menschen heute selbstständig eine Vielzahl gesundheitsbezogener Parameter in ihrem Alltag aufzeichnen (Abb. 1). Dies geschieht über manuelle Einträge in Apps (z.B. Symptomtagebücher, Medikamenteneinnahme) oder über Messungen mit eingebauten Sensoren (z.B. Herzfrequenz, Blutzucker).

Gesundheits-Apps und Wearables bilden eine heterogene Gruppe, die man grob in zwei große Kategorien unterteilen kann.[2] Auf der einen Seite stehen die CE-pflichtigen Gesundheits-Apps, die unter das Medizinproduktegesetz fallen und für spezifische medizinische Anwendungsfälle entwickelt wurden. Diese Apps müssen die Anforderungen der Medizinprodukteverordnung erfüllen und sind damit reguliert. In mehreren EU-Ländern, darunter Deutschland, Belgien und Frankreich, wurden spezielle Erstattungssysteme für Gesundheits-Apps eingeführt, da man ihren Nutzen erkannt hat, und ihre Integration ins Versorgungssystem erleichtern will.[3] Um sich in Deutschland für den Erstattungsweg "App auf Rezept" zu qualifizieren, müssen App-Hersteller spezifische Standards bei Sicherheit, Funktionalität, Datenschutz und Interoperabilität erfüllen. Außerdem müssen die Apps einen entsprechenden medizinischen Nutzen oder patienten-

1 *OECD*, Health at a Glance 2023 2023; *Robert Koch-Institut*, Gesundheit in Deutschland 2015; *PwC Deutschland*, Fachkräftemangel im Gesundheitswesen: Wenn die Pflege selbst zum Pflegefall wird.

2 *Sadare u. a.*, Can Apple and Google continue as health app gatekeepers as well as distributors and developers?, Npj Digit. Med. 2023, 1.

3 *van Kessel u. a.*, Digital Health Reimbursement Strategies of 8 European Countries and Israel: Scoping Review and Policy Mapping, JMIR MHealth UHealth 2023, e49003.

Abbildung 1: Beispiele von Patient:innen selbst erfassten Gesundheitsdaten aus Apps und Wearables sowie mögliche Nutzungsszenarien.

relevante Struktur- und Verfahrensverbesserungen nachweisen.[4] Die zweite Kategorie an Gesundheits-Apps sind die Lifestyle- und Wellness-Apps, die nicht für einen spezifischen medizinischen Anwendungsfall entwickelt wurden und keine CE-Zertifizierung brauchen. Entsprechend sind diese Apps unreguliert und nicht kontrolliert.

Gesundheits-Apps und Wearables erweitern das Gesundheitssystem und lassen die Gesundheitsversorgung heute mit dem Smartphone in der Hosentasche oder dem Smart Ring am Finger beginnen. Sie bieten den Anwender:innen eine Vielzahl an Funktionen fürs eigene Gesundheitsmanagement, wie beispielsweise personalisierte Gesundheitsinformationen, Erinnerungsfunktionen, Trainingspläne zum Erreichen von Gesundheitszielen sowie das Aufzeichnen und Überwachen gesundheitsbezogener Parameter.[5] In der Interaktion mit den Apps und Wearbles werden wertvolle und detaillierte Verlaufs- und Echtzeitdaten gesammelt, die vollkommen neue Einblicke in den Gesundheits- und Krankheitszustand eines Men-

4 DiGAV - Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung, abrufbar unter https://www.gesetze-im-internet.de/digav/BJNR076800020.html.

5 *Mendiola u. a.,* Valuable Features in Mobile Health Apps for Patients and Consumers: Content Analysis of Apps and User Rating, JMIR MHealth UHealth 2015.

schen geben. Von Patient:innen auf diese Weise selbst erfasste Gesundheitsdaten sind kritische Informationen für die eigene Versorgung, da sie Prävention, Diagnostik und Therapie verbessern können und personalisierte Medizin ermöglichen.[6] So können beispielsweise Menschen mit Diabetes mellitus über digitale Diabetes-Management-Tools und kontinuierliches Blutzuckermonitoring engmaschig Informationen zu Krankheitsverlauf und Lebensstil aufzeichnen. Diese Daten sind weitaus detaillierter und umfassender als sie jemals während der Besuche bei den entsprechenden Ärzt:innen protokolliert werden könnten. Zugang und Analyse dieser Daten sind die Grundlage, um aus den Informationen individuelle Beratungen zu Lebensstiländerungen oder auch Therapieanpassungen vornehmen zu können.[7] Auch für den Bereich Mental Health stecken in den von Patient:innen digital selbst erfassten Gesundheitsdaten große Potenziale: Von Smartwatches aufgezeichnete Herzfrequenz- and Atemfrequenzdaten liefern wichtige Informationen zu Stresserfahrungen und können beispielsweise beim Stressmanagement am Arbeitsplatz eingesetzt werden.[8] Außerdem könnten Fitnesstracker u.a. bei der Therapie von Posttraumatischen Belastungsstörungen helfen, die von Patient:innen und Ärzt:innen festgesetzten Gesundheitsziele zu überwachen und anzupassen.[9] Wie in klassischen, nicht-digitalen Therapieansätzen spielt auch bei Gesundheits-Apps die Patientencompliance eine zentrale Rolle. Denn um den vollen Nutzen der Anwendungen zu erfahren, müssen Patient:innen diese langfristig und konsequent nutzen, was bisher noch eine Herausforderung darstellt.[10]

Auch außerhalb der Patientenversorgung, in der sogenannten Sekundärnutzung von Gesundheitsdaten, sind die Daten aus Apps und Wearables von großer Bedeutung. In diesen Bereich fallen viele Anwendungsszenarien, darunter medizinische Forschung, Public Health Monitoring, Entwicklung von Medizinprodukten und Politikgestaltung. Die Verbindung

6 *Jim u. a.*,Innovations in research and clinical care using patient-generated health data, CA. Cancer J. Clin. 2020.

7 *Nagpal u. a.*, Patient-Generated Data Analytics of Health Behaviors of People Living With Type 2 Diabetes: Scoping Review, JMIR Diabetes 2021, e29027.

8 *Lucas u. a.*, Sex differences in heart rate responses to occupational stress, Stress 2020, 13.

9 *Saleem u. a.*, Veteran and Staff Experience from a Pilot Program of Health Care System–Distributed Wearable Devices and Data Sharing, Appl. Clin. Inform. 2022, 532.

10 Vaghefi/Tulu, The continued use of mobile health apps: insights from a longitudinal study, JMIR MHealth UHealth 2019.

von Datensätzen unterschiedlicher Herkunft schafft hier neue Erkenntnisse und Potenziale. So konnten beispielsweise während der Corona-Pandemie durch "Datenspenden", d.h. über eine auf Einwilligung basierende, freiwillige Freigabe von Daten aus Fitnesstrackern, in Forschungsprojekten in Deutschland und Großbritannien Erkenntnisse zu Krankheitsverläufen und zum Pandemiegeschehen gewonnen werden.[11]

Egal ob für Patientenversorgung oder für die Sekundärnutzung, um Gesundheitsdaten aus Apps und Wearables verwertbar zu machen, werden die parallelen rasanten Fortschritte in der Entwicklung und dem Einsatz Künstlicher Intelligenz, wie z.B. Deep Learning oder Foundational Models, eine wichtige Rolle spielen.[12] Mithilfe dieser Algorithmen können große Mengen an Daten aus verschiedenen Quellen gesammelt, aufgearbeitet und analysiert werden.

2. Die Zukunft der Gesundheitsdatennutzung: Kontroverse um die Einwilligungsfrage beim Europäischen Gesundheitsdatenraum

Geprägt von den Erfahrungen aus der Corona-Pandemie, in denen der Zugriff - oder eben der fehlende - auf Echtzeit-Gesundheitsdaten der Bevölkerung wichtig war, wurde im Mai 2022 der erste Entwurf zum Europäischen Gesundheitsdatenraum (European Health Data Space, EHDS) vorgelegt.[13] Diese regulatorische Initiative hat den Anspruch, EU-weit einheitliche Rahmenbedingungen mit klaren Regeln, Standards, Verfahren, Infrastruktur und Data Governance für die gemeinsame Nutzung von Gesundheitsdaten zu schaffen. Zum einen sollen Gesundheitsdaten für die Patientenversorgung für Bürger:innen und Behandler:innen besser zugänglich sein. Zum anderen soll auf diese Weise auch die Sekundärnutzung durch Wissenschaft und Industrie sowie Politik und Regulatorik zum Zwecke des Gemeinwohls ermöglicht werden. Erstmals werden dabei neben den traditionellen klinischen Gesundheitsdaten auch die Daten von Apps und Wearables aufgeführt. Ein Aspekt im Entwurf zum EHDS hat dabei eine große Debatte ausgelöst: Der derzeitige Entwurf sieht keine Kontrollmechanismen für Bür-

11 *Menni u. a.*, Real-time tracking of self-reported symptoms to predict potential COVID-19, Nat. Med. 2020, 1037.

12 *Howell u. a.,* Three Epochs of Artificial Intelligence in Health Care*, JAMA 2024, 242.*

13 Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space.

ger:innen bei der Weitergabe von anonymisierten bzw. pseudonymisierten Gesundheitsdaten aus den elektronischen Patientenakten der Patient:innen vor. Dieses Vorgehen ist von der Europäischen Datenschutzgrundversorgung gestattet, die eine Weitergabe entpersonalisierter Gesundheitsdaten unter bestimmten Bedingungen erlaubt.[14] Für den EHDS werden dazu auf nationaler Ebene Zugangsstellen geschaffen, die über Anträge zu Datenanfragen basierend auf dem Forschungszweck und nicht dem Antragsteller entscheiden. Studien haben gezeigt, dass viele Menschen grundsätzlich auch bereit sind, ihre Gesundheitsdaten für Forschungszwecke zu teilen.[15] Diese Bereitschaft hängt jedoch davon ab, dass die Menschen entscheiden können, welche Daten mit wem geteilt werden und ob es Transparenz bezüglich der Datenempfänger gibt. Während die Teilungsbereitschaft für Forschungsprojekte von Gesundheitsfachkräften oder öffentlichen Gesundheitseinrichtungen hoch ist (71% bzw. 53%), finden privatwirtschaftlich geleitete Projekte (z.B. von Pharma- oder Medizintechnologie-Unternehmen) nur geringe Unterstützung (>=17%).[16] Wird die Bevölkerung nicht aktiv in die Aushandlungen der Bedingungen von Datennutzungsprogrammen einbezogen, kann dies zu Ablehnung und Misstrauen führen, wie die fehlgeschlagene Strategie zum Datennutzungsprogramm *care.data* des National Health Service NHS in Großbritannien gezeigt hat.[17] Dass eine Sekundärnutzung traditioneller Gesundheitsdaten ohne Patienteneinwilligung aufgesetzt werden kann, wird unter anderem damit begründet, dass Gesundheitsdaten in einem solidarisch finanzierten Gesundheitssystem als Gemeingut klassifiziert werden können und somit für Zwecke des Gemeinwohls verwendbar sein sollten.[18] Da die Smartphones und Fitnesstracker, über die Bürger:innen und Patient:innen in ihrem Alltag in eigener Motivation Gesundheitsdaten sammeln, eigenfinanziert werden, gilt dieses Argument nicht. Zudem lassen die sensiblen Informationen tiefgreifende

14 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) (Text von Bedeutung für den EWR).

15 *Buhr u. a.*, Attitudes Toward Mobile Apps for Pandemic Research Among Smartphone Users in Germany: National Survey, JMIR MHealth UHealth 2022, e31857; *Weisband u. a.*, GIHF-AI Study 2023.

16 *BEUC*, Consumer attitudes to health data sharing.

17 *Mundasad*, NHS data-sharing project scrapped.

18 *Mills/Miller*, Why we need a new social contract for data in healthcare, abrufbar unter https://www.weforum.org/agenda/2019/03/why-we-need-a-new-social-contract-for-data-in-healthcare/.

Schlüsse nicht nur über die Lebenssituation, Verhaltensmuster, sexuelle und religiöse Orientierungen der Person zu, die die App benutzt, sondern auch über Menschen, mit denen sie interagiert. Es ist fraglich, wie man Menschen dazu bewegen kann, solche sensiblen Daten in die elektronische Patientenakte zu laden, wenn sie danach nicht mehr über die weitere Verwendung mitentscheiden können. Diese Problemsituation wurde auch vom Europäischen Datenschutzausschuss (European Data Protection Board, EDPB) benannt, und in einer Stellungnahme wird gefordert, die Sekundärnutzung der Daten aus Apps und Wearables ausschließlich nach Informed Consent zu erlauben.[19] Letztlich besteht zudem ein Restrisiko zur Re-Identifizierung von Personen, da die Pseudonymisierung im Hintergrund von sich rasant weiterentwickelnden Methoden der Künstliche Intelligenz und des Machine Learning keinen vollkommenen Schutz bieten kann.[20] Aus all den genannten Gründen braucht es für die Nutzung von Gesundheitsdaten aus Apps und Wearables einen neuen Gesellschaftsvertrag, der auf Einwilligung und Transparenz basiert.[21]

Es gibt auch Kritiker, die den grundsätzlichen Nutzen von Daten aus Apps und Wearables anzweifeln. Dies wird vor allem mit einer mangelnden Qualität, Validität und Interoperabilität der Daten begründet. Gerade das Thema Interoperabilität ist ein Problem, das auch klinische Versorgungsdaten betrifft und zweifelsohne konsequent angegangen werden muss. Als besonders hilfreich wird sich auch hier der Einsatz von künstlicher Intelligenz, wie beispielsweise Deep Learning oder Foundational Models, erweisen.[22] Sie können große Mengen von Daten prozessieren und für die Verarbeitung zugänglich machen, und sie können auch für Qualitäts-Checks eingesetzt werden, um fehlerhafte bzw. inkonsistente Daten zu markieren.

Es bleibt zu hoffen, dass die fehlenden Kontrollmechanismen über die Sekundärnutzung von Gesundheitsdaten aus Apps und Wearables in der nächsten Entwurfsversion zum EHDS angegangen werden und nicht zum Ausschluss der Daten aus der Initiative führen. Würde diesen Problemen

19 *EDPB-EDPS*, EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space | European Data Protection Board, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en.

20 *Rocher u. a.*, Estimating the success of re-identifications in incomplete datasets using generative models, Nat. Commun. 2019, 3069.

21 *Mills/Miller*, [Fn., 18].

22 *Howell u. a.*, [Fn., 12].

adäquat begegnet, würde der EHDS seinem Anspruch gerecht, ein nachhaltiges Gesundheitsdatenökosystem für alle Beteiligten zu schaffen.[23]

3. Ein standardisierter Einwilligungsansatz für das Teilen von Gesundheitsdaten

Wie könnte ein Kontrollsystem für das Teilen von Gesundheitsdaten aus Apps und Wearables aussehen, das auf Einwilligung beruht und Bürger:innen transparente Informationen über die Nutzung von Gesundheitsdaten bietet? Im folgenden Abschnitt beschreiben die Autor:innen den Ansatz für ein standardisiertes, zentrales System für das Einholen und Verwalten von Einwilligungen zum Teilen von Gesundheitsdaten aus Apps und Wearables, der Standard Health Consent.[24] Das hier beschriebene Konzept zum Standard Health Consent wurde im Rahmen des interdisziplinären Forschungsprojekts PATH „Personal Mastery Health & Wellness Data" unter der Leitung der Technischen Universität Dresden entwickelt.[25] Forschungsschwerpunkt des Projekts sind die Untersuchung unterschiedlicher Ansätze zur Nutzung von Gesundheitsdaten aus Apps und Wearables und die damit verbundenen Einwilligungsverfahren. Über Interviews, Umfragen und Fokusgruppenarbeit werden von Beginn an die Bedürfnisse und Erwartungen der verschiedenen Stakeholdergruppen (vor allem der Bürger:innen und Patient:innen, aber auch der Gesundheitsfachkräfte und Digital Health Industrie) erfasst und in einem iterativen Prozess in die Konzepte, Interface-Designs und funktionale Prototypen der Standard Health Consent-Plattform übersetzt. Die entwickelten Prototypen werden mit den Nutzergruppen getestet und sollen am Ende des Projekts als Open-Source-Module veröffentlicht werden. Weiterhin sollen Optionen für die Nachverfolgung von Einwilligungen sowie Möglichkeiten zur Verbindung mit Datentreuhänder untersucht werden. In Abschnitt 3 werden erste Ergebnisse einer kleinen Pilotstudie mit Ärztinnen vorgestellt, die zu Gesundheitsdaten aus Apps und Wearables sowie digitalem Einwilligungsmanagment befragt wurden.

---

23 *Gilbert u. a.*, Citizen data sovereignty is key to wearables and wellness data reuse for the common good, Npj Digit. Med. 2024, 1.

24 *Brückner u. a.*, The Social Contract for Health and Wellness Data Sharing Needs a Trusted Standardized Consent, Mayo Clin. Proc. Digit. Health 2023, 527.

25 *Brückner u. a.*, [Fn. 25], 527; PATH — Vernetzung und Sicherheit digitaler Systeme, abrufbar unter https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/path-1.

Die Standard Health Consent setzt sich aus einem Cockpit zum Verwalten von Einwilligungsoptionen sowie standardisierten Prozessen zur Einholung der Zustimmung zusammen. Über die Plattform können Nutzer:innen ein persönliches Standard Health Consent-Profil erstellen und dieses mit Gesundheits-Apps verknüpfen, sofern diese den Standard Health Consent unterstützen. Im Profil können Nutzer:innen festlegen, welche Gesundheitsdaten sie für welche Verwendungszwecke freigegeben oder beschränken wollen. Der Standard Health Consent greift auf bekannte Formen der Patienteneinwilligung in der medizinischen Forschung zurück, darunter Broad Consent, Dynamic Consent und Meta-Consent. Broad Consent ist das zentrale Element vieler Forschungsinitiativen, wie beispielsweise in Biobanks oder auch der Medizin-Informatik-Initiative, bei dem die Patienteneinwilligung nicht an einen spezifischen Verwendungszweck gebunden ist und Forschende somit ein höheres Maß an Flexibilität haben, die gesammelten Patientendaten/-proben in zukünftigen Forschungsprojekten einsetzen zu dürfen.[26] Die Übertragbarkeit des Ansatz für eine breite Einwilligung in die Sekundärnutzung von Gesundheitsdaten aus Apps und Wearables ist bislang rechtswissenschaftlich nicht erörtert und Forschungsgegenstand der Projekts PATH. Dynamic Consent ermöglicht es Patient:innen, ihre Einwilligungen kontinuierlich über eine digitale Plattform zu überprüfen und zu ändern.[27] Meta-Consent baut auf den genannten Konzepten auf, wobei Patient:innen über eine digitale Plattform ihre Consent-Präferenzen für spezifische Datentypen und Forschungszwecke vorab festlegen.[28] Der Standard Health Consent für das Teilen von Gesundheitsdaten aus Apps und Wearables vereint Elemente dieser Konzepte in einer einzigen standardisierten Plattform und befähigt so die Bürger:innen zur Souveränität über ihre Daten. Die Interaktion mit dem Standard Health Consent kann über drei Wege erfolgen: a) über die Website/App von Krankenkassen oder die elektronische Patientenakte, b) über Tablets/Terminals

26 *Zenker u. a.*, Data protection-compliant broad consent for secondary use of health care data and human biosamples for (bio)medical research: Towards a new German national standard, J. Biomed. Inform. 2022, 104096; *Stein/Terry*, Reforming Biobank Consent Policy: A Necessary Move Away from Broad Consent Toward Dynamic Consent, Genet. Test. Mol. Biomark. 2013, 855.

27 *Kaye u. a.*, Dynamic consent: a patient interface for twenty-first century research networks, Eur. J. Hum. Genet. 2015, 141.

28 *Ploug/Holm*, Meta consent: a flexible and autonomous way of obtaining informed consent for secondary research, BMJ 2015, h2146.

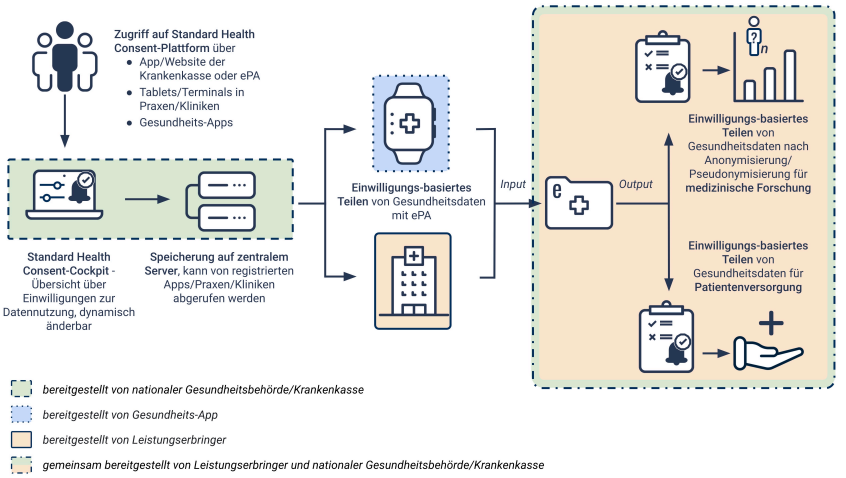

Abbildung 2: Interaktion zwischen Bürger:innen und der Standard Health Consent-Plattform; Einwilligung für das Teilen von Gesundheitsdaten mit der elektronischen Patientenakte (Input) und für die die Nutzung der Gesundheitsdaten für die eigene Versorgung oder medizinische Forschung (Output).

in Praxen und Kliniken oder c) über Gesundheits-Apps/Wearables, die die Standard Health Consent-Plattform unterstützen (Abb.2).

Nach einem ausführlichen, standardisierten Aufklärungsprozess, der in verständlicher Sprache über die Vorteile und Risiken der Gesundheitsdatennutzung informiert, können Bürger:innen ihre Präferenzen zum Teilen ihrer Daten mit der eigenen elektronischen Patientenakte, Gesundheitseinrichtungen und für die Sekundärnutzung in ihrem persönlichen Profil speichern und jederzeit über das Consent-Cockpit einsehen und dynamisch ändern. Teil des Forschungsprojekts ist die Untersuchung von neuen Methoden für Informed Consent, um die Verständlichkeit für die Nutzer:innen zu erhöhen. Dafür werden unterschiedliche Text- und Graphik-gestützte Aufklärungselemente mit Nutzergruppen getestet. Neue Gesundheits-Apps, die das Standard Health Consent-System unterstützen, können von den Bürger:innen mit dem eigenen Profil verbunden und die allgemeinen Consent-Settings importiert werden (Abb. 3). Somit müssen Nutzer:innen nur einmalig ihre Einwilligungspräferenzen festlegen. Individuelle Änderungen für neue Apps können aber jederzeit vorgenommen werden. Die Standard Health Consent-Plattform kann auch als Kommu-

nikationskanal dienen, über den im Verlauf einer Sekundärdatennutzung Informationen zu Datennutzer und zu relevanten Forschungsergebnissen geteilt werden können. Transparente Kommunikation kann ein wichtiger Hebel sein, um Vertrauen zu bilden und die Bereitschaft zum Teilen von Gesundheitsdaten zu steigern.[29]

Obschon für den der Nutzung vorausgehenden Prozess von Einführung und Aufklärung noch keine Position existiert und diese Verantwortung bei beständig knappen Ressourcen des Fachpersonals im Gesundheitswesen einer Aushandlung bedarf, könnte der Standard Health Consent Chancen für alle Stakeholder bieten: Bürger:innen würden über einen ausführlichen, standardisierten Prozess zur Einholung der Einwilligung, der für Verständnis und Einfachheit optimiert ist, neutral über Nutzen und Risiken beim Teilen von Gesundheitsdaten aufgeklärt und aktiv Kontrolle über ihre Datennutzung ausüben. Studien haben gezeigt, dass die Bereitschaft zum Teilen von Gesundheitsdaten für die Sekundärnutzung von verschiedenen Faktoren abhängt, darunter, (a) dass Bürger:innen (oder Patient:innen) über Vorteile, Risiken und Prozesse bei der Datennutzung aufgeklärt werden; (b) dass sie Wahlmöglichkeiten darüber haben, welche Daten sie mit welchen Empfänger für welche Zwecke teilen; (c) Einwilligungen widerrufen werden können und (d) Informationen darüber erhalten, zu welchen Forschungsergebnisse ihre Daten beigetragen haben.[30] Diese Erkenntnisse werden in der Entwicklung von Funktionalitäten und Eigenschaften der Standard Health Consent-Plattform berücksichtigt und in zukünftigen Nutzerstudien mit Bürger:innen und Patient:innen getestet.

Auch für Ärzt:innen und Akteure der Sekundärnutzung würde der Einsatz eines standardisierten Einwilligungsmanagement-Systems Vorteile bringen. Sie könnten darauf vertrauen, dass Daten, die über die Standard Health Consent-Plattform geteilt werden, sicher genutzt werden können, wie es schon seit langem in internationalen medizinischen Leitlinien beispielsweise von der *American Diabetes Association* (ADA) und der *European Association for the Study of Diabetes* (EASD) gefordert wird.[31]

29 *Baines u. a.*, Patient and Public Willingness to Share Personal Health Data for Third-Party or Secondary Uses: Systematic Review, J. Med. Internet Res. 2024

30 *Baines u. a.*, [Fn. 30].

31 *Davies u. a.*, Management of hyperglycaemia in type 2 diabetes, 2022. A consensus report by the American Diabetes Association (ADA) and the European Association for the Study of Diabetes (EASD), Diabetologia 2022, 1925.

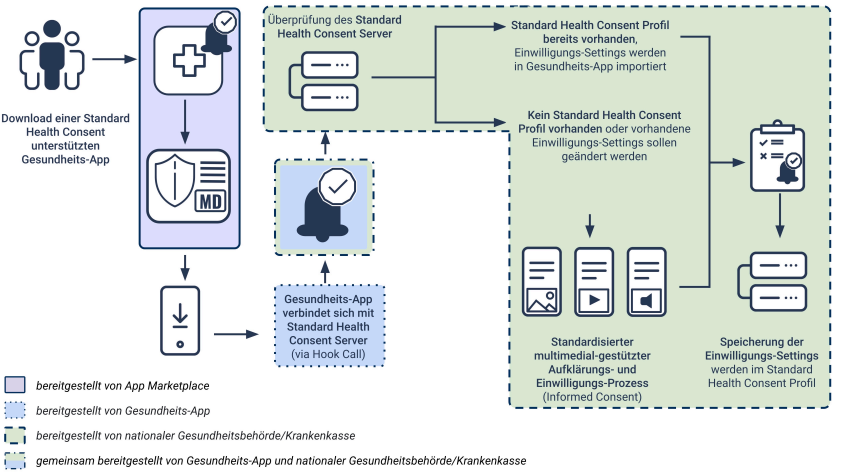

Abbildung 3: Download und Verknüpfung einer Standard Health Consent-gestützten Gesundheits-App mit dem persönlichen Standard Health Consent-Profil. Ist bereits ein Standard Health Consent-Profil angelegt, können Nutzer:innen ihre Einstellungen für das Teilen von Gesundheitsdaten direkt auf die neue Gesundheits-App übertragen. Wenn dies die erste Interaktion mit dem Standard Health Consent ist, erhalten Nutzer:innen die Möglichkeit ein eigenes Standard Health Consent-Profil anzulegen. Anschließend werden sie durch einen standardisierten Einwilligungsprozess geführt, der über die Datennutzung, Vorteile, Risiken und Verfahren aufklärt. Nutzer:innen können dann ihre Präferenzen für die Datennutzung festlegen. Im persönlichen Standard Health Consent-Profil können jederzeit die Einwilligungen eingesehen, überprüft und geändert werden. Auch verknüpfte Apps können überprüft und bearbeitet werden.

Ein solches Einwilligungssystem könnte als Voraussetzung für Apps und Wearables eingeführt werden, um am Datenaustausch über den EHDS teilnehmen zu können. Der derzeitige EHDS-Entwurf sieht bereits Zulassungsverfahren für EHDS-interoperable Apps vor, die Ausgestaltung ist jedoch unklar.[32] Damit könnte die Implementierung des Standard Health

32 [Fn. 14].

Consent zu einem Qualitätsmerkmal für die Apps und Wearables werden, was ein Vorteil in einem hochkompetitiven Markt sein kann. Ohne einen entsprechenden regulatorischen Druck ist jedoch nicht davon auszugehen, dass sich eine solche Initiative für eine von Bürger:innen kontrollierte Datenweitergabe durch die Industrie entwickelt, da viele App- und Wearable-Anbieter aus dem Bereich der Konsumertechnologie einen Datenverkauf als Business-Modell haben. Das bedeutet, dass es für die Umsetzung, Koordination und Aufsicht des Standard Health Consent nationale oder EU-Behörden bzw. Institutionen bedarf.

4. Die Rolle der Ärzt:innen

Ärzt:innen und Therapeut:innen genießen ein großes Vertrauen seitens ihrer Patient:innen.[33] Damit haben die medizinischen Fachkräften eine besonders wichtige Rolle, Patient:innen über die Nutzung von Gesundheitsdaten für die eigene Behandlung aber auch die Sekundärnutzung aufzuklären. Vor allem mit Blick auf die elektronische Patientenakte, die ab 2025 für alle gesetzlich Versicherten in Deutschland mit Möglichkeit zum Opt-out bereitgestellt wird, wird es großen Informationsbedarf geben.[34] Über entsprechende Schnittstellen soll diese auch Daten aus Wearables und deren Apps importieren können.[35] Während Prozesse der Einwilligung von Patient:innen in klassische medizinische Behandlungen wie Operationen oder invasive diagnostische Verfahren klar standardisiert und aus der Erfahrung der Aufklärenden in der Durchführung der beschriebenen Eingriffe heraus erfolgen, stellt die digitale Welt eine ungleich komplexere Aufgabe. Digitale Technologien mit rasanten Produktweiterentwicklungen, Datenschutz- und Cybersecurity-Fragen sowie vielfältige Datennutzungsszenarien erfordern neue Fähigkeiten und Wissen, um Patient:innen adäquat aufzuklären. Da Ärzt:innen hier aufgrund der beschriebenen Dynamik der Entwicklungs-

33 *Ärzteblatt*, Ärzte genießen größtes Vertrauen, Politikverdrossenheit sichtbar, abrufbar unter https://www.aerzteblatt.de/nachrichten/148387/Aerzte-geniessen-groesstes-Vertrauen-Politikverdrossenheit-sichtbar.

34 *Bundesministerium für Gesundheit*, Digitalgesetze im Bundestag beschlossen, abrufbar unter https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/bundestag-verabschiedet-digitalgesetze-pm-14-12-23.

35 *Ärzteblatt*, Ampel will Befüllungspflichten bei elektronischer Patientenakte ausweiten, abrufbar unter https://www.aerzteblatt.de/nachrichten/147972/Ampel-will-Befuellungspflichten-bei-elektronischer-Patientenakte-ausweiten.

prozesse kaum auf dem notwendigen, aktuellsten Erfahrungsstand bleiben können, wäre im Status Quo zu befürchten, dass klassische Aufklärungsverfahren im digitalen Raum noch weniger effektiv sein dürften, als bereits jetzt zu befürchten ist.[36] In der Aus- und Weiterbildung von Gesundheitsfachkräften sollten diese Themen zentral verankert werden, damit sie ihre wichtige Rolle als Berater:in ihrer Patient:innen weiterhin wahrnehmen können. So sollten beispielsweise evidenzbasierte digitale Therapeutika bei entsprechender Indikation genauso sicher verordnet und pflegerisch begleitet werden können wie klassische Pharmazeutika. Die Komplexität digitaler Technologien und ihres Einsatzes wird hier jedoch nicht allein von Ärzt:innen abgedeckt werden können. Eine weitere Möglichkeit wäre die Schaffung einer neuen Rolle im Gesundheitssystem. Eine Fachkraft, ausgestattet mit hohem Grad an digitalen Kompetenzen, könnte in den Praxen oder auch remote über Tele-Services Patient:innen beim Umgang mit digitalen Tools, wie beispielsweise digitalen Systemen zum Einwilligungsmanagement, unterstützen.

In einem langjährigen Prozess entwickelten sich das Selbstbild vieler Ärzt:innen und der Standard-Ansatz der Entscheidungsfindung moderner Therapien zunehmend weg vom im 20. Jahrhundert üblichen paternalistischen Entscheidungsmodell, in dem insbesondere Ärzt:innen als Expert:innen über die (vermeintlich) richtige Behandlung mit wenig Beteiligung der Patient:innen entscheiden, hin zum Paradigma des Shared-Decision-Making.[37] Die Fortführung dieses Prozesses der gemeinsamen, zunehmend gleichwertigen Rolle der Patient:innen und Ärzt:innen im Bereich der Gesundheitsdatennutzung erscheint trotz konzeptueller und kultureller Unterschiede konsequent und von vielen medizinischen Fachkräften gewünscht.[38]

36 *Kessels*, Patients' memory for medical information, J. R. Soc. Med. 2003, 219.

37 *Kaplan/Frosch*, Decision Making in Medicine and Health Care, Annu. Rev. Clin. Psychol. 2005, 525.

38 *Makoul/Clayman*, An integrative model of shared decision making in medical encounters, Patient Educ. Couns. 2006, 301; *Suurmond/Seeleman*, Shared decision-making in an intercultural context: Barriers in the interaction between physicians and immigrant patients, Patient Educ. Couns. 2006, 253; *Pollard u. a.*, Physician attitudes toward shared decision making: A systematic review, Patient Educ. Couns. 2015, 1046.

5. Perspektiven von Ärzt:innen auf Gesundheitsdaten aus Apps und Wearables sowie auf digitales Einwilligungsmanagement – Vorstellung einer Pilotumfrage

Die Bedürfnisse und Perspektiven von Bürger:innen und Gesundheitsfachkräften an die Nutzung von Gesundheitsdaten aus Apps und Wearables sowie Verfahren zur Einwilligung werden im Rahmen des Forschungsprojekts PATH unter anderem über eine Reihe von Online-Befragungen und Interviews erhoben. Die gewonnenen Ergebnisse informieren die Entwicklung der Einwilligungsmanagement-Plattform. Im Folgenden werden die Ergebnisse einer Online-Befragung mit Ärzt:innen vorgestellt. Diese Pilotumfrage ist Teil einer Reihe von Befragungen mit Gesundheitsfachkräften verschiedener Berufsgruppen und in verschiedenen Behandlungssettings (stationär und ambulant).

5.1 Methoden

Im März 2023 wurde ein Online-Fragebogen mit Ärzt:innen pilotiert. Alle Teilnehmer:innen wurden über einen ärztlichen Weiterbildungskurs durch einen der Co-Autoren (PS) rekrutiert. Von neun Teilnehmerinnen haben acht den Fragebogen vollständig beantwortet und werden in die Auswertung eingeschlossen. Die Befragung wurde mit Excel Version 16 ausgewertet. Tabelle 1 zeigt eine Übersicht zu den Merkmalen der teilnehmenden Ärzt:innen.

5.2 Ergebnisse

Die Hälfte der befragten Ärzt:innen hat mit ihren Patient:innen schon einmal über Gesundheits-Apps und Wearables gesprochen und 37,5 % (3/8) haben diese Tools in der Behandlung eingesetzt. In einem Fall wurden dabei auch Daten geteilt, die als hilfreich für die Behandlung eingeschätzt wurden. Die Mehrheit der Teilnehmer:innen (87,5 %; 7/8) schätzen die Daten aus Apps und Wearables als nützlich bzw. sehr nützlich für die Versorgung der Patient:innen ein. Darüber hinaus sehen alle Ärzt:innen einen Nutzen dieser Daten für die Sekundärnutzung.

Die Meinungen der Ärzt:innen zur Kontrolle über die Nutzung von Gesundheitsdaten variieren je nach Quelle der Gesundheitsdaten (Abbil-

Eigenschaft	**n**
Geschlecht	
weiblich	8
Männlich	0
Altersgruppen	
20-29	0
30-39	6
40-49	1
50-59	1
60-69	0
Arbeitsverhältnis	
eigene Praxis/Gemeinschaftspraxis	2
angestellt in Praxis	4
Angestellt in Krankenhaus	2

Tabelle 1: Demographische Merkmale der Studienteilnehmenden (N=8)

dung 4). Nur 37,5 % (3/8) der Ärzt:innen sind der Ansicht, dass die Kontrolle über die Weitergabe klinischer Gesundheitsdaten für die eigene Versorgung bei den Patient:innen liegen sollte, während ebenso viele die Kontrolle durch die Patient:innen ablehnen. Bei der Sekundärnutzung klinischer Gesundheitsdaten befürworten 62,5 % (5/8) der Ärztinnen eine Kontrolle durch die Patient:innen. Ein anderes Bild zeichnet sich bei der Nutzung von Gesundheitsdaten aus Apps und Wearables ab. Hier befürworten jeweils 75 % (6/8) der Ärzt:innen eine Kontrolle der Datennutzung durch die Patient:innen sowohl für die eigene Versorgung als auch bei der Sekundärnutzung.

Alle Ärzt:innen trauen mindestens der Hälfte ihrer Patient:innen den Einsatz eines digitalen Einwilligungs-Management-Systems zu, um informierte Entscheidungen über die Weitergabe ihrer Gesundheitsdaten zu treffen. Dabei sollten die Einwilligungsverfahren über Nutzen, Risiken und Verfahren beim Teilen von Gesundheitsdaten sowie über spezifische Anwendungsfälle, Datennutzer und mögliche Forschungsergebnisse aufklären.

Bei der Frage, wer Patient:innen bei der Benutzung eines digitalen Einwilligungs-Management-Systems unterstützen kann, sehen die Ärzt:innen

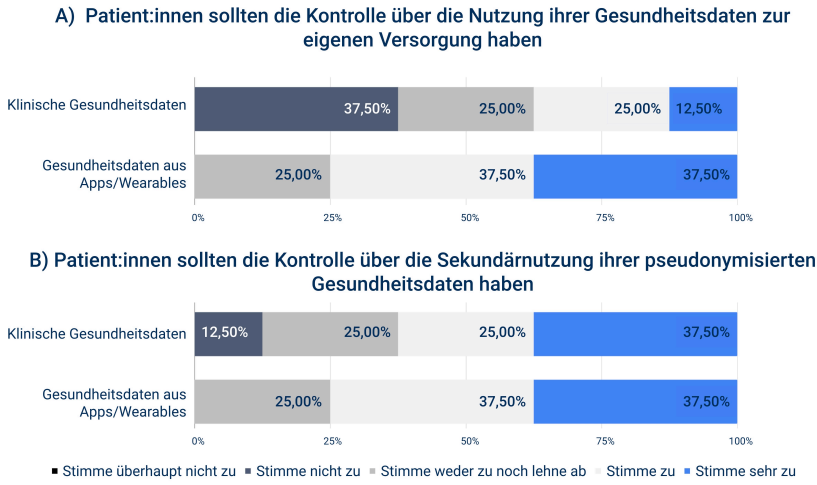

Abbildung 4: Perspektive der befragten Ärzt:innen nach der Patientenkontrolle bei der Nutzung klinischer Gesundheitsdaten oder Daten aus Gesundheits-Apps und Wearables für die Patientenversorgung selbst (A) oder anonymisiert/pseudonymisierter Daten für die Sekundärnutzung (B).

mehrheitlich die Pflicht bei den Krankenkassen (50 %; 4/8). Aber auch Haus- und Fachärzt:innen (37,5 %; 3/8) sowie medizinisch-technische Assistent:innen (37,5 %; 3/8) könnten unterstützen. Zudem wird von 62,5 % (5/8) der Ärzt:innen eine Chance in einer neuen Rolle gesehen, die gezielt Patient:innen und Digitalisierungsthemen übernimmt.

5.3 Diskussion

Das Ziel der Umfrage war die Pilotierung eines Fragebogens, um die Perspektiven von Ärzt:innen auf Gesundheitsdaten aus Apps und Wearables sowie digitales Einwilligungsmanagement zu erheben. Die Ergebnisse dieser Umfrage sind aufgrund der sehr kleinen Stichprobengröße und des Mangels an Geschlechtervielfalt (nur Frauen haben an der Befragung teilgenommen) nicht repräsentativ, weshalb keine allgemeinen Schlussfolgerungen gezogen werden können. Basierend auf dem Feedback aus dieser Umfragerunde wird der Fragebogen für den Einsatz mit unterschied-

lichen medizinische Berufsgruppen in unterschiedlichen Behandlungssettings (stationär und ambulant) und für Befragungen mit größeren Stichproben weiterentwickelt.

Die vorläufigen Ergebnisse aus dieser Pilotbefragung deuten darauf hin, dass Ärzt:innen mehrheitlich einen Nutzen im Zugang zu Gesundheitsdaten sehen, die von Patient:innen mithilfe von Apps und Wearables gesammelt wurden. Vorteile erwarten sie sowohl für die unmittelbare Patientenversorgung als auch für die Sekundärnutzung. Über die Weitergabe von diesen selbst erfassten Gesundheitsdaten sollten Patient:innen selbst entscheiden. Dies unterstreicht noch einmal die spezielle Natur dieser Daten, denn bei der Weitergabe der klinischen Gesundheitsdaten sehen die Ärzt:nnen weniger Patientenkontrolle. Grundsätzlich trauen alle Ärzt:innen mindestens der Hälfte ihrer Patient:innen den Umgang mit digitalen Einwilligungs-Systemen für das Teilen von Gesundheitsdaten zu. Da die Umfrage ausschließlich Meinungen von Ärzt:innen erfasst, lassen sich aus den Ergebnissen keine Rückschlüsse darauf ziehen, wie viele Patient:innen ein System für digitales Einwilligungs-Management tatsächlich nutzen würden und könnten. Um diese Wissenslücke zu schließen, werden im Rahmen des Forschungsprojekt PATH Befragungen und Nutzerstudien mit der allgemeinen Bevölkerung sowie mit Patient:innen des Universitätsklinikums Carl Gustav Carus an der Technischen Universität Dresden durchgeführt.

6. Fazit

Damit Initiativen zur Gesundheitsdatennutzung wie der EHDS Bürger:innen eine echte Kontrolle und Aufklärung geben können, schlagen die Autor:innen ein faires und transparentes Einwilligungsmanagement-System vor, den Standard Health Consent, über das Bürger:innen Zustimmungen für das Teilen von Gesundheitsdaten aus Apps und Wearables festhalten können. In einem partizipativen Entwicklungs-Ansatz werden gemeinsam mit Bürger:innen und Patient:innen das Konzept zum Standard Health Consent getestet und in funktionale Prototypen für eine Einwilligungsmanagement-Plattform weiterentwickelt. Da medizinische Gesundheitsfachkräfte eine zentrale Rolle bei der Unterstützung von Patient:innen im Bereich digitale Gesundheit einnehmen, wird auch diese Stakeholdergruppe in die Konzept- und Prototypenentwicklung über Befragungen und Interviews mit einbezogen.

Literatur

Ärzteblatt (11. Dez. 2023*)*: Ampel will Befüllungspflichten bei elektronischer Patientenakte ausweiten, *Deutsches Ärzteblatt*, URL: https://www.aerzteblatt.de/nachrichten/147972/Ampel-will-Befuellungspflichten-bei-elektronischer-Patientenakte-ausweiten (besucht am 27.02.2024).

Ärzteblatt (4. Jan. 2024): Ärzte genießen größtes Vertrauen, Politikverdrossenheit sichtbar, *Deutsches Ärzteblatt*, URL: https://www.aerzteblatt.de/nachrichten/148387/Aerzte-geniessen-groesstes-Vertrauen-Politikverdrossenheit-sichtbar (besucht am 27.02.2024).

Baines, Rebecca; Stevens, Sebastian; Austin, Daniela; Anil, Krithika; Bradwell, Hannah; Cooper, Leonie; Maramba, Inocencio Daniel; Chatterjee, Arunangsu und Leigh, Simon (2024): Patient and Public Willingness to Share Personal Health Data for Third-Party or Secondary Uses: Systematic Review. *Journal of Medical Internet Research*, e50421. doi: 10.2196/50421.

BEUC - The European Consumer Organisation. (2023): Consumer attitudes to health data sharing. URL: https://www.beuc.eu/reports/consumer-attitudes-health-data-sharing (besucht am 27.02.2024).

Brückner, Stefanie; Kirsten, Toralf; Schwarz, Peter; Cotte, Fabienne; Tsesis, Michael und Gilbert, Stephen (2023): The Social Contract for Health and Wellness Data Sharing Needs a Trusted Standardized Consent. *Mayo Clinic Proceedings: Digital Health*, S. 527–533. doi:10.1016/j.mcpdig.2023.07.008.

Buhr, Lorina; Schicktanz, Silke und Nordmeyer, Eike (2022): Attitudes Toward Mobile Apps for Pandemic Research Among Smartphone Users in Germany: National Survey. *JMIR MHealth UHealth*, e31857. doi:10.2196/31857.

Bundesamt für Justiz (2020): DiGAV - Verordnung über das Verfahren und die Anforderungen zur Prüfung der Erstattungsfähigkeit digitaler Gesundheitsanwendungen in der gesetzlichen Krankenversicherung, https://www.gesetze-im-internet.de/digav/BJNR076800020.html (besucht am 27.02.2024).

Bundesministerium für Gesundheit (2024): Digitalgesetze im Bundestag beschlossen. URL: https://www.bundesgesundheitsministerium.de/presse/pressemitteilungen/bundestag-verabschiedet-digitalgesetze-pm-14-12-23 [besucht am 27.02.2024].

Davies, Melanie J.; Aroda, Vanita R.; Collins, Billy S.; Gabbay, Robert A.; Green, Jennifer; Maruthur, Nisa M.; Rosas, Sylvia E.; Prato, Stefano Del; Mathieu, Chantal; Mingrone, Geltrude; Rossing, Peter; Tankova, Tsvetalina; Tsapas, Apostolos und Buse, John B (2022): Management of hyperglycaemia in type 2 diabetes: A consensus report by the American Diabetes Association (ADA) and the European Association for the Study of Diabetes (EASD). *Diabetes Care*, 45(11), S. 2753-2786. doi:10.2337/dci22-0034.

EDPB-EDPS, EDPB-EDPS (2022): Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space | European Data Protection Board, URL: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032022-proposal_en (besucht am 27.02.2024).

Europäisches Parlament und Rat der Europäischen Union (2016): 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). *Amtsblatt der Europäischen Union*, L 119. URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679 (besucht am 25.04.2024).

European Commission und Directorate-General for Health and Food Safety (2022): Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space. COM(2022) 197 final. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197 (besucht am 28.03.2024).

Gilbert, Stephen; Baca-Motes, Katie; Quer, Giorgio; Wiedermann, Marc und Brockmann, Dirk (2024): Citizen data sovereignty is key to wearables and wellness data reuse for the common good, *NPJ Digital Medicine,* 7(27), S. 1–3. doi.org/10.1038/s41746-024-01004-z

Howell, Michael D.; Corrado, Greg S. und DeSalvo, Karen B. (2024): Three Epochs of Artificial Intelligence in Health Care*, JAMA*, 331(3), S. 242–244. doi:10.1001/jama.2023.25057

Jim, Heather S. L.; Hoogland, Aasha I.; Brownstein, Naomi C.; Barata, Anna; Dicker, Adam P.; Knoop, Hans; Gonzalez, Brian D.; Perkins, Randa; Rollison, Dana; Gilbert, Scott M.; Nanda, Ronica; Berglund, Anders; Mitchell, Ross und Johnstone, Peter A. S. (2020): Innovations in research and clinical care using patient-generated health data*, CA. A Cancer Journal for Clinicians*, 70(3), S. 182-199. https://doi.org/10.3322/caac.21608

Kaplan, Robert M. und Frosch, Dominick L. (2005): Decision Making in Medicine and Health Care, *Annual Review of Clinical Psychology*, 1, S. 525-56. doi.org/10.1146/annurev.clinpsy.1.102803.144118.

Kaye, Jane: Whitley, Edgar A.; Lund, David; Morrison, Michael; Teare, Harriet und Melham, Karen (2015): Dynamic consent: a patient interface for twenty-first century research networks, *European Journal of Human Genetics*, 23, S. 141–146. doi.org/10.1038/ejhg.2014.71.

Kessel, Robin van; Srivastava, Divya; Kyriopoulos, Ilias; Monti, Giovanni; Novillo-Ortiz, David; Milman, Ran; Zhang-Czabanowski, Wojciech Wilhelm; Nasi, Greta; Stern, Ariel Dora; Wharton, George und Mossialos, Elias (2023): Digital Health Reimbursement Strategies of 8 European Countries and Israel: Scoping Review and Policy Mapping, JMIR MHealth UHealth, 29(11), e49003. doi: 10.2196/49003.

Kessels, Roy P C (2003): Patients' memory for medical information, *Journal of the Royal Society of Medicine*, 96(5), S. 219–222. doi:10.1258/jrsm.96.5.219.

Lucas, Bethany; Grayson, Stella; Hamidu, Halimah; Han, Andrew; No, Sandra; Varghese, Ajay und Campisi, Jay (2020*)*: Sex differences in heart rate responses to occupational stress, Stress, 23(1), S. 13-18. doi:10.1080/10253890.2019.1621282.

Makoul, Gregory und Clayman, Marla L. (2006): An integrative model of shared decision making in medical encounters, *Patient Education and Counseling*, 60(3), S. 301-12. doi:10.1016/j.pec.2005.06.010.

Mendiola, Martin F.; Kalnicki, Miriam und Lindenauer, Sarah (2015): Valuable Features in Mobile Health Apps for Patients and Consumers: Content Analysis of Apps and User Ratings, *JMIR MHealth UHealth*, 3(2), e40. doi:10.2196/mhealth.4283.

Menni, Cristina; Valdes, Ana M.; Freidin, Maxim B.; Sudre, Carole H.; Nguyen, Long H.; Drew, David A.; Ganesh, Sajaysurya; Varsavsky, Thomas; Cardoso, M. Jorge; El-Sayed Moustafa, Julia S.; Visconti, Alessia; Hysi, Pirro; Bowyer, Ruth C. E.; Mangino, Massimo; Falchi, Mario; Wolf, Jonathan; Ourselin, Sebastien; Chan, Andrew T.; Steves, Claire J. und Spector, Tim D. (2020): Real-time tracking of self-reported symptoms to predict potential COVID-19, Nature Medicine. 26(7), S. 1037-1040. doi:10.1038/s41591-020-0916-2.

Mills, Peter und Miller, Jennifer (21. März 2019), Why we need a new social contract for data in healthcare. URL: https://www.weforum.org/agenda/2019/03/why-we-need-a-new-social-contract-for-data-in-healthcare/ (besucht am 27.02.2024).

Mundasad, Smitha (6. Juli 2016): NHS data-sharing project scrapped, BBC News. URL: https://www.bbc.com/news/health-36723486 (besucht am 27.2.2024)

Nagpal, Meghan S; Barbaric, Antonia; Sherifali, Diana; Morita, Plinio P und Cafazzo, Joseph A. (2021): Patient-Generated Data Analytics of Health Behaviors of People Living With Type 2 Diabetes: Scoping Review, *JMIR Diabetes*, 6(4), e29027. doi: 10.2196/29027.

OECD, Health at a Glance 2023 (2023): OECD Indicators, *OECD Publishing, Paris*. URL: https://doi.org/10.1787/7a7afb35-en (besucht am 26.2.2024)

PATH — Vernetzung und Sicherheit digitaler Systeme, URL: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/path-1 (besucht am 29.02.2024).

Ploug, Thomas und Holm, Søren (2015): Meta consent: a flexible and autonomous way of obtaining informed consent for secondary research, *BMJ*, 350, h2146. doi.org/10.1136/bmj.h2146

Pollard, Samantha; Bansback, Nick und Bryan, Stirling (2015): Physician attitudes toward shared decision making: A systematic review, *Patient Education and Counseling*, 98(9), S. 1046-57. doi:10.1016/j.pec.2015.05.004.

PwC Deutschland (2020): Fachkräftemangel im Gesundheitswesen: Wenn die Pflege selbst zum Pflegefall wird. URL: https://www.pwc.de/de/gesundheitswesen-und-pharma/fachkraeftemangel-im-deutschen-gesundheitswesen-2022.html#cta2 (besucht am 26.2.2024)

Robert Koch-Institut (2025): Gesundheit in Deutschland. Gesundheitsberichterstattung des Bundes: gemeinsam getragen von RKI und DESTATIS, RKI, Berlin. URL: https://www.rki.de/DE/Content/Gesundheitsmonitoring/Gesundheitsberichterstattung/GesInDtld/gesundheit_in_deutschland_2015.html?nn=2379316 (besucht am 26.2.2024)

Rocher, Luc; Hendrickx, Julien M. und Montjoye, Yves-Alexandre de (2019): Estimating the success of re-identifications in incomplete datasets using generative models, *Nature Communications*, 10(1), 3069. doi:10.1038/s41467-019-10933-3.

Sadare, Olamide; Melvin, Tom; Harvey, Hugh; Vollebregt, Erik und Gilbert, Stephen (2023): Can Apple and Google continue as health app gatekeepers as well as distributors and developers?, *NPJ Digital Medicine*, 6(1), S. 8. doi:10.1038/s41746-023-00754-6

Saleem, Jason J.; Wilck, Nancy R.; Murphy, John J. und Herout, Jennifer (2022): Veteran and Staff Experience from a Pilot Program of Health Care System–Distributed Wearable Devices and Data Sharing, *Applied Clinical Informatics*, 13(3), S. 532-540. doi:10.1055/s-0042-1748857.

Stein, Dorit und Terry, Sharon (2013): Reforming Biobank Consent Policy: A Necessary Move Away from Broad Consent Toward Dynamic Consent, *Genetic Testing and Molecular Biomarkers*, 17(12):855-6. doi:10.1089/gtmb.2013.1550.

Suurmond, Jeanine und Seeleman, Conny (2006): Shared decision-making in an intercultural context: Barriers in the interaction between physicians and immigrant patients, *Patient Education and Counseling*, 60(2), 253-9. doi:10.1016/j.pec.2005.01.012.

Vaghefi, Isaac und Tulu, Bengisu (2019): The continued use of mobile health apps: insights from a longitudinal study, *JMIR MHealth UHealth*, 7(8), e12983. doi: 10.2196/12983.

Weisband, Yiska; Schachinger, Alexander; Sylvia und Balicer, Ran (2024): GIHF-AI Study 2023, URL: https://gihf-ai.eu/wp-content/uploads/2024/01/20240118_GIHF-AI_Survey_EN_WEB.pdf (besucht am 27.2.2024)

Zenker, Sven; Strech, Daniel; Ihrig, Kristina; Jahns, Roland; Müller, Gabriele; Schickhardt, Christoph; Schmidt, Georg; Speer, Ronald; Winkler, Eva; Kielmansegg, Sebastian Graf von und Drepper, Johannes (2022): Data protection-compliant broad consent for secondary use of health care data and human biosamples for (bio)medical research: Towards a new German national standard, *Journal of Biomedical Informatics*, 131, 104096. doi:10.1016/j.jbi.2022.104096.

Zur Evaluation der digitalen Kontaktverfolgung: ein Debattenbeitrag

Henrik Graßhoff und Stefan Schiffner

Zusammenfassung

Dieser Artikel soll einen Beitrag zur Bewertung von digitaler Kontaktverfolgung in einer Pandemie leisten und damit die allgemeine Bewertung von Schutzmaßnahmen unterstützen. Dazu betrachten wir Kontaktverfolgungsapps und analysieren den dadurch entstehenden Datenmarkt. Ausgehend von den Marktteilnehmern beschreiben wir deren Teilnahmegründe und Rahmenbedingungen. In einer narrativen Literaturstudie leiten wir aus den Ergebnissen der Technologieakzeptanzforschung Best Practices für Kontaktverfolgungsapps ab und stellen offene Fragen und mögliche Hindernisse zur Disposition. Unser Beitrag versteht sich als vorläufig; weitere Untersuchungen, insbesondere quantitative Betrachtungen, fehlen. Unsere Analyse zeigt, dass viele der Einflussfaktoren untereinander stark abhängig sind, somit ist eine klarere Formalisierung dieser Abhängigkeiten nötig. Insbesondere technologische Einflüsse sind derzeit aber schwer erforschbar, da die meisten Apps und auch Google und Apples Kontaktverfolgungsframework nicht mehr zugänglich sind.

1. Einleitung

Am 22. März 2024 jährte sich der erste Corona-Lockdown in Deutschland zum vierten Mal. Diesen Jahrestag nahmen viele Politiker:innen und Medien zum Anlass, auf die deutsche Corona-Politik zurückzublicken und die Notwendigkeit ihrer umfassende Aufarbeitung zu betonen.[1] Diese soll, so der augenscheinliche Konsens, die Verhältnismäßigkeit und Effektivität vergangener Schutzmaßnahmen bewerten, um hieraus Handlungsempfehlungen für zukünftige Pandemien abzuleiten.

Das Ziel dieses Kommentars ist es, einen Debattenbeitrag zur Evaluation der digitalen Kontaktverfolgung zu leisten. Hierzu nehmen wir eine

1 *Deutschlandfunk*, Worum es bei der Aufarbeitung der Corona-Maßnahmen geht.

neue Perspektive ein und beschreiben digitale Kontaktverfolgung in ihrer Gesamtheit als Datenmarkt, auf dem verschiedene Akteure Kontaktdaten generieren, sammeln, wertschöpfend verarbeiten und handeln. Wir betten den gegenwärtigen Erkenntnisstand in diese Marktperspektive ein, identifizieren Leerstellen und geben Impulse für eine zukünftige Forschungsausrichtung. Abseits dessen ergeben sich aus der Tatsache, dass der Kontaktverfolgungsmarkt unfrei und durch undemokratische Entscheidungen geprägt war und ist, zweifelhafte politische Abhängigkeiten von digitalen Gatekeepern. Die deshalb auftretenden (potenziellen) Konflikte werden im Rahmen dieses Kommentars beschrieben und können als Anstoß für notwendige, umfassendere, politische Erwägungen dienen.

2. Kontaktverfolgung als Datenmarkt

In einer pandemischen Notlage ist der folgende Grundgedanke gleichermaßen simpel wie nachvollziehbar: Werden Bürger:innen rechtzeitig nach einer Begegnung mit einer infizierten Person benachrichtigt, verhalten sie sich vorsichtiger und unterbrechen so eine mögliche Infektionskette. Falls hierbei zur Begegnungsermittlung im weitesten Sinne digitale Technologien eingesetzt werden, spricht man von *digitaler Kontaktverfolgung*.

Während der Coronapandemie hat sich dieser Ausdruck zunehmend als Synonym für so genannte *Kontaktverfolgungsapps* (KVAs) etabliert.[2] Unter diesem Begriff sind Smartphoneanwendungen für Endanwender:innen zusammengefasst, die letztere bei der Identifikation von Begegnungen mit Infizierten unterstützen. In vielen Ländern wurde die Entwicklung einer KVA durch die nationale Regierung selbst initiiert. Im europäischen Kontext sind diese in der Regel diejenigen KVAs mit den höchsten Nutzungsraten, sodass die durch Regierungen angetriebenen Apps gelegentlich als *die* nationalen KVAs referenziert werden.[3] In Deutschland stand zwischen Juni 2020 und Juni 2023 die *Corona-Warn-App* (CWA) in den App-Stores von Google und Apple zur Verfügung, ihre Weiterentwicklung wurde mittlerweile eingestellt.[4]

Vor diesem Hintergrund mag es zunächst einmal nicht naheliegend sein, digitale Kontaktverfolgung als Datenmarkt anzusehen. Vielmehr scheint

2 *Martin* u.a., Wireless Communications and Mobile Computing 2020.
3 Ebd.
4 *Robert Koch Institut*, Infektionsketten digital unterbrechen mit der Corona-Warn-App.

es so, dass Bürger:innen durch freiwillige Mitarbeit (Nutzung einer KVA) Gesundheitsämter bei der Erfüllung hoheitlicher Aufgaben (manuelle Kontaktverfolgung) unterstützen. In welchem Sinne lässt sich hier also von einem *Markt* sprechen?

Hierzu muss man muss lediglich feststellen, dass, sofern die KVA-Nutzung freiwillig erfolgt, alle beteiligten Akteur:innen nach einer rationalen Abwägung ihrer – wenn auch sehr unterschiedlich charakterisierten – Kosten und Nutzen handeln. Am offensichtlichsten gilt dies für Privatunternehmen, die während der Coronapandemie digitale Kontaktverfolgung in einer Vielzahl von Dienstleistungen und Produkte monetär verwerteten.[5, 6] Daneben wägen auch nationale Regierungen die Entwicklungs- und Betriebskosten gegenüber einem, im Bezug auf das öffentliche Gesundheitssystem teilweise auch monetären, Nutzen ab. Insbesondere bei einer freiwilligen KVA gilt Gleiches aber auch letztlich für einzelne Endanwender:innen. Nichtmonetäre Kostenkomponenten (z. B. Nutzungskosten oder eine empfundene Überwachungsgefahr) und Gewinnerwartungen (z. B. Gesundheitsschutz oder soziale Anerkennung) treten hierbei an die Stelle direkter monetärer Interessen und entscheiden darüber, ob eine Einzelperson eine KVA verwendet – mit anderen Worten, ob sie Marktteilnehmer:in wird.

3. Marktkomponenten

Im Folgenden nehmen wir nacheinander die auftretenden Marktkomponenten – Endanwender:innen, die öffentliche Hand, digitale Gatekeeper und Privatanbieter:innen – in den Blick, fassen jeweils Forschungsfragen und den hierzu gegenwärtigen Erkenntnisstand zusammen und beschreiben potentielle zukünftige Fragen und offene, zur Diskussion stehende Aspekte.

5 *Petereit*, Corona-App wird Magenta: Telekom und SAP erhalten Auftrag der Bundesregierung.

6 *Besser/Welch*, Australia's coronavirus tracing app's data storage contract goes offshore to Amazon.

3.1 Endanwender:innen

Als Endanwender:innen betrachten wir die Zielgruppe, die letztlich die App auf ihren Mobilgeräten installiert. Da die Effektivität von KVAs stark von ihrer Prävalenz in der Gesellschaft abhängt,[7] ist es nachvollziehbar, dass der überwiegende Anteil der Forschung im Bereich der Endanwender:innen auf Technikakzeptanzuntersuchungen entfällt.

Im März und April 2020 – als KVAs in nur einer Handvoll Ländern verfügbar waren – führten Altmann u.a.[8] eine Akzeptanzumfrage unter 5995 Teilnehmenden aus fünf Ländern durch (davon 1013 aus Deutschland). In allen Ländern waren über zwei Drittel der Befragten prinzipiell bereit, eine KVA zu nutzen. Der Gesundheitsschutz nahestehender Personen und die Hoffnung auf ein Ende der Pandemie wirkten dabei als stärkste Treiber; die Sorge vor staatlicher Überwachung und eine befürchtete Angreifbarkeit durch Hacker hingegen wurden am häufigsten als Barrieren genannt. Diese ersten Ergebnisse wurden im Verlauf der Coronapandemie durch zahlreiche weitere Studien präzisiert. In einer Literaturanalyse von 13 Arbeiten extrahierten Oyibo u.a.[9] insgesamt 56 Akzeptanzfaktoren, von denen als stärkste Treiber die empfundene Nützlichkeit für die eigene und die öffentliche Gesundheit wirkten, als stärkste Barrieren Privatsphärebedenken sowie ein empfundenes Misstrauen (insbesondere in die eigene Regierung). Zu einem ähnlichen Ergebnis kam Kuo[10] in einem Vergleich von 76 Studien und einer Metaanalyse der Daten aus 25 dieser Studien. Demzufolge sind die einflussreichsten Akzeptanztreiber der empfundene persönliche und soziale Nutzen, das Vertrauen in KVAs, soziale Normen sowie begünstigende Bedingungen. Überraschenderweise konnte dabei kein signifikanter Zusammenhang zwischen Privatsphärebedenken und der Nutzungsabsicht nachgewiesen werden. Kuo selbst stellt heraus, dass die untersuchten Studien hinsichtlich der Signifikanz der Privatsphärebedenken variieren und der Zusammenhang zur KVA-Akzeptanz noch aufzuklären ist.[11]

Insgesamt ist festzuhalten, dass die Einflussfaktoren auf die Nutzungsbereitschaft vergleichsweise gut verstanden sind. Aus ihren Ergebnissen leiten Oyibo u.a. sowie Kuo Empfehlungen für die Gestaltung von KVAs ab: (1) eine datensparsame App-Architektur, die Anwender:innen eine Wahl-

7 *Ferretini* u.a., Science 2020.
8 *Altmann* u.a., JMIR Mhealth Uhealth 2020.
9 *Oyibo* u.a., Front. Digit. Health 2022.
10 *Kuo*, BMC Medical Informatics and Decision Making 2023.
11 *Kuo*, BMC Medical Informatics and Decision Making 2023.

freiheit über das Teilen ihrer Daten lässt, (2) eine visuell ansprechende Erklärung der getroffenen Sicherheits- und Privatsphäremechanismen, (3) ein niedrigschwelliges und anregendes App-Design, (4) das aktive Bewerben des Gesundheitsnutzens in konventionellen und sozialen Medien sowie (5) die Herstellung öffentlichen Vertrauens durch Delegation des App-Betriebs an vertrauenswürdige Institutionen und die Veröffentlichung des Quellcodes.

Eine Umsetzung dieser Empfehlungen garantiert jedoch nicht hohe Nutzungsraten. So ließen sich durchweg große Differenzen zwischen der Nutzungsbereitschaft und den faktischen Nutzungszahlen von KVAs beobachten,[12] was auf die Präsenz einer *Intentions-Verhaltens-Lücke* hinweist. Diese Lücke – also das Auseinanderklaffen zwischen den Absichten einer Person, eine bestimmte Technologie zu verwenden, und ihrem tatsächlichen Verhalten[13] – ist Zetterholm u.a. zufolge „vermutlich eine der kritischsten Barrieren in Ländern mit freiwilligen KVAs"[14] und einer der wichtigsten Punkte für weitere Forschung.

Es erscheint uns daher angemessen, zukünftige Akzeptanzforschung auf die praktische Steigerung der Nutzungszahlen auszurichten. Legt man hierfür als Theorie vorherrschende Modelle der Technikakzeptanz und der Verhaltenspsychologie zugrunde,[15] gilt es, begünstigende Bedingungen sowie die empfundene Verhaltenskontrolle[16] zu fördern: Welche konkreten Elemente im UX- und UI-Design erhöhen die Selbstwirksamkeit der Anwender:innen? Kann (monetäres) Nudging in diesem Bereich erfolgreich eingesetzt werden?[17] Mit welchen Strategien kann die Funktionsweise der App effektiver kommuniziert werden? Wie muss eine KVA gestaltet werden, um den unterschiedlichen Anforderungen verschiedenster Bevölkerungsgruppen gerecht zu werden?

12 *Garrett* u.a., PLoS ONE 2021.
13 Siehe z. B. *Sheeran/Webb*, Social and Personality Psychology Compass 2016.
14 *Zetterholm* u.a., Informatics 2021.
15 Siehe Tabelle 3 in *Kuo*, BMC Medical Informatics and Decision Making 2023.
16 Im Modell der *Unified theory of acceptance and use of technology* wird die Intentions-Verhaltens-Lücke durch „begünstigende Bedingungen" (bspw. ausreichende Ressourcen) beeinflusst, in der *Theorie des geplanten Verhaltens* durch die empfundene Kontrolle über das eigene Verhalten (Selbstwirksamkeit). Siehe hierzu: *Venkatesh* u.a., MIS Quaterly 2003; *Ajzen*, Organizational Behavior and Human Decision Processes 1991.
17 *Munzert* u.a., Nature Human Behaviour 2021.

Bei all diesen Überlegungen gilt es selbstverständlich auch, eine App zu entwickeln, welche faktisch sicher ist, um die Integrität der App und den Schutz der Privatsphäre ihrer Anwender:innen zu gewährleisten. An dieser Stelle müssen wir jedoch eine Erkenntnislücke diagnostizieren, denn nur wenige Arbeiten widmen sich der Analyse realer Privatsphärerisiken der gängigsten KVAs. Baumgärtner u.a.[18] demonstrierten 2020 die Durchführbarkeit eines bereits bekannten Angriffs auf das Protokoll der CWA, indem sie die Bewegungen infizierter Nutzer:innen mithilfe passiver Bluetooth-Sensoren verfolgten. Ergebnisse von Graßhoff u.a.[19] deuten darauf hin, dass im Bereich eines solchen Sensors statistisch etwa 29 Smartphones mit aktivierter CWA durch Varianzen in ihrem Bluetooth-Sendeverhalten unterschieden werden können – was in einem gewissen Umfang auch das Tracking von Nichtinfizierten ermöglicht. Derartige technische Analysen bilden allerdings die Ausnahme in der KVA-Forschung; in der Regel werden gewünschte Sicherheitseigenschaften bei KVAs eher angenommen[20] oder aus formalen Protokollanalysen gefolgert.[21] Ein notwendiger und beworbener Privatsphäreschutz muss allerdings stets anhand der konkreten Implementierung validiert werden können. Hier ist für zukünftige Anwendungen technisch tiefergehende Forschung notwendig, die derzeit jedoch durch die Abschaltung der Corona-Warn-App und des darunterliegenden Betriebssystemframeworks[22] erschwert wird.

3.2 Öffentliche Hand und Gatekeeper

In unserem Modell des Kontaktverfolgungsdatenmarktes agiert die öffentliche Hand in einer Multirolle. Während die Legislative als Regulatorin des Marktes auftritt, ist die Exekutive zugleich Marktteilnehmerin durch die Entwicklung einer nationalen App (oder die Beauftragung hierzu),

18 *Baumgärtner* u.a., IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) 2020.
19 *Graßhoff* u.a., Proceedings of the 18th International Conference on Availability, Reliability and Security 2023.
20 Bei der CWA wurde beispielsweise verkürzt argumentiert, sie unterbinde Tracking, da sie lediglich Pseudonyme per Bluetooth aussende und diese aus kryptografisch sicheren Primitiven berechnet und regelmäßig geändert werden.
21 *Morio* u.a., 32nd USENIX Security Symposium (USENIX Security 23) 2023.
22 Siehe Fußnote 29.

von deren Nutzung wiederum das öffentliche Gesundheitssystem und die Gesellschaft als Ganzes profitieren.[23]

In ihrer Rolle als Marktteilnehmerin obliegt es ihr, durch die Architektur und Gestaltung der App wesentlich deren Rezeption und Akzeptanz in der Bevölkerung zu beeinflussen. Vor dem Hintergrund der beschriebenen Akzeptanzfaktoren (siehe 3.1), ist hierbei die Bildung von Vertrauen – gerade in individualistischen Gesellschaften[24] wie Deutschland – besonders hervorzuheben. Unter diesen Gesichtspunkten wurde die Konzeption und Entwicklung der CWA vielfach gelobt. Unter anderem der Chaos Computer Club[25] hob den Privacy-by-Design-Ansatz und die Umsetzung des Open-Source-Grundsatzes mit Feedbackschleifen für Expert:innen und Öffentlichkeit positiv hervor. Die CWA ist hier zweifelsfrei ein Projekt mit Modellcharakter, das erörterungswürdige Fragen für zukünftige öffentliche Digitalprojekte aufwirft: Welche Bedingungen begünstigen oder behindern den Erfolg solcher Open-Source-Entwicklungsprojekte? Welche Best Practices lassen sich für die Entwicklung anderer E-Governance-Dienste (auch auf kleineren Maßstabsebenen) lernen? Können Synergieeffekte im Hinblick auf demokratische Partizipation und Kostensenkung[26] aktiv gefördert werden (etwa durch Einbindung in Schulprojekte)?

Unabhängig von der Bereitstellung einer eigenen nationalen App, kommt der Legislative die Aufgabe zu, digitale Kontaktverfolgung zum Wohl der Gesellschaft zu regulieren. Sharon[27] beschrieb 2021 die entstehenden Gefahren, wenn diese Regulierungsrolle nicht durch legitimierte Institutionen, sondern privatwirtschaftliche Technologiekonzerne übernommen wird. In der De-facto-Standardisierung der Kontaktverfolgung durch die GAEN-Schnittstelle[28] von Google und Apple sieht sie einen solchen illegitimen

23 Die Effektivität von KVAs zur Pandemieeindämmung ist nicht Gegenstand dieses Artikels. Hierfür verweisen wir etwa auf: *Anglemyer* u.a., Cochrane Database of Systematic Reviews 2020.

24 Gemessen an der kulturellen Dimension *Individualismus–Kollektivismus* von Hofstede sind Privatsphärebedenken in individualistischen Gesellschaften (wie Deutschland und den USA) gewichtigere Nutzungsbarrieren als in kollektivistischen (wie Singapur). Siehe hierzu: *Kuo*, BMC Medical Informatics and Decision Making 2023; *Geber/Ho*, Information, Communication & Society 2023.

25 *RedaktionsNetzwerk Deutschland*, Erste Reaktionen auf die Corona-Warn-App: Ein großer Kritikpunkt bleibt.

26 *Der Spiegel*, Gesamtkosten für Corona-Warn-App steigen auf 220 Millionen Euro.

27 *Sharon*, Ethics and Information Technology 2021.

28 Bei *Google Apple Exposure Notification* (GAEN) handelt es sich um eine Betriebssystemschnittstelle für KVAs, welche 2020 in Android und iOS implementiert wurde.

„sector creep“[29] und bezeichnet dies als Beispiel für das allgemeinere Phänomen der „Gesundheits-Googlisierung“.[30] Paradoxerweise erhielt die technische Spezifikation der Schnittstelle durch zwei Gatekeeper, die in der Regel eher für invasive Datenpraktiken bekannt sind, weitreichende[31] – obgleich nicht einvernehmliche[32] – Anerkennung in der Privacy-Fachwelt. Dies stärkte mutmaßlich die rigorose Durchsetzbarkeit von GAEN: Verschiedene Repräsentant:innen nationaler Regierungen berichteten davon, dass Google und Apple etwa das korrekte Funktionieren ihrer Apps unterbanden, sofern diese nicht die GAEN-Schnittstelle verwendeten,[33] und hinterfragten, mit welchem Ausmaß diese Konzerne „einer demokratisch gewählten Regierung oder ihren Gesundheitsbehörden vorschreiben könnten, was ihre App leisten darf und was nicht“?[34]

Diese Probleme betten sich in eine wachsende, immer schärfer geführte Debatte um die Regulierung großer Technikkonzerne ein, die auf europäischer Ebene mittlerweile sehr präsent geführt wird. Digitale Kontaktverfolgung als Beispiel eines solchen „sector creeps“ muss in diesem größeren Zusammenhang politisch und juristisch diskutiert werden, sie ist eine konkrete Instanz eines sich ausprägenden Machtungleichgewichts. Die in diesem Bereich beobachtbare, deutliche Abhängigkeit demokratisch gewählter Regierungen von privatwirtschaftlichen Technologieriesen außerhalb Europas liefert somit ein weiteres Argument für die Notwendigkeit einer sorgfältig abgewogenen Regulierung.

Ist eine authorisierte App installiert und aktiviert, berechnet das Betriebssystem kryptografische Pseudonyme und sendet diese in kurzen Abständen per Bluetooth Low Energy aus, um hierdurch Begegnungen zu ermitteln. GAEN ist dezentralisiert, was bedeutet, dass Begegnungsdaten lediglich lokal auf dem Smartphone gespeichert werden. Seit dem 18. September 2023 ist GAEN nicht mehr verfügbar; ob eine Evaluation und Weiterentwicklung der Schnittstelle vorgesehen ist oder passiert, ist unklar.

29 *Sharon*, Ethics and Information Technology 2021.

30 *Sharon*, Personalized Medicine 2016.

31 *Sharon*, Ethics and Information Technology 2021.

32 *Hoepman*, A Critique of the Google Apple Exposure Notification (GAEN) Framework, 2021.

33 *Scott* u.a., How Google and Apple outflanked governments in the race to build coronavirus apps.

34 *Ilves*, Why are Google and Apple dictating how European democracies fight coronavirus?

3.3 Privatanbieter

Im Bereich allgemeiner digitaler Kontaktverfolgungslösungen[35] stellt sich grundlegend die Frage, wie viel privatwirtschaftlicher Wettbewerb zwischen verschiedenen Anbietern zuzulassen und wünschenswert ist. Es ließe sich erwarten, dass die Wahlfreiheit zwischen verschiedenen Anwendungen das Vertrauen in Kontaktverfolgung allgemein zu steigern vermag, indem sie die digitale Kontaktverfolgung dem Nimbus einer staatlichen Überwachung entzieht: Hat eine Anwenderin etwa Misstrauen in die nationale App, nutzt sie an deren Stelle möglicherweise ein anderes Produkt. Auf der anderen Seite sind negative Auswirkungen auf Effektivität, Sicherheit und Rezeption nicht auszuschließen; es gälte hierbei, eine allzu große Fragmentierung inkompatibler Ökosysteme zu vermeiden,[36] das Risiko auftretender Sicherheitslücken abzuwägen[37] sowie einzuschätzen, in welchem Maße derartige Lücken zu einer Kollektivbewertung von „digitaler Kontaktverfolgung allgemein" beitragen (bspw. könnten Mängel einer einzelnen KVA pauschalisierend als Defekt aller KVAs wahrgenommen werden). Vor diesem Hintergrund kann es durchaus profitabel erscheinen, das Angebot digitaler Kontaktverfolgungslösungen, insbesondere KVAs, zu beschränken.

In Deutschland hatten sich auf diesem Markt eine Vielzahl von Anbietern wie SmartMeeting oder die Darfichrein GmbH etabliert. Für Irritationen sorgte hier die Zweigleisigkeit zwischen der Bundesregierung und einigen Landesregierungen. Während erstere weiterhin die aus Steuermitteln finanzierte CWA bewarb, kauften letztere Lizenzen im Umfang von über 20 Millionen Euro[38] für die Nutzung der Luca-App der culture4life GmbH. Investitionen in diese App wurden nicht nur von Datenschützer:innen äußert kritisch gesehen. Auch die Start-up-Initiative „WirFürDigitalisierung" kritisierte eine exklusive Förderung der Luca-App und forderte stattdessen eine „kollaborative, offene und gemeinsame Schnittstelle".[39]

35 Dies umfasst neben KVAs beispielsweise auch Online-Check-in-Systeme umfasst.

36 Auf europäischer Ebene wurde zwischen Oktober 2020 und Februar 2023 unter dem Namen *European Federation Gateway Service* ein Dienst in Betrieb genommen, der eine grenzüberschreitende Interoperabilität der Apps aus 18 EU-Mitgliedsländern sowie Norwegen ermöglichte.

37 Die Sicherheit der Luca-App der culture4life GmbH wurde wegen ihrer zentralisierten Architektur und diverser Sicherheitsmängel vielfach kritisiert. Siehe: *Weiß*, Sicherheitsforscher: Risiken der Luca-App „völlig unverhältnismäßig".

38 *Köver/Fanta*, Mehr als 20 Millionen Euro für Luca.

39 *ZEIT ONLINE*, Start-up-Initiative gegen Einführung der Luca-App.

Für KVAs speziell wurde die Entwicklung einer solchen Schnittstelle erfolgreich von Google und Apple zugunsten ihrer eigenen GAEN-Schnittstelle verhindert (vgl. Abschnitt 3.2). Der Submarkt der digitalen KVAs ist folglich hochgradig unfrei und unterliegt Bedingungen, die von zwei Gatekeepern dominiert wurden und werden. Wie argumentiert, kann dies im Hinblick auf KVAs durchaus als wünschenswert angesehen werden. Angesichts jüngerer europäischer Regulationen[40] und Klagen des US-Justizministeriums gegen Apple[41] ergeben sich jedoch praktische Fragen, etwa ob eine Beschränkung der GAEN-Schnittstelle auf von Google und Apple authorisierte Apps überhaupt zulässig ist.

4. Schluss

Die meisten Kontaktverfolgungsapps sind aus den App-Stores verschwunden; die reale oder empfundene Bedrohung durch COVID ist stark gesunken. Untersuchungen zur Technikakzeptanz mit echten Nutzer:innen wird somit zunehmend schwieriger und sind allenfalls retrospektiv durchführbar. Mit dem zumindest nach außen kommunizierten Ende des Supports des GAEN-Frameworks ist eine quantitative Untersuchung wichtiger technischer Komponenten der Corona-Warn-App stark erschwert.

Das gesellschaftliche Wohl im Blick, ist es aber offensichtlich, dass es sich lohnt, sich frühzeitig um die Technik und deren Akzeptanz zu kümmern. Ansonsten werden wir bei der nächsten Pandemie wieder beobachten, dass auf „schnelle und einfache" Lösungen zurückgegriffen wird, die im Zweifel weder demokratisch legitimiert noch ausgereift sind. Mit den Worten Ulrich Kelbers: „Die Software braucht also eine ständige Pflege und Weiterentwicklung, auch wenn gerade keine Krise ist. Der digitale Austausch muss gewährleistet sein. Die Rechtsgrundlagen müssen evaluiert und angepasst werden".[42]

40 Insbesondere Digital Markets Act, Data Act und Data Governance Act.

41 Ein Anklagepunkt ist des US-Justizministeriums ist exakt, Apple schränke den Zugriff auf Hardware- und Software-Schnittstellen für Dritte ein, siehe: U.S. Department of Justice Office of Public Affairs, 2024.

42 *Kelber*, in: Schmoeckel (Hrsg.), Herausforderung der Rechtsordnung durch die Pandemie, 2021, 195 (210).

Literatur

Ajzen, Icek (1991): The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), S. 179–211. doi:10.1016/0749-5978(91)90020-T.

Altmann, Samuel; Milsom, Luke; Zillessen, Hannah; Blasone, Raffaele; Gerdon, Frederic; Bach, Ruben; Kreuter, Frauke; Nosenzo, Daniele; Toussaert, Séverine und Abeler, Johannes (2020): Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study. *JMIR Mhealth Uhealth*, 8(8). doi:10.2196/19857.

Anglemyer, Andrew; Moore, Theresa HM; Parker, Lisa; Chambers, Timothy; Grady, Alice; Chiu, Kellia; Parry, Matthew; Wilczynska, Magdalena; Flemyng, Ella und Bero, Lisa (2020): Digital contact tracing technologies in epidemics: a rapid review. *Cochrane Database of Systematic Reviews*, 2020(8). doi:10.1002/14651858.CD013699.

Baumgärtner, Lars; Dmitrienko, Alexandra; Freisleben, Bernd; Gruler, Alexander; Höchst, Jonas; Kühlberg, Joshua; Mezini, Mira; Mitev, Richard; Miettinen, Markus; Muhamedagic, Anel; Nguyen, Thien Duc; Penning, Alvar; Pustelnik, Dermot; Roos, Filipp; Sadeghi, Ahmad-Reza; Schwarz, Michael und Uhl, Christian (2020): Mind the GAP: Security & Privacy Risks of Contact Tracing Apps. *IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. doi:10.1109/TrustCom50675.2020.00069.

Besser, Linton und Welch, Dylan (26. Apr. 2020): Australia's coronavirus tracing app's data storage contract goes offshore to Amazon. URL: https://www.abc.net.au/news/2020-04-24/amazon-to-provide-cloud-services-for-coronavirus-tracing-app/12176682 (besucht am 14. Mai 2024).

Der Spiegel (03. Dez. 2022): Gesamtkosten für Corona-Warn-App steigen auf 220 Millionen Euro. URL: https://spiegel.de/netzwelt/gesamtkosten-fuer-corona-warn-app-steigen-auf-220-millionen-euro-a-0202c5e9-f2f9-4586-a8f1-e469fd5437fb (besucht am 14. Mai 2024).

Deutschlandfunk (2024): Worum es bei der Aufarbeitung der Corona-Maßnahmen geht. URL: https://www.deutschlandfunk.de/corona-massnahmen-aufarbeitung-pandemie-lockdown-100.html (besucht am 31. März 2024).

Ferretini, Luca; Wymant, Chris; Kendall, Michelle; Zhao, Lele; Nurtay, Anel; Abeler-Dörner, Lucie; Parker, Michael; Bonsall, David und Fraser, Christophe (2020): Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, 368(6491). doi:10.1126/science.abb6936.

Garrett, Paul M.; White, Joshua P.; Lewandowsky, Stephan; Kashima, Yoshihisa; Perfors, Andrew; Little, Daniel R.; Geard, Nic; Mitchell, Lewis; Tomko, Martin und Dennis, Simon (2021): The acceptability and uptake of smartphone tracking for COVID-19 in Australia. *PloS ONE*, 16(1). doi:10.1371/journal.pone.0244827.

Geber, Sarah und Ho, Shirley S. (2022): Examining the cultural dimension of contact-tracing app adoption during the COVID-19 pandemic: a cross-country study in Singapore and Switzerland. *Information, Communication & Society*, 26(11), S. 2229–2249. doi:10.1080/1369118X.2022.2082880.

Graßhoff, Henrik; Adamsky, Florian und Schiffner, Stefan (2023): Smartphones in a Microwave: Formal and Experimental Feasibility Study on Fingerprinting the Corona-Warn-App. *Proceedings of the 18th International Conference on Availability, Reliability and Security*, doi:10.1145/3600160.3605011.

Hoepman, Jaap-Henk (2021): *A Critique of the Google Apple Exposure Notification (GAEN) Framework*. doi:10.48550/arXiv.2012.05097.

Ilves, Ieva (16. Juni 2020): Why are Google and Apple dictating how European democracies fight coronavirus? URL: https://theguardian.com/commentisfree/2020/jun/16/google-apple-dictating-european-democracies-coronavirus (besucht am 14. Mai 2024).

Kelber, Ulrich (2021): Datenschutz und Datensicherheit in Corona-Zeiten. In: Schmoeckel, Matthias (Hrsg.): *Herausforderung der Rechtsordnung durch die Pandemie* (58). Baden-Baden: Nomos, S. 195–210. doi:10.5771/9783748912767.

Köver, Chris und Fanta, Alexander (12. April 2021): Mehr als 20 Millionen Euro für Luca. URL: https://netzpolitik.org/2021/digitale-kontaktverfolgung-fast-20-millionen-euro-fuer-luca/ (besucht am 14. Mai 2024).

Kuo, Kuang-Ming (2023): Antecedents predicting digital contact tracing acceptance: a systematic review and meta-analysis. *BMC Medical Informatics and Decision Making*, 23. doi:10.1186/s12911-023-02313-1.

Martin, Tania; Karopoulos, Georgios; Hernández-Ramos, José L.; Kambourakis, Georgios und Nai Fovino, Igor (2020): Demystifying COVID-19 Digital Contact Tracing: A Survey on Frameworks and Mobile Apps. *Wireless Communications and Mobile Computing*, 2020, S. 1–29. doi:10.1155/2020/8851429.

Morio, Kevin; Esiyok, Ilkan; Jackson, Dennis und Künnemann, Robert (2023): Automated Security Analysis of Exposure Notification Systems. *32nd USENIX Security Symposium (USENIX Security 23)*. S. 6593–6610.

Munzert, Simon; Selb, Peter; Gohdes, Anita; Stoetzer, Lukas F. und Lowe, Will (2021): Tracking and promoting the usage of a COVID-19 contact tracing app. *Nature Human Behaviour*, 5, S. 247–255. doi:10.1038/s41562-020-01044-x.

Oyibo, Kiemute; Sahu, Kirti Sundar; Oetomo, Arlene und Morita Plinio Pelegrini (2022): Factors Influencing the Adoption of Contact Tracing Applications: Systematic Review and Recommendations. *Front. Digit. Health*, 4. doi:10.3389/fdgth.2022.862466.

Petereit, Dieter (01. Mai 2020): Corona-App wird Magenta: Telekom und SAP erhalten Auftrag der Bundesregierung. URL: https://t3n.de/news/corona-app-magenta-telekom-sap-1274327/ (besucht am 14. Mai 2024).

RedaktionsNetzwerk Deutschland (17. Juni 2020): Erste Reaktionen auf die Corona-Warn-App: Ein großer Kritikpunkt bleibt. URL: https://rnd.de/digital/corona-warn-app-erste-reaktionen-zeigen-grossen-kritikpunkt-GJECMZBZAVF2JF545XI26OEZZY.html (besucht am 14. Mai 2024).

Robert Koch Institut (15. Feb. 2024): Infektionsketten digital unterbrechen mit der Corona-Warn-App. URL: https://rki.de/cwa (besucht am 14. Mai 2024).

Scott, Mark; Braun, Elisa; Delcker, Janosch und Manancourt, Vincent (15. Mai 2020): How Google and Apple outflanked governments in the race to build coronavirus apps. URL: https://politico.eu/article/google-apple-coronavirus-app-privacy-uk-france-germany/ (besucht am 14. Mai 2024).

Sharon, Tamar (2016): The Googlization of Health Research: From Disruptive Innovation to Disruptive Ethics. *Personalized Ethics*, 13(6), S. 563–574. doi:10.2217/pme-2016-0057.

Sharon, Tamar (2021): Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology*, 23, S. 45–57. doi:10.1007/s10676-020-09547-x.

Sheeran, Paschal und Webb, Thomas L. (2016): The Intention-Behavior Gap. *Social and Personality Psychology Compass*, 10(9), S. 503–518. doi:10.1111/spc3.12265.

U.S. Department of Justice Office of Public Affairs (2024): Justice Department Sues Apple for Monopolizing Smartphone Markets. URL: https://www.justice.gov/opa/pr/justice-department-sues-apple-monopolizing-smartphone-markets (besucht am 31. März 2024).

Venkatesh, Viswanath; Morris, Michael G.; Davis, Gordon B. und Davis, Fred D. (2003): User Acceptance of Information Technology: Toward a Unified View. *MIS Quaterly*, 27(3), S. 425–478.

Weiß, Eva-Maria (29. April 2021): Sicherheitsforscher: Risiken der Luca-App „völlig unverhältnismäßig". URL: https://heise.de/news/Sicherheitsforscher-Risiken-der-Luca-App-voellig-unverhaeltnismaessig-6031770.html (besucht am 14. Mai 2024).

ZEIT ONLINE (05. März 2021): Start-up-Initiative gegen Einführung der Luca-App. URL: https://zeit.de/news/2021-03/05/start-up-initiative-gegen-einfuehrung-der-luca-app (besucht am 14. Mai 2024).

Zetterholm, My Villius; Lin, Yanqing und Jokela, Päivi (2021): Digital Contact Tracing Applications during COVID-19: A Scoping Review about Public Acceptance. *Informatics*, 8(3). doi:10.3390/informatics8030048.

Betroffenenrechte in der digitalen Selbstvermessung

Fabiola Böning und Uwe Laufs

Zusammenfassung

Der Beitrag verdeutlicht die Wichtigkeit der Beschäftigung mit der effektiven, individualisierten und einfachen Ausübung der Betroffenenrechte im Zeitalter der ubiquitären Datafizierung, die auch vor den eigenen Körpervorgängen keinen Halt macht. Selbstvermesser haben ein gesteigertes Interesse an der Verarbeitung ihrer Daten. Mit dem Umfang der Datenverarbeitung steigt auch die Notwendigkeit, die nutzerfreundliche Ausübung der in der Datenschutz-Grundverordnung (DS-GVO) kodifizierten Betroffenenrechte zu ermöglichen. Im Beitrag wird anhand des in Art. 15 DS-GVO normierten Auskunftsrechts die Funktion des im Projekt TESTER[1] entwickelten und erforschten Privacy-Assistenten zur Unterstützung der Selbstvermesser erläutert. Dabei erfolgt die Ausübung der Betroffenenrechte bei dem Anbieter eines Selbstvermessungsgerätes selbst direkt über eine Schnittstelle oder mittels eines Anfragengenerators und dem Einsatz vorgefertigter Templates, die individualisiert und an die Bedürfnisse der Nutzer angepasst werden können.

1. Einleitung

Die Datenverarbeitung durch private und öffentliche Stellen wird auch in den nächsten Jahren stetig zunehmen. Diese Tatsache entspricht zum einen der generellen Marktentwicklung im Bereich der Datenverarbeitung[2] und wird zum anderen auch durch die nationalen und europäischen Gesetzgeber gefördert, die sich durch ein vermehrtes Datenteilen gesamtgesell-

1 Das Projekt „TESTER – Digitale Selbstvermessung selbstbestimmt gestalten" wird im Rahmen der BMBF-Förderrichtlinie „Forschung Agil" für eine Dauer von drei Jahren bis August 2024 gefördert. Es trägt das Förderkennzeichen KIS6AGSE022; s. https://www.tester-projekt.de/.

2 *Statistisches Bundesamt*, Umsatz der Branche Datenverarbeitung und Hosting in Deutschland von 2012 bis 2019 und Prognose bis zum Jahr 2025, 2021.

schaftliche Vorteile – gerade auch im Bereich der Gesundheitsversorgung – erhoffen.[3]

1.1 Selbstvermessung

Ein Teilaspekt der umfassenden Datafizierung der Umwelt ist die wachsende Bedeutung der digitalen Selbstvermessung,[4] bei der digitale Technologien eingesetzt werden, um tägliche Erfahrungen, Gewohnheiten und körperliche Prozesse aufzuzeichnen und in Daten umzuwandeln. Ermöglicht wird dies durch zunehmend erschwingliche und leicht handhabbare intelligente Sensortechnologie. Der Einsatz dieser Technologien im privaten Umfeld kann einen Einfluss auf die eigene Körperwahrnehmung haben, was in positiver Hinsicht als ein wichtiger Schritt auf dem Weg hin zu einer präventiven und personalisierten Gesundheitsversorgung gesehen werden kann. Darüber hinaus kommen Selbstvermessungstechnologien auch in der Versorgung zunehmend zum Einsatz. Ein negativer Aspekt der digitalen Selbstvermessung kann ein zunehmend zwanghaftes Verhalten der Nutzer sein.[5] Mit der Zunahme der Verwendung von Wearables zum Zwecke der Selbstvermessung[6] steigt auch die Datenverarbeitung durch Anbieter in diesem sensiblen Bereich kontinuierlich, was wiederum zu ethischen und rechtlichen Fragestellungen führt

3 S. z.B. *BMG*, Digitalstrategie für das Gesundheitswesen und die Pflege, 2023 und *Europäische Kommission*, COM(2022) 197 final vom 03.05.2022; s. zum europäischen Datenraum insgesamt *Roßnagel*, ZRP 2021, 173.

4 Auch bekannt als Self-Tracking, Self-Monitoring, Self-Logging, Lifelogging oder Personal Informatics.

5 S. insgesamt zum Begriff und zur Geschichte der Selbstvermessung bereits *Böning u.a.*, in: Friedewald u.a. (Hrsg.), Daten-Fairness in einer globalisierten Welt, 2023, 247 (248 ff.); s. zum Gegenstand der digitalen Selbstvermessung darüber hinaus z.B. *Rode/Stern*, in: Lessenich (Hrsg.), Geschlossene Gesellschaften. Verhandlungen des 38. Kongresses des Deutschen Gesellschaft für Soziologie, 2016.

6 S. zum Absatz von (Core-)Wearables in Deutschland zwischen 2015 und 2023 *gfu*, Absatz von Wearables in Deutschland in den Jahren 2015 bis 2023 (in Millionen Stück), 2024 und zum erwarteten weltweiten Absatz von Wearables *IDC*, Absatz von Wearables weltweit von 2014 bis 2022 und Prognose bis 2027, 2024.

1.2 Probleme bei der Ausübung von Betroffenenrechten

Die Kombination aus dem gesellschaftlichen Wandel, der auf der digitalen Teilhabe einzelner Personen basiert, der steigenden Anzahl von Datenverarbeitungsvorgängen und der potentiell stark steigenden Anzahl von datenverarbeitenden Stellen kann zu einer Überforderung der einzelnen Person führen, wenn es darum geht, in der DS-GVO kodifizierte Betroffenenrechte auch auszuüben. Dies kann zum einen erschwert sein, weil schon keine Kenntnis über bestehende Betroffenenrechte besteht.[7] Zum anderen kann die Ausübung der Betroffenenrechte an sich problematisch sein, weil unterschiedliche rechtliche Voraussetzungen gegeben sein müssen, die die betroffene Person nicht notwendigerweise nachvollziehen kann.

Technische Lösungen können einen Beitrag zur Stärkung der informationellen Selbstbestimmung der betroffenen Personen leisten, was letztlich der gesamten Gesellschaft zugutekommen kann.

1.3 Überblick über TESTER

In dem Projekt „TESTER – Digitale Selbstvermessung selbstbestimmt gestalten" wird das Ziel verfolgt, Selbstvermesser beim Umgang mit den aus der Selbstvermessung generierten Daten durch die Herstellung von Transparenz und Intervenierbarkeit zu unterstützen. Hierfür wird ein Privacy-Assistent entwickelt und erforscht, der den Nutzern zunächst in interaktiver und personalisierter Weise Informationen über die von den verschiedenen Anbietern von Selbstvermessungsgeräten verarbeiteten Daten ver- und übermittelt. Die weitere Funktion des Privacy-Assistenten besteht in der Erleichterung der Ausübung von Betroffenenrechten, durch die der Nutzer bei der Datenverarbeitung durch Anbieter von Selbstvermessungsgeräten intervenieren kann. Den Privacy-Assistenten wird es dabei zum einen als allgemeine Variante geben, über die der Nutzer Einblick in die Datenverarbeitung durch verschiedene Geräte der Selbstvermessung hat, und zum anderen als eingebettete Variante, die in die Softwareumgebung der Anbieter von Selbstvermessungsgeräten integriert werden kann.

7 S. zur Problematik der Informiertheit der betroffenen Person schon *Böning u.a.*, in: Friedewald u.a. (Hrsg.), Daten-Fairness in einer globalisierten Welt, 2023, 247.

1.4 Die Ausübung der Betroffenenrechte mithilfe von TESTER

Das im Privacy Assistenten entwickelte System zur Intervention funktioniert zum einen über eine Softwareschnittstelle und zum anderen über einen Generator für Datenschutzanfragen zur Ausübung der Betroffenenrechte per E-Mail oder per Brief.

Die vorgesehene Schnittstelle wird sowohl über den Webstandard REST[8] als auch nativ über eine Java-Schnittstelle bereitgestellt. Diese Schnittstelle hat eine zweifache Funktion. Zum einen ermöglicht sie die Authentifizierung des Anwenders. Hierbei wird unter Einsatz eines sicheren Authentifizierungsverfahrens festgestellt, um welchen Nutzer es sich handelt und ob es tatsächlich dieser Nutzer ist. Zum anderen ermöglicht die Schnittstelle die direkte Durchführung spezifischer Interventionen auf dem System des Anbieters. Der Privacy-Assistent oder in die Selbstvermessungs-Apps integrierte Privacy-Funktionen, welche die Schnittstelle verwenden, können hierbei im kontrollierten Rahmen Daten über die Schnittstelle abrufen, ändern oder löschen. Die Schnittstelle wird im Projekt exemplarisch im Produkt eines Anwendungsunternehmens aus dem Bereich Telemedizin umgesetzt, ist aber grundsätzlich dafür geeignet, auch in anderen Umgebungen eingesetzt zu werden.

Für den Fall, dass ein Anbieter diese Softwareschnittstelle nicht unterstützt, ist als Rückfalllösung ein Generator für Datenschutzanfragen vorgesehen. Dieser Generator erstellt Dokumente für die betroffene Person, die über den traditionellen Weg (wie E-Mail oder Brief) an den Verantwortlichen zugestellt werden können. Der Text für diese Dokumente wird anhand vorgefertigter Textbausteine (Templates) generiert, die mittels einer Template Engine[9] zu einer vollständigen Datenschutzanfrage in einem Textdokument kombiniert werden. Die Textbausteine sind vorgefertigte Textblöcke für die jeweilige Intervention (z.B. Ausübung des Auskunftsrechts), welche um die konkreten und im Hinblick auf die betroffene Person individualisierten Daten ergänzt werden.

8 https://www.w3.org/2001/sw/wiki/REST.
9 https://velocity.apache.org/.

2. Technische Grundlagen

Die Entwicklung des TESTER Privacy-Assistenten erfolgt auf Basis von Java[10] als einer der am weitesten verbreiteten und bekanntesten Programmiersprachen,[11] wobei grundsätzlich auch die Verwendung anderer Programmiersprachen in Betracht kommt.

Das im Rahmen von TESTER entwickelte System zur Intervention funktioniert zum einen über eine Softwareschnittstelle und zum anderen über einen Generator für Datenschutzanfragen zur Ausübung der Betroffenenrechte per E-Mail oder Brief.

Die Geschäftslogik von TESTER zeigt auch die folgende Abbildung, die einen Ausschnitt aus der Gesamtarchitektur darstellt:

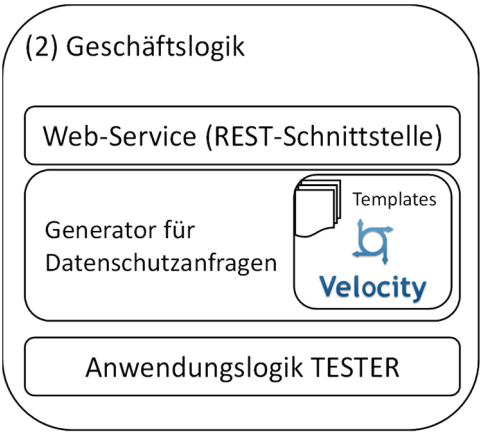

Abbildung 1: Interventionsmodell von TESTER

10 *Meyer*, Touch of Class. Learning to Program Well with Objects and Contracts, 2009, S. 321-360.

11 *TIOBE*, TIOBE Index for March 2024. Als plattformunabhängige und etablierte Programmiersprache bietet Java eine Vielzahl frei verfügbarer Softwarebibliotheken. Somit kann bei der Umsetzung der benötigten Funktionalitäten auf ein umfangreiches Angebot zurückgegriffen werden.

2.1 Schnittstelle zur Intervention

Die Schnittstelle zur Intervention stellt exemplarisch einen produktübergreifenden Standard dar. Ein solcher Standard ermöglicht es Anbietern, eine konsistente Reihe von Datenschutzfunktionen zu implementieren, die von Drittanbietertools und -diensten genutzt werden können, um die Interoperabilität und Nutzerfreundlichkeit zu verbessern. Die Schnittstelle bietet eine Reihe generischer Funktionen, die es Anwendungen ermöglichen, Nutzern einen konsistenten und verständlichen Zugang zu ihren Daten zu gewähren. Funktionen wie authenticateUser, listData, listDataDescriptors, listDataOperations, deny und delete sind so gestaltet, dass sie in einer Vielzahl von Systemen ohne spezifische Anpassungen integriert werden können.

Durch die Standardisierung dieser Funktionen können verschiedene Systeme und Anwendungen in der Lage sein, miteinander zu kommunizieren und Daten gemäß den Nutzerpräferenzen zu verarbeiten. Dies erleichtert es den Nutzern, ihre Datenschutzeinstellungen über verschiedene Dienste hinweg zu verwalten.

Eine zentrale Funktion der Schnittstelle ist die Möglichkeit abzufragen, welche Aktionen für bestimmte Datentypen unterstützt werden. Diese Funktion ist entscheidend, um sicherzustellen, dass keine Daten gelöscht oder manipuliert werden, die für die grundlegende Funktionalität des Systems unerlässlich sind. Zum Beispiel kann eine supportedActions(DataDescriptor)-Funktion eine Liste von Aktionen zurückgeben, die für bestimmte Daten verfügbar sind.

Während die Schnittstelle generische Funktionen definiert, liegt es an den einzelnen Anbietern zu entscheiden, welche Funktionen für welche Daten freigegeben werden. Dadurch können Anbieter sicherstellen, dass die Integrität und Funktionalität ihrer Systeme gewahrt bleibt, während sie gleichzeitig Flexibilität und die Kontrolle des Nutzers über seine Daten erhöhen.

Für die Nutzer bietet dieser Ansatz eine transparente und kontrollierte Möglichkeit, ihre Datenschutzrechte auszuüben. Für Anbieter bietet er eine klare Richtlinie zur Implementierung von Datenschutzfunktionen, die die Einhaltung gesetzlicher Vorschriften wie der DS-GVO erleichtern und das Vertrauen der Nutzer stärken können.

Die Implementierung einer solchen Schnittstelle würde einen signifikanten Fortschritt bedeuten. Dies sowohl in Bezug auf die technische Aus-

führung von Datenschutzfunktionen als auch in der Harmonisierung der Nutzererfahrung über verschiedene Plattformen und Dienste hinweg.

Um Zugriff auf die Daten zu erhalten, muss der Nutzer sich zuerst authentifizieren. Dies erfolgt durch die authenticateUser-Funktion, die Nutzernamen und Anmeldeinformationen als Parameter verwendet, um die Identität des Nutzers zu bestätigen.

Die Funktion listData gibt eine Übersicht über alle gespeicherten Daten des Nutzers. listDataDescriptors bietet eine Beschreibung der Daten, was für eine transparente Datenverarbeitung sorgt. Mit listDataOperations kann der Nutzer eine Auflistung aller Datenverarbeitungsaktivitäten einsehen, die mit seinen Daten durchgeführt wurden.

Durch deny(ID), deny(DataOperation) und denyAll()[12] kann der Nutzer spezifische oder alle Datenverarbeitungen verbieten. Diese Funktionen erlauben es den Nutzern, Widerspruch gegen bestimmte Verarbeitungsarten einzulegen, zum Beispiel gegen die Weitergabe der Daten zu Werbezwecken.

Die delete(DataDescriptor)-Funktion ermöglicht es dem Nutzer, die Löschung spezifischer Datentypen durchzuführen. Mit deleteAll kann er die Löschung aller über ihn gespeicherten Daten beantragen. Alternativ kann er die Daten selbst löschen, falls der Verantwortliche dies zulässt. Dies könnte z.B. bei der E-Mail-Adresse der Fall sein, falls sie nur für die Zusendung von Newslettern und Werbung verwendet wird und für das System nicht zwingend benötigt wird.

Alle Daten werden im JSON-Format[13] übertragen, das für seine Leichtgewichtigkeit und Kompatibilität mit Web-Technologien bekannt ist.

2.2 Anfragengenerator

Zur Generierung der Texte zur Ausübung der Betroffenenrechte, die die betroffene Person selbst per E-Mail oder Brief an den Verantwortlichen verschicken kann, wird eine Template Engine verwendet, die auf Basis der im System vorhandenen Informationen über den Umgang mit den personenbezogenen Daten gezielt nach Wunsch des Nutzers Anfragen erstellt.

Template Engines können den Prozess der Generierung von Datenschutzanfragen erheblich vereinfachen und standardisieren. Sie bieten eine

12 ( ) ist in diesem Fall kein Übergabeparameter, da es um alle vorhandenen Daten geht.
13 https://www.json.org/json-en.html.

flexible und effiziente Methode, um individuelle und professionelle Dokumente zu erstellen, ohne diese jedes Mal von Grund auf neu zu schreiben. Die in TESTER verwendete Template Engine Apache Velocity bietet hierfür eine einfache Syntax, um Textvorlagen mit konkreten Daten zu individualisieren.

3. Rechtliche Grundlagen von Art. 15 DS-GVO

Das Auskunftsrecht nach Art. 15 DS-GVO[14] ist wegen der grundsätzlichen Individualisierbarkeit des Auskunftsersuchens ein exzellentes Beispiel, um die Funktionen des Privacy-Assistenten vorzustellen.[15] Vorbereitend werden die relevanten rechtlichen Grundlagen in den folgenden Ausführungen erläutert.

3.1 Antragsberechtigung

Den Antrag auf Auskunft nach Art. 15 DS-GVO kann eine betroffene Person stellen.[16] Die Betroffenheit muss dann nicht vorliegen, wenn der Verantwortliche der Person eine sogenannten „Negativauskunft" auf der ersten Stufe gibt,[17] also durch den Verantwortlichen keine personenbezogenen Daten verarbeitet werden. In diesem Fall ist die DS-GVO entsprechend Art. 2 Abs. 1 DS-GVO grundsätzlich nicht anwendbar, sodass eigentlich kein Auskunftsrecht nach Art. 15 DS-GVO gegeben ist.

14 S. ausführlich zum Auskunftsanspruch z.B. *Peisker*, Der datenschutzrechtliche Auskunftsanspruch, 2023.

15 S. zu den Beispielen für die Funktion des Privacy-Assistenten die Ausführungen unter 4 und 5.

16 S. zu Fragen des Personenbezugs z.B. *Hornung/Wagner*, CR 2019, 565; EuG, Urteil vom 26.4.2023 – T-557/20, eur-lex, Rn. 60 ff. m. Anm. *Baumgartner*, ZD 2023, 399; EuGH, Urteil vom 20.12.2017 – C434/16, curia, Rn. 27 ff.

17 *Franck*, in: Gola/Heckmann (Hrsg.), DS-GVO BDSG, Art. 15 DS-GVO, Rn. 28; s. dazu auch die Ausführungen unter 3.3.

3.2 Identifizierung des Antragsstellers

Bei begründeten Zweifeln des Verantwortlichen an der Identität der auskunftsersuchenden Person kann jener nach Art. 12 Abs. 6 DS-GVO zusätzliche Informationen anfordern, die zur Bestätigung der Identität der betroffenen Person erforderlich sind.[18] Dabei ist der Grundsatz der Datenminimierung zu beachten. Es muss ein angemessenes Verhältnis zwischen dem Umfang und der Sensitivität der übermittelten Daten und den Anforderungen an die Identitätsprüfung bestehen.[19] Die zum Zwecke der Identifizierung der auskunftsersuchenden Person erhaltenen Daten darf der Verantwortliche auch nur zur Identifizierung verwenden und muss sie danach löschen.[20] Kann die auskunftsersuchende Person nicht identifiziert werden, so führt dies dazu, dass der Verantwortliche der betroffenen Person keine Auskunft erteilen muss und darf, [21] damit nicht eine unberechtigte Person Auskunft erhält.

Nach EG 64 DS-GVO, der als Gesetzesbegründung im Sinne des Art. 296 Abs. 2 AEUV für die Auslegung herangezogen werden kann,[22] soll der Verantwortliche alle vertretbaren Mittel nutzen, um die Identität einer auskunftssuchenden Person zu überprüfen. Die Notwendigkeit einer Identitätsprüfung wird für Online-Dienste und Online-Kennungen in EG 64 S. 1 DS-GVO betont. Im Falle der Übermittlung von Informationen an eine nicht berechtigte Person drohen dem Verantwortlichen Schadensersatzansprüche, Sanktionen und zivilrechtliche Ansprüche.[23] In der Anwendung TESTER kann die betroffene Person grundsätzlich anhand des Login-Mechanismus identifiziert werden, im Schriftverkehr zum Zwecke der Intervention in der Form der Ausübung von Betroffenenrechten, indem

18 S. auch *Kremer*, CR 2018, 560 (566 f.); *Bienemann*, in: Sydow/Marsch (Hrsg.), DS-GVO | BDSG, Art. 15 DS-GVO, Rn. 21; *Piltz*, K&R 2016, 629 (631).

19 S. *Engeler/Quiel*, NJW 2019, 2201 (2205); *Bienemann*, in: Sydow/Marsch (Hrsg.), DS-GVO | BDSG, Art. 15 DS-GVO, Rn. 22; *Schmidt-Wudy*, in: Wolff u.a. (Hrsg.), BeckOK Datenschutzrecht, Art. 15 DS-GVO, Rn. 37.

20 S. *Schmidt-Wudy*, in: Wolff u.a. (Hrsg.), BeckOK Datenschutzrecht, Art. 15 DS-GVO, Rn. 39.

21 S. *Paal*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 15 DS-GVO, Rn. 10; *Bienemann*, in: Sydow/Marsch (Hrsg.), DS-GVO | BDSG, Art. 15 DS-GVO, Rn. 21.

22 S. z.B. *Calliess*, in: Calliess/Ruffert (Hrsg.), Art. 296 AEUV, Rn. 11 ff.; s. zu den Grenzen der Auslegung, die anhand des Wortlauts des Gesetzestextes zu bestimme sind aber z.B. EuGH, Urteil vom 26.10.2023 – C-307/22, curia, Rn. 44.

23 S. näher *Bienemann*, in: Sydow/Marsch (Hrsg.), DS-GVO | BDSG, Art. 15 DS-GVO, Rn. 21.

sie entsprechende Merkmale wie beispielsweise die Kundennummer oder die Anschrift eingibt.[24] Diese Anforderung steht auch in einem angemessenen Verhältnis zum Auskunftsbegehren der betroffenen Person, weil durch die Eingabe der identifizierenden Merkmale verhindert werden kann, dass der Anbieter die Daten an einen unbefugten Dritten herausgibt.

3.3 Mögliche Mehrstufigkeit des Antrags

Das Auskunftsrecht wird durch die betroffene Person – theoretisch – in zwei Stufen ausgeübt. Zunächst erfolgt der Antrag der betroffenen Person, ohne den der Verantwortliche nicht tätig werden muss.[25] Der betroffenen Person muss dann eine Mitteilung darüber gemacht werden, ob personenbezogene Daten über sie verarbeitet werden. Diese Mitteilung muss in Form einer „Negativauskunft"[26] auch dann gemacht werden, wenn keine personenbezogenen Daten verarbeitet werden.[27] Werden personenbezogene Daten verarbeitet, kann die betroffene Person mit einem zweiten Antrag Auskunft darüber verlangen, welche personenbezogenen Daten verarbeitet wurden.[28]

Es ist umstritten, ob die betroffene Person zusätzlich zu dem Antrag auf die Mitteilung der Bestätigung der Verarbeitung personenbezogener Daten einen Antrag auf Auskunft über diese personenbezogenen Daten und die in Art. 15 Abs. 1 DS-GVO aufgezählten Informationen stellen muss.[29] Ein Antrag auf die Erteilung einer Auskunft darüber, ob durch den Verantwortlichen personenbezogene Daten des Nutzers verarbeitet werden, wäre nach dieser Logik ein Antrag auf der „ersten Stufe". Ein Antrag auf die Erteilung einer Auskunft darüber, welche Daten verarbeitet werden, wäre ein Antrag auf der „zweiten Stufe".

---

24 Ausführlich zur Identifizierung *Steiger*, ZD 2024, 143; zu beachten sind im diesem Kontext jedoch weiterhin die Datenschutzgrundsätze, zu denen auch der Grundsatz der Datenminimierung gehört.

25 S. *Dix*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, Art. 15 DS-GVO, Rn. 3, der von einer „Holschuld" der betroffenen Person spricht.

26 *Paal*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 15 DS-GVO, Rn. 19.

27 S. *Franck*, in: Gola/Heckmann (Hrsg.), DS-GVO BDSG, Art. 15 DS-GVO, Rn. 5.

28 S. *Dix*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, Art. 15 DS-GVO, Rn. 12.

29 S. zum Überblick über die Struktur der Vorschrift z.B. *Bienemann*, in: Sydow/Marsch (Hrsg.), DS-GVO | BDSG, Art. 15 DS-GVO, Rn. 6 ff. und weitergehend zum Detaillierungsgrad *Schmidt-Wudy*, in: Wolff u.a. (Hrsg.), BeckOK Datenschutzrecht, Art. 15 DS-GVO, Rn. 50 ff.

Ein Auskunftsersuchen, das sich explizit darauf bezieht, welche Daten durch den Verantwortlichen verarbeitet werden, enthält bei lebensnaher Auslegung auch einen Antrag auf Auskunft darüber, ob der Verantwortliche überhaupt personenbezogene Daten verarbeitet.[30] Hingegen kann man sich in dem Fall, in dem im Antrag zunächst ein Auskunftsersuchen nach Art. 15 Abs. 1 Hs. 1 DS-GVO enthalten ist, also die Auskunft, ob der Verantwortliche überhaupt personenbezogene Daten der betroffenen Person verarbeitet, einerseits auf den Standpunkt stellen, dass für die erste und die zweite Stufe jeweils ein eigenständiger Antrag zu stellen ist.[31] Andererseits kann man auch in diesem Fall argumentieren, dass der Antrag in Bezug auf die Frage, ob überhaupt personenbezogene Daten verarbeitet werden, auch den Antrag enthält, welche personenbezogenen Daten verarbeitet werden.[32] Wenngleich das Antragsbegehren grundsätzlich ausgelegt werden kann, empfiehlt es sich für die betroffene Person – und damit auch für den Privacy-Assistenten TESTER – die Anträge so konkret wie möglich zu formulieren und deutlich zu machen, ob lediglich Auskunft darüber erteilt werden soll, ob Daten durch den Verantwortlichen verarbeitet werden, oder ob auch Auskunft über die Kategorien der verarbeiteten Daten erteilt werden soll.[33] Mithilfe der Individualisierung der Textbausteine soll indes möglichst eine Einstufigkeit des Auskunftsersuchens in der Form erreicht werden, dass keine Nachfrage des Verantwortlichen mehr notwendig ist.

30 S. *Paal*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 15 DS-GVO, Rn. 21; so wohl auch *EDSA*, Guidelines 01/2022 on data subject rights – Rights of access: "This confirmation [whether or not personal data are being processed] may be communicated separately, or it may be encompassed as part of the information on the personal data being processed."

31 S. z.B. *Paal*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 15 DS-GVO, Rn. 21 und *Däubler*, in: Däubler u.a. (Hrsg.), EU-DSGVO und BDSG, Art. 15 EU-DSGVO, Rn. 8; offenlassend aber auf die inhaltliche Mehrstufigkeit verweisend *Krämer/Burghoff*, ZD 2022, 428 (429).

32 S. *Kamlah*, in: Plath (Hrsg.), DSGVO BDSG TTDSG, Art. 15 DSGVO, Rn. 3; *Dix*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, Art. 15 DS-GVO, Rn. 13.

33 S. für die Verbindung der beiden Anträge auch *Kamlah*, in: Plath (Hrsg.), DSGVO BDSG TTDSG, Art. 15 DSGVO, Rn. 3.

3.4 Inhalt des Antragsbegehrens

Es ist nicht erforderlich, dass die betroffene Person den Antrag begründet oder auf ihr rechtliches oder berechtigtes Interesse verweist.[34] Der Verantwortliche muss aus der Anfrage der betroffenen Person erkennen können, was diese will,[35] ohne dass allzu hohe Anforderungen an die Artikulierung des Antragsbegehrens zu stellen sind.[36]

3.5 Präzisierung des Auskunftsersuchens

EG 63 S. 7 DS-GVO sieht vor, dass der Verantwortliche, der eine große Menge an Informationen über die betroffene Person verarbeitet, verlangen kann, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt. Fraglich ist, ab wann der datenschutzrechtlich Verantwortliche große Mengen von Informationen über die betroffene Person verarbeitet. Dies könnte der Fall sein, wenn zwischen der betroffenen Person und dem Verantwortlichen über mehrere Jahre hinweg ein Dauerschuldverhältnis besteht.[37] Im Kontext der digitalen Selbstvermessung kann eine vertragliche Beziehung zwischen dem Verantwortlichen und der betroffenen Person unter Umständen ebenfalls einen langen Zeitraum umfassen. Charakteristisch für die Selbstvermessung ist gerade die Erfassung und Auswertung von Daten über einen langen Zeitraum hinweg. Ebenfalls sind Nutzer von Selbstvermessungsgeräten eher ambivalent, wenn es darum geht, das Gerät bzw. die Anwendung zu wechseln.[38] Insofern kann im Einzelfall auch im Rahmen der digitalen Selbstvermessung davon ausgegangen werden, dass der Verantwortliche große Mengen an Informationen über die betroffene Person verarbeitet.

34 S. z.B. EuGH, Urteil vom 26.10.2023 – C-307/22, curia, Rn. 38.
35 S. *Klein/Schwartmann*, in: Schwartmann u.a. (Hrsg.), DS-GVO/BDSG, Art. 15 DS-GVO, Rn. 8.
36 S. *Kamlah*, in: Plath (Hrsg.), DSGVO BDSG TTDSG, Art. 15 DSGVO, Rn. 4.
37 *Starke*, ZD 2024, 63.
38 S. dazu schon *Böning u.a.*, in: Friedewald u.a. (Hrsg.), Daten-Fairness in einer globalisierten Welt, 2023, 247 (266).

Die Möglichkeit der betroffenen Person, diese Präzisierung vorzunehmen, setzt ihre ausreichende Informiertheit voraus.[39] Die Präzisierungsanfrage des Verantwortlichen führt nicht dazu, dass die betroffene Person ihr Auskunftsersuchen auch präzisieren muss.[40] Erfolgt keine Präzisierung, so muss umfassend Auskunft erteilt werden.[41] Dennoch kann es auch im Sinne einer Vereinfachung der Ausübung der Betroffenenrechte und im Sinne der angestrebten Transparenz für die betroffene Person von Vorteil sein, wenn sie ihr Auskunftsersuchen entsprechend präzisiert. Es ist durchaus denkbar, dass die betroffene Person Auskunft über einzelne Datenkategorien wie z.B. Blutdruck oder Kalorienverbrauch erhalten möchte.

3.6 Zurverfügungstellung einer Kopie

Nach Art. 15 Abs. 3 S. 1 DS-GVO hat die betroffene Person auch einen Anspruch auf die Zurverfügungstellung einer unentgeltlichen ersten Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung beim Verantwortlichen sind.[42] Im Falle eines elektronischen Antrags sind nach Art. 15 Abs. 3 S. 3 DS-GVO die Informationen grundsätzlich in einem gängigen elektronischen Format zur Verfügung zu stellen.

Bezüglich des Verhältnisses von Art. 15 Abs. 1 DS-GVO zu Art. 15 Abs. 3 S. 1 DS-GVO hat der EuGH mittlerweile entschieden, dass Art. 15 Abs. 1 DS-GVO und Art. 15 Abs. 3 S. 1 DS-GVO Teilaspekte des

39 S. *Klein/Schwartmann*, in: Schwartmann u.a. (Hrsg.), DS-GVO/BDSG, Art. 15 DS-GVO, Rn. 10.

40 S. *Laue u.a.*, in: Laue u.a. (Hrsg.), Das neue Datenschutzrecht in der betrieblichen Praxis, § 4, Rn. 28; *Dix*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, Art. 15 DS-GVO, Rn. 11.

41 S. *Dix*, in: Simitis u.a. (Hrsg.), Datenschutzrecht, Art. 15 DS-GVO, Rn. 11, der sich jedoch für die Zurückweisung eines pauschalen Auskunftsersuchens mit dem Inhalt des Gesetzeswortlauts ausspricht, so auch *Klein/Schwartmann*, in: Schwartmann u.a. (Hrsg.), DS-GVO/BDSG, Art. 15 DS-GVO, Rn. 10; LG Heidelberg, Urteil vom 6.2.2020 – 4 0 6/19, openjur, Rn. 31 ff.; zu denken ist in diesem Fall noch an durch die Verweigerung der Präzisierung rechtsmissbräuchliches Verhalten im Sinne von Art. 12 Abs. 5 DS-GVO, s. dazu FG Berlin-Brandenburg, Urteil vom 26.1.2022 – 16 K 2059/21, openjur, Rn. 94 ff. und *Greve*, in: Sydow/Marsch (Hrsg.), DS-GVO | BDSG, Art. 12 DS-GVO, Rn. 28.

42 Bei der Zurverfügungstellung weiterer Kopien kann nach Art. 15 Abs. 3 S. 2 DS-GVO ein angemessenes Entgelt verlangt werden.

Auskunftsrechts sind[43] und das Recht auf die Zurverfügungstellung einer Kopie kein vom „eigentlichen" Auskunftsanspruch getrennter Anspruch ist.[44] Für einen einheitlichen Anspruch könnte dabei der Wortlaut von Art. 15 Abs. 3 S. 1 DS-GVO sprechen, wenn man davon ausgeht, dass dieser lediglich die Modalitäten des Auskunftsrechts festlegt.[45] Für die Trennung der Ansprüche aus Art. 15 Abs. 1 DS-GVO und Art. 15 Abs. 3 S. 1 DS-GVO könnte unter anderem eine mögliche Überforderung der betroffenen Person bei der bloßen Übermittlung einer Kopie als Ersatz für eine (aufbereitete) Auskunft sprechen.[46]

Für beide Ansichten wird jeweils die Entstehungsgeschichte von Art. 15 DS-GVO herangezogen. Bezüglich Art. 12 DS-RL, der kein Recht auf die Zurverfügungstellung einer Kopie enthielt, entschied der EuGH, dass die Übermittlung einer Übersicht der personenbezogenen Daten zur Wahrung dieses Auskunftsrechts genügt.[47] Die Einführung eines Rechts auf die Zurverfügungstellung einer Kopie in Art. 15 DS-GVO kann man einerseits so interpretieren, dass sich Art. 15 Abs. 3 DS-GVO inhaltlich an Art. 12 DS-RL orientieren soll und der Anspruch auf die Zurverfügungstellung einer Kopie den Auskunftsanspruch aus Art. 15 Abs. 1 DS-GVO nicht erweitert.[48] Andererseits kann man sich auch auf den Standpunkt stellen, dass gerade die Einführung des Art. 15 Abs. 3 DS-GVO der betroffenen Person ein zusätzliches Recht auf die Zurverfügungstellung einer Kopie „des Dokuments oder der Originaldatei" einräumt, da der Gesetzgeber ansonsten die Formulierung des Art. 12 DS-RL beibehalten hätte.[49]

Zum Umfang des Rechts auf die Übermittlung einer Kopie hat der EuGH entschieden, dass Art. 15 Abs. 3 S. 1 DS-GVO der betroffenen Person ein Recht auf den Erhalt einer originalgetreuen und verständlichen Reproduktion aller personenbezogenen Daten zugesteht, die Gegenstand der

43 EuGH, Urteil vom 4.5.2023 – C-487/21, curia, Rn. 33; s. zuvor schon z.B. *Paal*, in: Paal/Pauly (Hrsg.), DS-GVO/BDSG, Art. 15 DS-GVO, Rn. 33 m.w.N.; *Zikesch/Sörup*, ZD 2019, 239 (240); *Wybitul/Brams*, NZA 2019, 672 (675).

44 So z.B. *Koreng*, NJW 2021, 2692 (2693) mit einem Fokus auf die Rechtsfolgenseite; *Bäcker*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, Art. 15 DS-GVO, Rn. 39; *Härting*, CR 2019, 219 (220 f.).

45 So wohl EuGH, Urteil vom 4.5.2023 – C-487/21, curia, Rn. 30 ff.

46 *Bäcker*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, Art. 15 DS-GVO, Rn. 39.

47 S. EuGH, Urteil vom 17.7.2014 – C-141/12 und C-372/12, curia, Zweiter Leitsatz.

48 So wohl *BayLDA*, 8. Tätigkeitsbericht 2017/2018, 46 f.; *Wybitul/Brams*, NZA 2019, 672 (675).

49 S. *Koreng*, NJW 2021, 2692 (2693), Rn. 15; i.d.S. auch OVG Münster, Urteil vom 8.6.2021 – 16 A 1582/20, openjur, Rn. 141.

Verarbeitung sind.[50] Dafür spricht, dass die Abbildung des tatsächlichen Verarbeitungsprozesses die Überprüfung der Rechtmäßigkeit der Datenverarbeitung sowie der Richtigkeit und Vollständigkeit der Daten erheblich erleichtern kann.[51] Dagegen spricht, dass die Datenschutz-Grundverordnung auch an anderen Stellen zwischen Daten und den die Daten enthaltenen Dokumenten unterscheidet.[52]

Problematisch ist im Kontext der Selbstvermessung die Einschränkung des EuGH dahingehend, dass ein Anspruch auf eine Kopie in Form von Auszügen aus Dokumenten, ganzen Dokumenten, Auszügen aus Datenbanken etc. nur besteht, wenn die Zurverfügungstellung einer solchen Kopie unerlässlich ist, um der betroffenen Person die wirksame Ausübung ihrer Rechte zu ermöglichen.[53] Im Kontext der Selbstvermessung werden überwiegend keine Daten aus Dokumenten verarbeitet, sondern Daten verarbeitet, die die betroffene Person dem Verantwortlichen selbst zur Verfügung gestellt hat. Es ist insofern unwahrscheinlich, dass es auf die genaue Reproduktion der Daten ankommt, wie sie beim Verantwortlichen vorliegen.

Weiterhin drängt sich die – in ähnlicher Form bei der Einwilligung diskutierte – Frage auf, ob durch eine Übermittlung aller beim Verantwortlichen vorhandenen Daten die betroffene Person überfordert wird.[54] Allerdings ist die Situation, in der sich die betroffene Person befindet, bei der Ausübung des Auskunftsrechts eine ganz andere als vor der Entscheidung darüber, ob die Einwilligung in die Datenverarbeitung des Verantwortlichen erteilt werden soll, weil kein (subjektiv empfundener) zeitlicher Druck besteht, den gewünschten Dienst des Anbieters in Anspruch nehmen zu wollen. Im Zweifel kann die betroffene Person sich ausführlich

50 EuGH, Urteil vom 4.5.2023 – C-487/21, curia, Rn. 45 und EuGH, Urteil vom 26.10.2023 – C-307/22, curia, Rn. 35; ähnlich weit gehend schon *Koreng*, NJW 2021, 2692 (2693), Rn. 10; für die Übermittlung der Rohdaten z.B. *Laoutoumai/Hoppe*, K&R 2019, 296 (297); *Schwartmann/Klein*, in: Schwartmann u.a. (Hrsg.), DS-GVO/BDSG, Art. 15 DS-GVO, Rn. 28, wenn die in einem Dokument enthaltenen Daten auf eine andere Art zur Verfügung gestellt werden können; *BayLDA*, 8. Tätigkeitsbericht 2017/18, 46; restriktiver z.B. *Zikesch/Sörup*, ZD 2019, 239 (241).

51 S. EuGH, Urteil vom 4.5.2023 – C-487/21, curia, Rn. 39 ff.; EuGH, Urteil vom 26.10.2023 – C-307/22, curia, Rn. 79; *Bienemann*, in: Sydow/Marsch (Hrsg.), DS-GVO | BDSG, Art. 15 DS-GVO, Rn. 33.

52 *Bienemann*, in: Sydow/Marsch (Hrsg.), DS-GVO | BDSG, Art. 15 DS-GVO, Rn. 33 mit Verweis auf Art. 86 DS-GVO und EG 154 DS-GVO; *Laoutoumai/Hoppe*, K&R 2019, 296 (297).

53 EuGH, Urteil vom 4.5.2023 – C-487/21, curia, Rn. 45.

54 So auch angedeutet bei *Bäcker*, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, Art. 15 DS-GVO, Rn. 39.

mit der Kopie der übermittelten Daten beschäftigen, ohne dass dieses zu einem unmittelbaren Nachteil für sie führt. Der Transparenzgrundsatz aus Art. 5 Abs. 1 lit. a DS-GVO kann aufgrund der kognitiven Überforderung gleichwohl tangiert sein.

Im Hinblick auf eine Softwareschnittstelle zum System des Anbieters von Selbstvermessungsgeräten werden die Daten als strukturierte und aufbereitete Daten übermittelt. Bezüglich des Anfragengenerators kann auf die oben aufgeführte Rechtsprechung des EuGH verwiesen werden, nach der im Zweifel Kopien von Dokumenten oder Auszüge daraus verlangt werden dürfen. Ob den Nutzern damit jedoch geholfen ist, bleibt zweifelhaft, weswegen die Anfrage dahingehend konkretisiert werden sollte, ob die Nutzer tatsächlich eine Kopie der verarbeiteten Daten oder eine zusammengefasste Auskunft begehren.

4 Die Ausübung des Auskunftsrechts über die Schnittstelle

Die Schnittstelle zur Intervention schafft Nutzern von Selbstvermessungsgeräten auf technischem Weg den Zugang und die Kontrolle über ihre Daten, bei denen es sich ganz überwiegend um personenbezogene Daten handelt. Durch einen standardisierten Ansatz können Nutzer ihre Daten bei verschiedenen, die Schnittstelle unterstützenden Anbietern von Selbstvermessungsgeräten abfragen und einsehen. Dies umfasst die Möglichkeit, eine Liste aller gespeicherten personenbezogenen Daten zu erhalten, sowie eine Beschreibung dieser Daten und der durchgeführten Datenverarbeitungsaktivitäten.[55] Auch zusätzliche Informationen wie beispielsweise der Zweck der Datenverarbeitung sollen zukünftig abrufbar sein.

5 Die Ausübung des Auskunftsrechts mithilfe des Anfragengenerators

Ein beispielhaftes Template für das Auskunftsrecht nach Art. 15 DS-GVO verdeutlicht die Individualisierbarkeit der Anfrage. Die nach dem Schema $Variable[56] aufgebauten Teile des Templates sind Platzhalter, welche von

55 S. dazu auch die Ausführungen unter 2.1.

56 Das Schema $Variable ist ein feststehendes Schema bei der Verwendung von Velocity. Die Variablen beginnen standardmäßig mit $, bevor der Name der Variable eingefügt wird.

der Template Engine durch die jeweiligen Daten ersetzt werden. Individualisiert werden kann die Ausübung des Auskunftsrechts im Hinblick auf die Daten, über die die betroffene Person Auskunft erhalten möchte, im Hinblick auf mögliche Beschränkungen sowie im Hinblick auf die in Art. 15 Abs. 1 S. 2 DS-GVO aufgeführten Informationen und das Verlangen der Zurverfügungstellung einer Kopie der gespeicherten Daten.[57]

5.1 Erstes Beispiel

Sehr geehrte Damen und Herren,

hiermit übe ich mein Auskunftsrecht gemäß Art. 15 DS-GVO aus.

Ich möchte wissen, ob mich betreffende personenbezogene Daten verarbeitet werden.

Darüber hinaus bezieht sich mein Auskunftsersuchen ausdrücklich nicht auf die in Artikel 15 Abs. 1 Hs. 2 DS-GVO aufgeführten Informationen.

In diesem Beispiel möchte der Nutzer lediglich wissen, ob beim Anbieter personenbezogene Daten über ihn verarbeitet werden. Dementsprechend wird die Anfrage auch nicht im Hinblick auf einzelne Daten konkretisiert. Klargestellt wird jedoch, dass der Nutzer kein Interesse an den in Art. 15 Abs. 1 Hs. 2 DS-GVO aufgezählten Informationen hat.

5.2 Zweites Beispiel

Sehr geehrte Damen und Herren,

hiermit übe ich mein Auskunftsrecht gemäß Art. 15 DS-GVO aus.

Meine Anfrage umfasst sowohl die Frage danach, ob Sie mich betreffende personenbezogene Daten verarbeiten, als auch die Frage danach, welche personenbezogenen Daten verarbeitet werden.

Meine Anfrage betrifft alle Daten, die Sie in der Vergangenheit über mich verarbeitet haben und aktuell verarbeiten.

Darüber hinaus bezieht sich mein Auskunftsersuchen auf die in Artikel 15 Abs. 1 Hs. 2 DS-GVO aufgeführten Informationen.

Über die inhaltliche Zusammenfassung der mich betreffenden durch Sie verarbeiteten personenbezogenen Daten hinaus, fordere ich Sie dazu auf,

57 S. dazu die Ausführungen unter 3.

Ihrer Pflicht zur Übermittlung einer Kopie der gespeicherten personenbezogenen Daten an mich nachzukommen.

In diesem Beispiel stellt der Nutzer klar, dass er sowohl wissen möchte, ob Daten über ihn verarbeitet werden, als auch, welche Daten verarbeitet werden. Der Nutzer präzisiert sein Auskunftsersuchen in der Hinsicht, dass er ausdrücklich Auskunft über alle Daten verlangt, die Gegenstand aktueller oder vergangener Datenverarbeitungsvorgänge sind oder waren. Er hat darüber hinaus ein Interesse an den in Art. 15 Abs. 1 Hs. 2 DS-GVO aufgezählten Informationen und an einer Kopie der verarbeiteten Daten.

6. Fazit

Die zunehmende Datenverarbeitung durch private und öffentliche Stellen in Form der Datafizierung der Umwelt schlägt sich auch in der vermehrten Selbstvermessung mittels Wearables nieder. Durch die potentielle Überforderung der Selbstvermesser aufgrund vermehrter Datenverarbeitungsvorgänge, wird eine effektive und einfache Ausübung der Betroffenenrechte gegenüber den Anbietern von Selbstvermessungsanwendungen und -geräten immer wichtiger. Dabei kann TESTER die betroffenen Personen in der Form unterstützen, dass die Betroffenenrechte zum einem über eine Schnittstelle direkt bei den Anbietern ausgeübt werden und zum anderen per Brief oder E-Mail bei denjenigen Anbietern ausgeübt werden können, welche die Schnittstelle nicht unterstützen.

Bei der Ausübung des Auskunftsrechts können rechtliche Probleme und Fragen aufkommen, die sich auf die Ausübung dieses Rechts über die Schnittstelle oder den Anfragengenerator auswirken. Die Ausübung des Auskunftsrechts setzt die tatsächliche Betroffenheit der betroffenen Person voraus, wenngleich auch die Auskunft erteilt werden kann, dass der Anbieter gar keine Daten über die entsprechende Person verarbeitet. In jedem Fall muss von dem Verantwortlichen sichergestellt werden, dass die das Auskunftsrecht ausübende Person identifiziert werden kann, da eine Auskunft an eine nicht betroffene Person rechtswidrig wäre. Die Identifizierung der betroffenen Person kann durch die Eingabe entsprechender Merkmale, wie z.B. der Anschrift, sichergestellt werden. Im Hinblick auf den Inhalt des Antrags kann man danach unterscheiden, ob die betroffene Person lediglich Auskunft darüber enthalten möchte, ob personenbezogene Daten über sie verarbeitet werden, oder ob sie auch wissen möchte, welche Daten über sie verarbeitet werden. Obwohl der Verantwortliche erkennen können

muss, worauf sich das Auskunftsbegehren bezieht, besteht keine Pflicht der betroffenen Person, den Antrag zu begründen oder auf ein rechtliches oder berechtigtes Interesse hinzuweisen. Bezüglich eines möglichen Präzisierungsverlangens des Verantwortlichen stellt sich die Frage, ab wann im Rahmen der Selbstvermessung große Mengen an Informationen über die betroffene Person verarbeitet werden. Diese Einschätzung ist einzelfallabhängig, kann aber in den Fällen angenommen werden, in denen eine langjährige Vertragsbeziehung zwischen dem Anbieter und dem Nutzer besteht. Zu beachten ist jedoch, dass die betroffene Person im Zweifel einen Anspruch auf die Übermittlung der vollständigen Informationen hat. Dazu gesellt sich der Anspruch der betroffenen Person auf die Übermittlung der in Art. 15 Abs. 1 Hs. 2 DS-GVO aufgeführten Informationen, die sich zum Teil von den nach Art. 13 DS-GVO zu übermittelnden Informationen unterscheiden. Zum Auskunftsanspruch aus Art. 15 DS-GVO gehört auch das Recht der betroffenen Person, eine Kopie, also nach dem Verständnis des EuGH eine originalgetreue und verständliche Reproduktion der verarbeiteten Daten, zu erhalten, wenn dies unerlässlich dafür ist, dass die betroffene Person ihre Recht wirksam ausüben kann. Die Unerlässlichkeit der Übermittlung ganzer Dokumente oder Auszügen aus Dokumenten kann im Kontext der Selbstvermessung fraglich sein, weil überwiegend nur Daten vom Verantwortlichen verarbeitet werden, die die betroffene Person ihm selbst durch die Eingabe oder die Aufzeichnungen der Daten zur Verfügung gestellt hat.

Die Schnittstelle zur Intervention im Projekt TESTER kann es als produktübergreifender Standard dem Anbieter ermöglichen, eine konsistente Reihe von Datenschutzfunktionen zu implementieren, die zur Verbesserung der Interoperabilität und Nutzerfreundlichkeit führen können. Dies erfolgt mithilfe generischer Funktionen, die in eine Vielzahl von Systemen integriert werden können. Der Anfragengenerator bietet den betroffenen Personen die Möglichkeit, die Ausübung ihrer Betroffenenrechte entsprechend ihrer Bedürfnisse zu individualisieren.

Durch den hohen Grad an Individualisierbarkeit und die Vereinfachung der Intervenierbarkeit hinsichtlich der Datenverarbeitung aus Selbstvermessungsgeräten kann TESTER einen Beitrag zur Stärkung des informationellen Selbstbestimmungsrechts von Selbstvermessern leisten.

Literatur

Bayerisches Landesamt für Datenschutzaufsicht (März 2019): 8. Tätigkeitsbericht des Bayerischen Landesamts für Datenschutzaufsicht für die Jahre 2017 und 2018. Ansbach: Bayerisches Landesamt für Datenschutzaufsicht. https://www.lda.bayern.de/media/baylda_report_08.pdf.

BMG (2023): Gemeinsam Digital. Digitalisierungsstrategie für das Gesundheitswesen und die Pflege. Berlin: Bundesministerium für Gesundheit. https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/D/Digitalisierungsstrategie/BMG_Broschuere_Digitalisierungsstrategie_bf.pdf.

Böning, Fabiola; Astfalk, Stefanie; Sellung, Rachelle und Laufs, Uwe (2023): Informiertheit und Transparenz im Kontext digitaler Selbstvermessung. In: Friedewald, Michael; Roßnagel, Alexander; Neuburger, Rahild, Bieker, Felix und Hornung, Gerrit (Hrsg.): *Daten-Fairness in einer globalisierten Welt*. Baden-Baden: Nomos, S. 247-273. doi.org/10.5771/9783748938743.

Calliess, Christian und Ruffert, Matthias (Hrsg.) (2022): *EUV | AEUV. Das Verfassungsrecht der Europäischen Union mit Europäischer Grundrechtecharta. Kommentar.* 6. Aufl. München: 2022.

Däubler, Wolfgang; Wedde, Peter; Weichert, Thilo und Sommer, Imke (Hrsg.) (2020): *EU-DSGVO und BDSG. Kompaktkommentar.* 2. Aufl. Frankfurt a.M.: Bund-Verlag.

Engeler, Malte und Quiel, Philipp (2019): Recht auf Kopie und Auskunftsanspruch im Datenschutzrecht. *Neue Juristische Wochenschrift (NJW)*, 72(31), S. 2201-2206.

EuG m. Anm. Baumgartner, Ulrich (2023): Bestimmung des Personenbezugs von Daten. *Zeitschrift für Datenschutz (ZD)*, 13(7), S. 399-404.

Europäischer Datenschutzausschuss (EDSA) (28.03.2023): Guidelines 01/2022 on data subject rights – Right of access. Version 2.0. https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf.

Gfu Consumer & Home Electronics GmbH (2024): Absatz von Wearables in Deutschland in den Jahren 2015 bis 2023 (in Millionen Stück). *Statista*. https://de.statista.com/statistik/daten/studie/551366/umfrage/absatz-von-wearables-in-deutschland/.

Gola, Peter und Heckmann, Dirk (Hrsg.) (2022): *Datenschutz-Grundverordnung. VO (EU) 2016/679. Bundesdatenschutzgesetz. Kommentar.* 3. Aufl. München: Beck.

Härting, Niko (2019): Was ist eigentlich eine „Kopie"? Zur Auslegung des Art. 15 Abs. 3 Satz 1 DSGVO. *Computer und Recht (CR)*, 35(4), S. 219-225.

Hornung, Gerrit und Wagner, Bernd (2019): Der schleichende Personenbezug. Die Zwickmühle der Re-Identifizierbarkeit in Zeiten von Big Data und Ubiquitous Computing. *Computer und Recht (CR)*, 35(9), S. 565-574.

IDC Corporate (2024): Absatz von Wearables weltweit von 2024 bis 2022 und Prognose bis 2027. *Statista*. https://de.statista.com/statistik/daten/studie/417580/umfrage/prognose-zum-absatz-von-wearables/.

Koch, Getraud (2022): Digitale Selbstvermessung. In: Baur, Nina und Blasius, Jörg (Hrsg.): *Handbuch Methoden der empirischen Sozialforschung*. Wiesbaden: Springer VS, S. 1377-1385. https://doi.org/10.1007/978-3-658-37985-8.

Koreng, Ansgar (2021): Reichweite des datenschutzrechtlichen Auskunftsanspruchs. *Neue Juristische Wochenschrift (NJW)*, 74(37), S. 2692-2694.

Krämer, Michael und Burghoff, Ramon (2022): Praxisgerechter Umgang mit Auskunftsersuchen nach Art. 15 DS-GVO. Empfehlungen für Unternehmen. *Zeitschrift für Datenschutz (ZD)*, 12(8), S. 428-433.

Kremer, Sascha (2018): Das Auskunftsrecht der betroffenen Person in der DSGVO. Eine sorgfältige Aufbereitung für die Praxis im Unternehmen. *Computer und Recht (CR)*, 34(9), S. 560-569.

Kühling, Jürgen und Buchner, Benedikt (Hrsg.) (2024): *Datenschutz-Grundverordnung/BDSG*. Kommentar. 4. Aufl. München: Beck.

Laoutoumai, Sebastian und Hoppe, Adrian (2019): Das Recht auf Erhalt einer Kopie personenbezogener Daten. Gewährt Art. 15 Abs. 3 S. 1 DSGVO ein Recht auf Herausgabe von Dokumenten? *Kommunikation und Recht (K&R)*, (5), S. 296-300.

Laue, Philip; Nink, Judith und Kremer, Sascha (2019): *Das neue Datenschutzrecht in der betrieblichen Praxis*. 2. Aufl. Baden-Baden: Nomos.

Meyer, Bertrand (2009): *Touch of Class. Learning to Program Well with Objects and Contracts*. Heidelberg: Springer.

Paal, Boris P. und Pauly, Daniel A. (Hrsg.) (2021): *Datenschutz-Grundverordnung Bundesdatenschutzgesetz*. 3. Aufl. München: Beck.

Peisker, Yannick (2023): *Der datenschutzrechtliche Auskunftsanspruch. Grundlagen, Reichweite und praktische Probleme des Art. 15 DSGVO im Beschäftigungskontext*. Baden-Baden: Nomos.

Piltz, Carlo (2016): Die Datenschutz-Grundverordnung. Teil 2: Rechte der Betroffenen und korrespondierende Pflichten des Verantwortlichen. *Kommunikation und Recht (K&R)*, (10), S. 629-636.

Plath, Kai-Uwe (Hrsg.) (2023): *DSGVO BDSG TTDSG. Kommentar*. 4. Aufl. Köln: Dr. Otto Schmidt.

Rode, Daniel und Stern, Martin: „Oh Shit, die Uhr" Zur körperlichen Dynamik des Self-Tracker-Werdens", in: Stephan Lessenich (Hrsg.) (2017): *Geschlossene Gesellschaften. Verhandlungen des 38. Kongresses des Deutschen Gesellschaft für Soziologie*. Bamberg. https://publikationen.soziologie.de/index.php/kongressband_2016/article/view/500/pdf_229.

Roßnagel, Alexander (2021): Grundrechtsschutz in der Datenwirtschaft. Vorsorgepflichten in der Data-Governance. *Zeitschrift für Rechtspolitik (ZRP)*, 54(6), S. 173-176.

Schwartmann, Rolf; Jaspers, Andreas; Thüsing, Gregor und Kugelmann, Dieter (Hrsg.) (2020): *DS-GVO/BDSG. Datenschutz-Grundverordnung Bundesdatenschutzgesetz*. 2. Aufl. Heidelberg: C.F. Müller.

Simitis, Spiros; Hornung, Gerrit und Spiecker gen. Döhmann (Hrsg.) (2019*): Kommentar Datenschutzrecht (DSGVO mit BDSG)*. Baden-Baden: Nomos.

Starke, Christian Paul (2024): Der Umgang mit ausforschenden datenschutzrechtlichen Auskunftsersuchen. Was bleibt nach dem Urteil des EuGH zum Einwand des Rechtsmissbrauchs bei zweckwidrig motivierten Auskunftsersuchen? *Zeitschrift für Datenschutz (ZD),* 14(3), S. 63-68.

Statistisches Bundesamt (2021): Umsatz der Branche Datenverarbeitung und Hosting in Deutschland von 2012 bis 2019 und Prognose bis zum Jahr 2025 (in Millionen Euro). 29. Juli 2021. *Statista*. https://de.statista.com/prognosen/314206/datenverarbeitung-und-hosting-umsatz-in-deutschland.

Steiger, Carolin (2024): Feststellung der Identität bei der Geltendmachung eines Auskunftsanspruchs. Überblick und Praxishinweise zur Umsetzung. *Zeitschrift für Datenschutz (ZD)*, 14(3), S. 143-146.

Sydow, Gernot und Marsch, Nikolaus (Hrsg.) (2022): *DS-GVO | BDSG. Handkommentar*. 3. Aufl. Baden-Baden: Nomos.

TIOBE – the software quality company, TIOBE Index for March 2024. https://www.tiobe.com/tiobe-index/.

Wolff, Heinrich Amadeus; Brink, Stefan und Ungern-Sternberg, Antje (Hrsg.) (2023): *BeckOK Datenschutzrecht*. 46. Ed. München: Beck.

Wybitul, Tim und Brams, Isabelle (2019): Welche Reichweite hat das Recht auf Auskunft und auf eine Kopie nach Art. 15 I DS-GVO? Zugleich eine Analyse des Urteils des LAG Baden-Württemberg vom 20.12.2018. *Neue Zeitschrift für Arbeitsrecht (NZA)*, 36(10), S. 672-677.

Zikesch, Philipp und Sörup, Thorsten (2019): Der Auskunftsanspruch nach Art. 15 DS-GVO. Reichweite und Begrenzung. *Zeitschrift für Datenschutz (ZD)*, 9(6), S. 239-245.

Daten informiert teilen: Die Möglichkeiten von Differential Privacy für die Gesellschaft nutzbar machen[1]

Daniel Franzen, Claudia Müller-Birn

Zusammenfassung

Die Nutzung personenbezogener Daten, beispielsweise Mobilitätsdaten, ist für die Bewältigung aktueller gesellschaftlicher Herausforderungen von großer Bedeutung. Allerdings können die benötigten Daten auch einen Eingriff in die Privatsphäre der Datengebenden bedeuten. Die Einschätzung, ob ein Privatsphärenrisiko verhältnismäßig ist, hängt unter anderem vom verwendeten Anonymisierungsverfahren und dem individuellen Privatsphärebedürfnis ab und sollte, im Rahmen einer sogenannten informierten Entscheidung, von den Datengebenden getroffen werden. Wir schlagen daher „Privacy Decision User Interfaces" vor, in denen Datengebenden verständlich kommuniziert wird, wie das verwendete Anonymisierungsverfahren das Privatsphärenrisiko beeinflusst.

Ein solches Anonymisierungsverfahren ist Differential Privacy (DP), das besonders geeignet ist, informierte Entscheidungen zu unterstützen: Im Vergleich zu anderen Verfahren erlaubt DP eine feinere Kontrolle des Kompromisses zwischen der Genauigkeit der weitergebenen Daten (die verrauscht werden) und dem damit verbundenen Privatsphärenrisiko. Allerdings ist die Vermittlung dieses Kompromisses an bisher wenig erforscht. Dadurch wird das Potenzial von DP, informierte Entscheidungen für den Einzelnen aber auch für die Gesellschaft unter Wahrung der Privatsphäre zu unterstützen, bisher zu wenig genutzt.

In unserem Beitrag geben wir einen Überblick über die Herausforderungen und bisherigen Erkenntnisse zur Kommunikation von DP, berichten über unsere Ergebnisse aus zwei empirischen Studien zur Kommunikation des Privatsphäreschutzes durch den Einsatz von *Privacy Decision User*

1 Der vorliegende Beitrag entstand im Rahmen des Verbundprojekts „freemove - Transdisziplinäre Erforschung der Datenschutz-bewussten Verfügbarmachung von Bewegungsdaten für nachhaltige urbane Mobilität", das seit 2021 vom Bundesministerium für Bildung und Forschung gefördert wird (Förderkennzeichen: 01UV2090B).

Interfaces und diskutieren, was diese Ergebnisse für informierte Entscheidungen über die Weitergabe von personenbezogenen Daten bedeuten.

1. Der Wertekonflikt zwischen Genauigkeit und Privatsphäre in Datensätzen

Um die gegenwärtigen Herausforderungen unserer Gesellschaft zu bewältigen, werden Daten benötigt, die die Bedürfnisse der Gesellschaft genau widerspiegeln. Beispielsweise sind für nachhaltige Mobilitätskonzepte Bewegungsdaten erforderlich, die Aufschluss darüber geben, wie Bürger:innen die bestehenden Angebote nutzen und an welchen Stellen Engpässe bestehen. Die Erhebung und Nutzung solcher Daten unterliegt allerdings häufig einem *Wertekonflikt*. Ein solcher Wertekonflikt bezeichnet eine Situation, in der es einen Widerspruch zwischen konkurrierenden oder unvereinbaren Interessen oder Zielen gibt, die von Individuen oder Gruppen als wichtig für ihr Leben empfunden werden (Friedman u. a. 2019). In der Datenerhebung und -nutzung steht der Bedarf an möglichst genauen Daten, um einen Mehrwert für das Gemeinwohl zu erzeugen, dem Bedürfnis des Einzelnen nach Schutz der Privatsphäre gegenüber, da eine solche Datensammlung häufig auch sensible Informationen enthält. Bewegungsdaten können beispielsweise Aufschluss über den Wohn- und Arbeitsort von Individuen geben. Der Vergleich von Bewegungsdaten Einzelner mit denen anderer Personen erlaubt potenziell die Identifikation von sozialen Beziehungen und der Abgleich mit markanten Orten erlaubt Rückschlüsse auf Hobbys, religiöse oder politische Einstellungen, sexuelle Orientierung, sowie die medizinische Verfassung.

Zum Schutz der Datengebenden, aber auch um das Vertrauen von Datengebenden in öffentliche Datensammlungen zu fördern, sollte deshalb dieses Privatsphärerisiko einer Verletzung der Privatsphäre mit effektiven Verfahren reduziert werden. Eine „naive" Anonymisierung, wie das Entfernen von Namen und ähnlichen eindeutigen Identifikatoren, reicht im Allgemeinen nicht aus, da häufig aus vermeintlich nicht personenbezogenen Daten in einem Datensatz auf die Identität oder sensible Informationen der Datengebenden geschlossen werden kann (de Montoje u. a. 2013). Aus diesem Grund modifizieren fortgeschrittene Anonymisierungsverfahren[2] die Daten zusätzlich so, dass das Risiko eines solchen Privatsphäreverlusts verringert wird.

2 Als Anonymisierung bezeichnen wir hier nicht nur das Entfernen von Identifikatoren (des Personenbezugs), sondern auch die Verringerung des Risikos, dass selbst ohne

Die rechtliche Situation in Bezug auf personenbezogene oder anonymisierte Daten ist in der Datenschutz-Grundverordnung (DSGVO) geregelt: Personenbezogene Daten unterliegen strengen Anforderungen und müssen angemessen geschützt werden, während die Verwendung „anonymisierter Daten" durch die DSGVO nicht grundsätzlich eingeschränkt wird. Diese binäre Einteilung spiegelt jedoch die Bandbreite der technischen Anonymisierungsmethoden nur unzureichend wider. Auch fortgeschrittene Anonymisierungsmethoden können eine Verletzung der Privatsphäre nicht gänzlich ausschließen, sondern lediglich das Risiko einer solchen Verletzung reduzieren. Das Schutzniveau, also wie stark dieses Risiko reduziert wird, bewegt sich auf einem kontinuierlichen Spektrum und hängt von der gewählten Methode und von den gewählten Parametern der Methode ab. Ein höheres Schutzniveau („bessere" Privatsphäre) geht dabei auch mit einem höheren Verlust an Datengenauigkeit einher.

Wir erweitern daher die binäre Sichtweise auf Anonymität im Sinne der DSGVO um dieses Kontinuum und widmen uns aus der menschzentrierten Perspektive (Human-Centered Design, Kling u. a. 1998 und Moggridge 2007) dem Wertekonflikt zwischen Datengenauigkeit und Schutz der Privatsphäre. Uns interessiert, wie das Schutzniveau von Anonymisierungsmethoden mit dem individuellen Bedürfnis der Datengebenden nach Privatsphäre in Einklang gebracht werden kann, um individuelle Mobilitätsdaten für die Gesellschaft wertebasiert nutzbar zu machen.

1.1 Informierte Entscheidung zum Teilen von persönlichen Daten

Moderne Anonymisierungsmethoden stellen, analog zu dem anfangs angesprochenen Wertekonflikt, einen Kompromiss zwischen Datengenauigkeit und Privatsphäreschutz dar: Um die Privatsphäre stärker zu schützen, müssen Daten stärker modifiziert werden, was sich jedoch negativ auf die Genauigkeit und damit auch auf den Nutzen der Daten für die Analyse auswirkt. Verfahren wie beispielsweise k-Anonymität erreichen dies durch die Entfernung einzelner Datensätze (Ausreißer) oder durch eine Verallgemeinerung der Daten (Alter: „20-25" statt „23"). DP hingegen modifiziert die Daten durch einen Zufallsprozess (vgl. Abschnitt 2.1). Der Parameter ε von DP erlaubt es den Kompromiss zwischen Schutzniveau und Datenge-

Identifikatoren sensible Informationen aus den gesammelten Daten abgeleitet werden können.

nauigkeit präzise einzustellen. Dabei gilt: Je höher der Wert für den Parameter ε gewählt wird, desto weniger weichen die modifizierten Daten von den tatsächlichen Daten ab. Das resultiert in höherer Datengenauigkeit, allerdings gleichzeitig in einem höheren Risiko für die Privatsphäre. Das angemessene Schutzniveau (d. h. der geeignete Wert für den Parameter ε) ist vom jeweiligen Anwendungsfall abhängig, unter anderem davon, welche Daten von welchen Datengebenden erhoben werden. Wird der Parameter ε (Schutzniveau) zu niedrig gewählt vermittelt DP als fortgeschrittene Anonymisierungsmethode ein hohes wahrgenommenes Schutzniveau, jedoch besteht eine hohe Wahrscheinlichkeit, dass Angreifende auf die sensiblen Daten der Datengebenden schließen können. Mobilitätsdaten sind für eine solche Verletzung der Privatsphäre in besonderem Maße gefährdet, da hier typischerweise die einzelnen Messpunkte mit Zeitstempeln versehen und in Trajektorien verbunden sind. Das bietet zahlreiche Gelegenheiten die Identitäten von Personen aus den vermeintlich anonymisierten Daten wiederherzustellen.

Da es bisher an einer rechtlichen Regelung oder allgemein akzeptierten Standards zum erforderlichen Schutzniveau in unterschiedlichen Kontexten fehlt (Dwork u. a. 2019), ist eine gängige Vorgehensweise, ein angemessenes Schutzniveau zu finden, die sogenannte „informierte Entscheidung": Datengebende sollen alle nötigen Informationen bekommen und auf dieser Grundlage selbst entscheiden, ob das gewählte Schutzniveau dem Zweck der Erhebung angemessen ist oder ob ein höheres Schutzniveau gegeben sein müsste, um dem Privatsphärebedürfnis zu entsprechen. Unter einer informierten Entscheidung verstehen wir gemäß der Definition von Bekker u. a. eine Wahl, die (1) unter Berücksichtigung aller relevanten Informationen und (2) in Übereinstimmung mit den individuellen Überzeugungen getroffen wird (Bekker u. a. 1999). Von entscheidender Bedeutung ist hierbei, dass die wichtigen Informationen in einer verständlichen Art und Weise zur Verfügung gestellt werden, sodass diese Informationen von den Datengebenden in die Entscheidung einbezogen werden können. Die technischen Details von DP sind allerdings zu kompliziert, um sie für Laien verständlich auszudrücken und selbst die Bedeutung des Parameters ε ist schwer zu kommunizieren. Um den Privatsphäreschutz verständlicher zu machen, kann ε allerdings als ein Privatsphärenrisiko formuliert werden: „Wie wahrscheinlich ist es, dass aus den Daten korrekte Informationen über mich abgeleitet werden können?" Das Konzept des „Privatsphärerisikos" ist in der allgemeinen Bevölkerung noch nicht geläufig, aber Risiken im Allgemeinen sind aus anderen Kontexten wie Wettervorhersagen, Glücksspiel

oder der Medizin bekannt. Das Forschungsgebiet der Privacy Decision User Interfaces überträgt die Erkenntnisse zur Risikokommunikation aus diesen Kontexten auf die Privatsphäre. Ziel ist es, eine informierte Entscheidung für oder gegen das Teilen von Daten zu unterstützen.

1.2 Unser Beitrag

Im Rahmen unserer Forschungsarbeit befassen wir uns mit der folgenden übergreifenden Forschungsfrage: „Wie kann die informierte Entscheidung von Laien bei der Nutzung von Differential Privacy mittels Privacy Decision User Interfaces (PD-UIs) effektiv unterstützt werden?“ Nach einer kurzen Einführung zu den Eigenschaften von DP (Kap. 2), beschreiben wir das Design unserer Interfaces und unserer Studien (Kap. 3). Anschließend präsentieren wir die Ergebnisse der Untersuchungen dar(Kap. 4) und diskutieren auf Basis dieser Ergebnisse verschiedene Konsequenzen und Vorgehensweisen für den Einsatz von DP zum Nutzen der Gesellschaft (Kap. 5).

2. Das Potenzial und die Herausforderungen von DP

Der Privatsphäreschutz, der durch DP erreicht werden kann, birgt ein großes Potenzial für informierte Entscheidungen. Allerdings sind noch einige Herausforderungen zu bewältigen, bevor DP dieses Potenzial vollständig entfalten kann. Das folgende Kapitel beleuchtet diese Dualität aus Potenzial und Herausforderungen.

2.1 Differential Privacy und die Vorteile gegenüber anderen Anonymisierungsverfahren

Datensätze, die von urbanen Mobilitäts-Dienstleistenden oder öffentlichen Nahverkehrsanbietenden, aber auch von Citizen Science-Projekten gesammelt werden, können der Gesellschaft helfen, bedarfsgesteuerte Lösungen zu finden. Um bei der Datennutzung die Privatsphäre der Datengebenden zu schützen, werden Daten mit unterschiedlichen Verfahren anonymisiert.

Naive Maßnahmen, wie das Entfernen eindeutiger Identifikatoren (z.B. Namen), sind nicht ausreichend, um die Privatsphäre der Datengebenden

effektiv zu schützen. Der Bezug zu Individuen kann oft leicht wiederhergestellt werden, indem die Daten mit öffentlich verfügbaren Datenquellen, wie beispielsweise Zensusdaten, verknüpft werden (Douriez u. a. 2016, Narayanan u. a. 2008). Gerade bei Bewegungsdaten hat eine Studie gezeigt, dass schon die Kenntnis von zwei Punkten mit Aufenthaltsort und -zeit einer Person ausreicht, um 50% aller Individuen in einem typischen Datensatz eindeutig zu identifizieren (de Montoje u. a. 2013). Selbst ohne eine solche Identifikation könnten sensible Information ermittelt werden. Wenn beispielsweise die Menge aller möglichen Taxifahrten, die eine Zielperson in einem Zeitraum durchgeführt haben könnte, alle an einem sensiblen Ort enden, kann geschlossen werden, dass die Zielperson diesen Ort aufgesucht hat ohne ihre exakte Taxifahrt zu kennen. Daher sind gerade bei Bewegungsdaten effektivere Schutzverfahren nötig.

Zusätzlich zur Entfernung von Identifikatoren modifizieren fortgeschrittene Anonymisierungsverfahren, wie beispielsweise k-Anonymität (Sweeney 2002), die Daten auf gezielte Art und Weise um eine Re-identifikation oder das Lernen einer sensiblen Information zu erschweren. Je mehr die Daten verändert werden, desto stärker ist der Privatsphäreschutz, aber desto ungenauer werden die Daten. Allerdings erlauben auch diese fortgeschrittenen Verfahren keine differenzierten Aussagen zum Schutz der Privatsphäre, beispielsweise hinsichtlich der Wahrscheinlichkeit, dass sensible Informationen aus den Daten erschlossen werden können. Stattdessen werden die Daten nach Anwendung des Anonymisierungsverfahren typischerweise als anonym angenommen. Falls jedoch ein neuer Datensatz gefunden wird, der durch einen Abgleich die Re-Identifikation einer Person ermöglicht, ist der Schutz plötzlich sehr gering. Folglich können Datengebenden lediglich sehr ungenaue Angaben zur Höhe oder Qualität des Schutzes der Privatsphäre kommuniziert werden.

Eine mögliche Lösung könnte DP darstellen. DP wurde als eine mathematische Anonymisierungs-Eigenschaft definiert (Dwork 2006) und kann durch verschiedene Algorithmen erreicht werden (Dwork 2006, Kairouz u. a. 2015, Wang u. a. 2016)[3]. Anonymisierungsverfahren, die die DP-Eigenschaft erfüllen, garantieren exakte Obergrenzen für das Privatsphärenrisiko

3 Die mathematische Definition und die technische Funktionsweise von Differential Privacy wird an dieser Stelle aus Platzgründen nicht im Detail vorgestellt. Im Rest des Beitrags reicht es zu verstehen, dass mit dem Parameter ε der Kompromiss zwischen Genauigkeit der Daten und dem Privatsphäreschutz eingestellt werden kann. Für eine einfache Beschreibung der Arbeitsweise von DP, verweisen wir auf unsere Veröffentlichung (Franzen u. a. 2022).

der Datengebenden. Die DP-Garantie lässt sich vereinfacht wie folgt beschrieben: „Wenn die DP-geschützten Daten weitergegeben werden, dann steigt die Wahrscheinlichkeit, dass jemand Informationen erraten kann, höchstens um diesen Faktor: X". Die Höhe des Faktors kann von den Datensammelnden über den Parameter ε exakt justiert werden, um den Kompromiss zwischen der Genauigkeit der Daten und dem Schutz der Privatsphäre für den jeweiligen Anwendungsfall zu optimieren.

Anonymisierungsverfahren, wie auch DP, nutzen ein Angriffsmodell um zu beschreiben, welcher Privatsphäreschutz erreicht wird. Das Angriffsmodell beschreibt, welches zusätzliche Wissen und welche Fähigkeiten hypothetische Angreifende haben müssen, um sensible Informationen über eine Zielperson aus den Daten zu lernen. Im Unterschied zu allen anderen Anonymisierungsverfahren nimmt das Angriffsmodell von DP an, dass Angreifende bereits alle Informationen außer der sensiblen Information über die Zielperson kennen. Da die Schutzgarantie von DP auf dieser Grundlage gegeben wird, behält sie auch mit der Veröffentlichung von weiteren zukünftigen Datensätzen ihre Gültigkeit. Des Weiteren nimmt DP an, dass Angreifenden stets eine fundierte Vermutung über die sensible Information der Zielperson möglich ist, welche mit einer gewissen Wahrscheinlichkeit korrekt ist. Diese Wahrscheinlichkeit beträgt 100 %, wenn die Information zweifelsfrei aus anderen Quellen verfügbar ist. Aber selbst ohne nützliche Hintergrundinformationen, können Angreifende beispielsweise Ja/Nein-Attribute (wie eine medizinische Diagnose) über einen einfachen Münzwurf mit einer Wahrscheinlichkeit von 50 % korrekt raten. Basierend auf dem Konzept der Wahrscheinlichkeit der Vermutung, modifiziert DP die Daten so, dass sich die Wahrscheinlichkeit der Korrektheit der Vermutung durch die neue Datenweitergabe höchstens um einen bestimmten Faktor (abhängig von dem Parameter ε) vergrößern kann. Der Parameter ε stellt damit den Kompromiss von DP zwischen Privatsphäreschutz und Genauigkeit der Daten dar. Je kleiner der Parameter ε gewählt wird, desto kleiner wird dieser Faktor und desto weniger können Angreifende über die Zielperson herausfinden, aber gleichzeitig verringert sich die Genauigkeit der Daten für die Auswertung.[4]

4 Die Definition und die Funktionsweise von Differential Privacy wird an dieser Stelle aus Platzgründen nicht im Detail vorgestellt. Im Rest des Beitrags reicht es zu verstehen, dass mit dem Parameter ε der Kompromiss zwischen Genauigkeit der Daten und dem Privatsphäreschutz eingestellt werden kann. Für eine einfache Beschreibung der Arbeitsweise von DP, verweisen wir auf unsere Veröffentlichung (Franzen u. a. 2022).

Dieses besondere Angriffsmodell von DP erlaubt es, eine numerische Grenze für das Privatsphärenrisiko zu garantieren, statt lediglich eine ungenaue Versicherung anzugeben, dass „fast kein Risiko" besteht. Da bei DP laut Annahme Angreifende bereits über das maximale Wissen verfügen, ist der Privatsphäreschutz auch nicht davon abhängig, welche Datensätze in der Zukunft verfügbar werden (im Gegensatz zu Verfahren wie k-Anonymität). DP ermöglicht somit eine Kommunikation des genauen Risikos für die Privatsphäre an Datengebende und kann damit eine Grundlage für eine informierte Entscheidung bereitstellen.

2.2 Die Herausforderung von Differential Privacy

DP wird bereits in unterschiedlichen Datenerhebungen eingesetzt, beispielsweise von Microsoft, Apple und Google (Domingo-Ferrer u. a. 2021) oder von der U.S. Zensusbehörde (Kenny u. a. 2021). Allerdings ist die Angabe, dass DP für eine Datensammlung genutzt wird, alleine nicht aussagekräftig. Der Schutz für die Privatsphäre ist *maßgeblich abhängig von dem Parameter ε*. Mit sinnvoll kleinen ε-Werten stellt DP einen guten Privatsphäreschutz dar, aber größere Werte können unter Umständen keinen aussagekräftigen Schutz der sensiblen Daten gewährleisten. Ohne Angabe des Parameters ist es den Datengebenden somit nicht möglich, den Schutz ihrer Daten einzuschätzen (Dwork u. a. 2019).

Die Kommunikation des Privatsphärenrisikos von DP ist mit zwei Herausforderungen konfrontiert: einerseits die Komplexität von DP (Wie erreicht DP den Schutz?) und andererseits die Komplexität von Risikokommunikation (Was bedeutet ein Risiko von 34% und wie kann es verständlich erklärt werden?). In Anbetracht dieser Komplexität könnte seitens der Datensammelnden die Befürchtung bestehen, dass eine leichtfertige Erwähnung des „Risikos" Datengebende von der Weitergabe ihrer Daten abschrecken könnte. Erschwerend kommt hinzu, dass Risikokommunikation kontextabhängig ist, d. h. die Effekte der Kommunikation auf das Risikoverständnis der Datengebenden von dem Kontext des Risikos abhängen. Aus diesem Grund ist die Übertragung der Ergebnisse aus der Forschung zu Risikokommunikation in anderen Fachbereichen, wie beispielsweise aus der Medizin oder dem Katastrophenschutz auf die Privatsphärekommunikation möglicherweise nicht ohne Weiteres möglich. Das führt dazu, dass in der Praxis der gewählte ε-Wert oder die dadurch abgeleiteten Privatsphäregarantien den Datengebenden üblicherweise nicht kommuniziert werden

(Cummings u. a. 2021) und das Potenzial von DP somit nicht genutzt werden kann.

Die bisherigen Forschungsarbeiten zum Thema „Kommunikation von DP" beschränkten sich auf *qualitative* Beschreibungen von DP, wie sie in der Praxis verwendet werden, im Gegensatz zu einer möglichen quantitativen Kommunikation der Höhe des Privatsphäreschutzes: Cummings u. a. identifizierten aus 76 DP-Beschreibungen, die in der Praxis genutzt werden, sechs verschiedene Themen (z. B. „Methode", „Vertrauen" oder „Risiko"). In ihrer Vergleichsstudie (Cummings u. a. 2021) zur Wahrnehmung dieser Themen haben die Autorinnen herausgestellt, dass verschiedene Themen verschiedene Privatsphäreerwartungen der Datengebenden wecken. Xiong u. a. untersuchten in zwei aufeinander aufbauenden Studien den Effekt von Beschreibungen von DP auf die Bereitschaft von Datengebenden, ihre Daten weiterzuzugeben. In der ersten Studie (Xiong u. a. 2020) wurden verschiedene Beschreibungen von DP verglichen. Dabei konnte festgestellt werden, dass einige Faktoren (z. B. die Bekanntheit und das Vertrauen in die datensammelnde Organisation) einen größeren Einfluss auf die Weitergabebereitschaft der Datengebenden haben, als die Unterschiede der DP-Beschreibungen. Mit mehrfach verbesserten Beschreibungen von DP ist es Xiong u. a. gelungen das Verständnis der Studienteilnehmenden bezüglich DP unter bestimmten Voraussetzungen zu verbessern. In ihrer zweiten Studie (Xiong u. a. 2022) untersuchten die Autor:innen zusätzlich den Einfluss von Symbolen und Animationen in PD-UIs. Die Ergebnisse zeigen, dass statische Symbole keinen Nachteil gegenüber Animationen aufweisen, und dass die Teilnehmenden zwar einen stärkeren Privatsphäreschutz bevorzugen, jedoch auch gewillt sind, Privatsphärerisiken für sinnvolle Zwecke zu akzeptieren. Die Ergebnisse dieser bisher durchgeführten Studien sind vielversprechend, was die Kommunikation von Privatsphärerisiken angeht, beziehen sich aber alle auf qualitative Beschreibungen von DP bei denen der Wert des Parameters ε und der daraus resultierender Privatsphäreschutz nicht einbezogen wurde.

Abschließend sei eine weitere Herausforderung für die Kommunikation von Privatsphärerisiken genannt: die individuellen statistischen Kenntnisse, die sogenannte „Numeracy" (Cokely u. a. 2012). Personen mit geringen statistischen Kenntnissen überschätzen, im Gegensatz zu Personen mit besseren statistischen Kenntnissen, oft ihre Fähigkeiten Risiken einzuschätzen (Kruger u. a. 2000). Eine nicht abgestimmte Risikokommunikation könnte diesen Personen ein unbegründetes Sicherheitsgefühl vermitteln und sie damit verleiten, häufiger zu teilen, ohne die wirklichen Konsequenzen ver-

standen zu haben. Dadurch könnten sensible Daten unbeabsichtigt preisgegeben werden.

Zusammenfassend lässt sich sagen, dass DP als erstes Anonymisierungsverfahren das Potenzial birgt das quantifizierte Privatsphärenrisiko einer Datenweitergabe verständlich zu kommunizieren und damit zu einer informierten Entscheidung beizutragen. Um dieses Potenzial allerdings voll zu entfalten, müssen neue Kommunikationsansätze für DP entwickelt werden.

3. Privacy Decision User Interfaces für DP

Im Folgenden beschreiben wir die Überlegungen, die letztlich zur Gestaltung der von uns vorgeschlagenen und evaluierten Kommunikationsansätzen geführt haben.

3.1 Das Ziel von Privacy Decision User Interfaces

Das Ziel unserer User Interfaces ist die Unterstützung einer informierten Entscheidung. Für eine informierte Entscheidung (Bekker u. a. 1999) müssen die Datengebenden entscheiden können, ob sie das Risiko der Datenweitergabe als für den Zweck angemessen empfinden. Dieses Empfinden hängt von individuellen Faktoren ab. Daher ist nicht zu erwarten, dass alle Teilnehmenden sich in der jeweiligen Situation gleich entscheiden, wodurch die Weitergabebereitschaft kein angemessenes Messinstrument für eine informierte Entscheidung darstellt. Stattdessen nehmen wir an, dass eine informierte Entscheidung vorliegt, wenn die Entscheidung der Teilnehmenden mit ihren Privatsphärebedenken korreliert: Wir erwarten, dass Teilnehmende mit niedrigem Privatsphärebedürfnis bei gleichem Grund und erhofften Nutzen der Erhebung auch in unserer Studie öfter ihre Daten teilen als Teilnehmende mit höherem Privatsphärebedürfnis. Um diese informierte Entscheidung zu unterstützen, ist es essenziell, dass Datengebende die Konsequenzen ihrer Entscheidung verstehen. Die technischen Details von DP sind selbst für Expert:innen schwer nachzuvollziehen (Lee u. a. 2011). Daher ist eine Kommunikation der vollständigen Funktionsweise von DP nicht zielführend, um die Konsequenzen einer Datenweitergabe verständlich zu machen. Die Gestaltung der hier vorgeschlagenen PD-UIs fokussiert sich stattdessen auf die Kommunikation der Auswirkungen von DP unter Berücksichtigung des gewählten Privatsphäre-Parameters ε. Die

User Interfaces sollen Datengebenden helfen, die Frage zu beantworten „Was bedeutet die Weitergabe meiner Daten für mein Privatsphärenrisiko?“ DP ist für diese Art der Kommunikation aus zwei Gründen besonders geeignet:

1. Der Schutz durch DP ist unabhängiger von äußeren Faktoren, da DP auf der Annahme basiert, dass Angreifende bereits alles potenziell verfügbare Wissen, außer der sensiblen Information, besitzen.
2. Die Definition von DP selbst beschreibt die Eigenschaft der Privatsphäre-Garantie, nicht aber den Algorithmus, wie diese Garantie erreicht wird. Die Garantie kann durch verschiedene Algorithmen umgesetzt werden und ist daher auch unabhängig vom genutzten Algorithmus formuliert.

Statt also die Funktionsweise eines DP-Algorithmus zu erklären, zielen die hier vorgeschlagenen PD-UIs darauf ab, den Datengebenden das Privatsphärenrisiko zu kommunizieren. Wir nutzen dazu ein Risiko-Modell (Mehner u. a. 2022) für DP. Dieses Modell berechnet aus dem Privatsphäre-Parameter ε ein Privatsphärenrisiko, welches angibt, wie wahrscheinlich es ist, dass Angreifende die sensible Information über die Zielperson richtig vermuten können[5].

Um das Privatsphärenrisiko verständlich zu vermitteln, beziehen wir Berücksichtigung bestehender Forschung zur generellen numerischen Risikokommunikation, zwei Aspekte ein: die *textuelle Vermittlung von Risiken* und der *Einsatz von interaktiven UI-Elementen*. Um den Effekt dieser Aspekte auf die informierte Entscheidung zu untersuchen, wurden zwei aufeinander aufbauende empirische Studien durchgeführt. Im Folgenden werden die betrachteten Optionen für beide Aspekte vorgestellt.

3.2 Studie 1: Textuelle Risikoformate

In der medizinischen Forschung wurden bereits vielfältige Erkenntnisse zur effektiven Risikokommunikation erzielt. Eine Richtung der Forschung in der Medizin fokussiert sich auf die Frage, welche textuellen Formate Patient:innen ein realistisches Risikoempfinden ermöglichen. Aus den empfohlenen Risikoformaten in der Medizin haben wir zwei besonders geeignete

5 Weitere Informationen zu diesem Modell und wie es in den PD-UIs genutzt wird findet sich in unserer Veröffentlichung (Franzen u. a. 2022).

Grundformate, Prozente (z. B. „52 %“) und Häufigkeiten (z. B. „26 aus 50“), ausgewählt, die auf Privatsphärerisiken übertragbar sind. Zusätzlich werden in der Medizin verschiedene Variationen der Risikokommunikation unabhängig vom gewählten Grundformat empfohlen. Im Rahmen der Risikokommunikation von DP-Privatsphärerisiken haben wir zwei vielversprechende Variationen ausgewählt: Eine negative Formulierung „Das Risiko tritt in 52 % der Fälle ein“ kann einen anderen Effekt auf die Entscheidung haben als die äquivalente positive Formulierung „Das Risiko tritt in 48 % der Fälle *nicht* ein“ (sog. „Framing Effect“). Unsere Variation „Outcome Framing“ beschreibt daher explizit beide Wahrscheinlichkeiten. In der Medizin wird ferner empfohlen Risiken mit anderen bekannten Risiken zu vergleichen, um einen intuitiveren Zugang zu ermöglichen. Da DP per Definition immer einen Vergleich zwischen dem Risiko vor und nach der Datenweitergabe darstellt, geben wir in der Variation „Comparison to status quo“ explizit beide diese Wahrscheinlichkeiten an.

Insgesamt ergaben sich aus den Grundformaten und Variationen sechs Risikobeschreibungen: jedes Grundformat jeweils ohne Variation, mit „Outcome Framing“ oder mit „Comparison to status quo“. Als siebte Risikobeschreibung nutzen wir eine gebräuchliche Beschreibung von DP, die kein numerisches Privatsphärenrisiko explizit nennt. Diese sieben Beschreibungen wurden für die erste Studie in eine typische Benutzeroberfläche eingebettet und Studienteilnehmenden im Kontext einer Ride-Sharing App präsentiert (Beispiele in Abb. 1).[6]

3.3 Studie 2: Grafische User Interface-Elemente

Die Repräsentation des Risikos in den verschiedenen textuellen Formaten, kann durch grafische Elemente sinnvoll unterstützt werden. Daher haben wir in einer Vorstudie zunächst aus Antworten zu qualitativen Fragen herausgearbeitet, dass vor allem drei Aspekte für das Verständnis des DP-Risikos wichtig sind:

Erstens ist numerisches Risiko an sich schwer zu verstehen und besonders Datengebende mit geringen statistischen Kenntnissen benötigen Unterstützung, um mit den angezeigten Zahlen umzugehen. Eine vielversprechende Methode ist die grafische Darstellung des Risikos. Wir visualisieren

6 Weitere Informationen zum Design der genutzten UIs und zum Studiendesign können nachgelesen werden in unserer Veröffentlichung zu dieser Studie (Franzen u. a 2022).

das Risiko als Icon Array, das 100 Kreise in einer zweidimensionalen Anordnung zeigt. Einige Kreise sind ausgefüllt und verdeutlichen, wie viele Personen von 100 von dem beschriebenen Risiko betroffen wären. Bei einem Risiko von 22 % wären beispielsweise 22 der 100 Kreise ausgefüllt. Wir vermuten, dass Icon Arrays aufgrund ihrer Anschaulichkeit eine intuitive Darstellung von Risiken bieten und damit insbesondere Personen mit geringen statistischen Kenntnissen helfen können, das Privatsphärenrisiko zu verstehen.

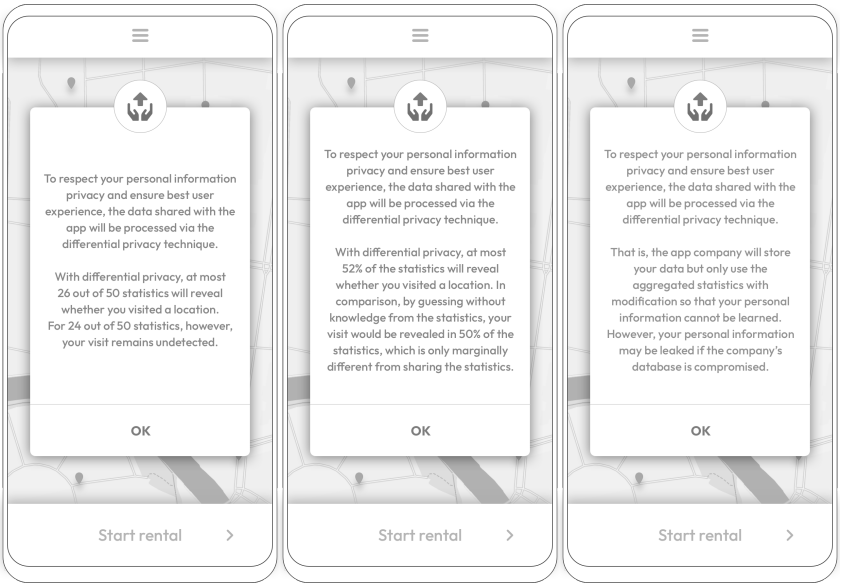

Abbildung 1: UIs mit textuellen Risikoformaten

Quelle: Franzen u.a. 2022

Abbildungslegende: Beispiele der benutzen UIs mit Risikoformaten. Gezeigt sind von links nach rechts: Häufigkeiten mit Outcome Framing, Prozente mit Vergleich zum Status Quo und Beschreibung ohne explizite Nennung des numerischen Risikos

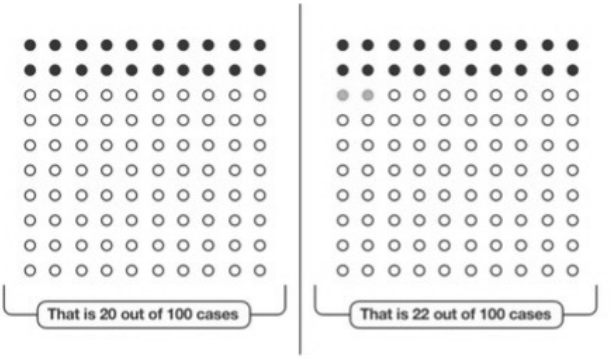

Abbildung 2: Icon-Arrays

Quelle: Franzen u.a. 2024

Abbildungslegende: Beispiele für die Icon Array-Visualisierung, links 20%, rechts 22%

Der zweite Aspekt beim Verständnis von DP ist der Umstand, dass DP zwei Risiken vergleicht: DP nimmt an, dass bereits vor der Datenweitergabe ein gewisses Vorrisiko existiert. Das bedeutet, dass Angreifende schon vor der betroffenen Datenerhebung mit einer gewissen Wahrscheinlichkeit eine korrekte Vermutung zur sensiblen Information anstellen können. DP vergleicht, wie sehr die neue Datenweitergabe dieses Vorrisiko im schlimmsten Falle anheben könnte. Dieser Vergleichscharakter von DP muss vermittelt werden. Eine Möglichkeit ist eine Gegenüberstellung der beiden Risiken. Wir haben daher unsere Benutzeroberfläche vertikal in zwei Hälften zum Risiko vor bzw. nach der Datenweitergabe unterteilt (vgl. Abb. 3).

Außerdem kann die Icon Array-Visualisierung auch den Unterschied zwischen den beiden Risiken in einer anderen Farbe darstellen (vgl. Abb. 2, rechts in grau), um die Intuition über den relativen Anstieg des Risikos weiter zu unterstützen.

Drittens hängt das Vorrisiko, mit dem DP vergleicht, von zahlreichen individuellen Faktoren ab, beispielsweise davon, wie oft eine Person bereits Daten geteilt hat, um welche Daten es sich handelt oder wie die Verteilung der sensiblen Information in der Allgemeinbevölkerung ist. Darüber hinaus können selbst für die gleiche Person unterschiedliche Informationen (wie z. B. verschiedene Orte) unterschiedliche Vorrisiken haben. Ein PD-UI kann daher nicht ein einziges Risikopaar präsentieren. Datengebende müssen vielmehr in der Lage sein, diese Risikopaare für verschiedene Situationen und Vorrisiken zu erkunden. Eine solche Exploration ist in unserem

Abbildung 3: Gegenüberstellung der Risiken in der Benutzeroberfläche

Quelle: Franzen u.a. 2024

Abbildungslegende: Benutzeroberfläche, die den Vergleich der beiden Risiken erleichtert. Links: Informationen zum Vorrisiko mit Bedienfeld „Nicht teilen", rechts: Informationen zum Risiko nach der Datenweitergabe mit Bedienfeld „Teilen"

Privacy Decision UI durch verbundene Slider realisiert (vgl. Abb. 4). Je ein Slider visualisiert das Risiko vor bzw. nach der Datenweitergabe. Datengebende können die Slider auf verschiedene Werte anpassen, wodurch der jeweils andere Slider automatisch anhand des durch DP garantierten Zusammenhangs auf die entsprechende Position gesetzt wird. Auf diese Weise können Datengebende entweder auf der linken Seite das Vorrisiko ihrer individuellen Situation anpassen und so das Risiko nach der Datenweitergabe auf dem rechten Slider sehen oder sie können rechts das maximal tolerierte Risiko nach der Datenweitergabe einstellen und auf dem linken Slider ablesen, bis zu welchem Vorrisiko ihre Informationen durch DP geschützt sind. Dadurch ist es Datengebenden möglich, den Privatsphäreschutz von DP auch für mehrere unterschiedliche Situationen zu explorieren und ein mentales Modell aufzubauen.

Wir erwarten, dass jedes dieser Elemente einen Einfluss auf die informierte Entscheidung haben könnte. Daher haben wir unterschiedliche Kombinationen dieser Elemente in PD-UIs realisiert und für die zweite Studie in eine fiktive Car-Sharing App eingebettet. Exemplarische Darstellungen dieser Benutzeroberflächen sind in Abb. 5 dargestellt.

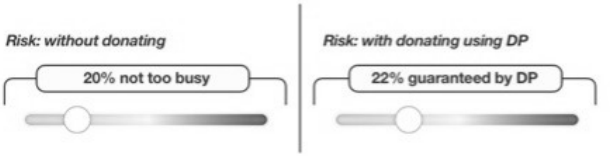

Abbildung 4: Verbundene Slider

Quelle: Franzen u.a. 2024

Abbildungslegende: Slider, mit denen Datengebende den Privatsphäreschutz erforschen können. Links: Slider mit Vorrisiko, rechts: Slider mit Risiko nach Datenweitergabe. Die Bedienung eines Slider führt automatisch zur Anpassung des anderen Sliders, in Übereinstimmung mit der DP-Garantie.

Abbildung 5: UIs mit unterstützenden UI-Elementen

Quelle: Franzen u.a. 2024

Abbildungslegende: Beispiele der erstellten Benutzeroberflächen mit unterschiedlichen Elementen. Gezeigt sind von links nach rechts: „Hybrid“ mit Slider und Icon-Arrays, „Interactive“ nur mit den verbundenen Slidern und “Beschreibung qualitativ” ohne weitere UI-Elemente

3.4 Studiendurchführung

Um den Effekt der textuellen und grafischen Risikokommunikation auf die informierte Entscheidung zu vergleichen, haben wir die Benutzeroberflächen mittels Crowdsourcing auf der Plattform „Mechanical Turk" von Amazon[7] evaluiert. Die Eckdaten der beiden Studien sind in der Tabelle 1 zusammengefasst. Im Rahmen der Studien wurden verschiedene Variablen erhoben, darunter die Entscheidung für oder gegen die Datenweitergabe, bestehende Privatsphärebedenken, das Verständnis der gezeigten Informationen sowie die Zufriedenheit im Umgang mit den UIs. Zusätzlich wurden Kompetenzen und Persönlichkeitsmerkmale der Teilnehmenden, beispielsweise statistische Kenntnisse, erfasst, um zu evaluieren, ob diese Faktoren einen Einfluss auf die Effektivität der UIs haben.

	Studie 1: Textuelle Formate	**Studie 2: Grafische Elemente**
Kontext	Ride-Sharing App	Car-Sharing App
Haupteinfluss	Risikoformate	UI-Elemente
Zielvariable	Verständnis (subjektiv, objektiv)	Informierte Entscheidung (Entscheidungen vgl. mit Privatsphärebedenken)
Rekrutierung	Crowdsourcing (Amazon Mechanical Turk)	
Teilnehmende	343	378
Gruppen	7 (~49 pro Gruppe)	5 (~75 pro Gruppe)
Studiendesign	Zwischenindividueller Vergleich	Zwischenindividueller Vergleich
Zusätzlich betrachtete Variablen	Privatsphärebedenken, statistisches Vorwissen, Geschlecht	Usability, Einprägsamkeit des Risikos / Entscheidung, statistisches Vorwissen, Entscheidungstyp, Kognitionsbedürfnis

Tabelle 1: Eckdaten der Studiendesigns

4. Kommunikation von Privatsphärerisiken für informierte Entscheidungen

Im Folgenden geben wir einen Überblick über die Ergebnisse der beiden Studien.

7 https://www.mturk.com/

4.1 Textuelle Risikokommunikationsformate

Unsere erste Studie untersuchte verschiedene textuelle Risikoformate. Die Ergebnisse zeigen, dass das objektive Verständnis der Teilnehmenden, gemessen mit Kontrollfragen zu Fakten über den Schutz der Privatsphäre, bei allen sieben Risikoformaten etwa gleich ist. Auffallend ist jedoch, dass das Verständnis im Mittel mit durchschnittlich 1,8 von maximal 4 Punkten generell schlecht ist. Dies unterstützt die Vermutung, dass die Vermittlung von Privatsphärerisiken mittels textueller Risikoformate nicht effektiv ist und alternative Ansätze zur Unterstützung notwendig sind.

Die Teilnehmenden wurden auch gefragt, wie gut sie sich auf einer Skala von 1 bis 7 informiert fühlen. Hierbei hat das Risikoformat ohne numerische Risikoangaben zu einer höheren Selbsteinschätzung (5,6 von 7) geführt als die sechs numerischen Risikoformate. Das schlechteste Risikoformat, „Frequenzen mit Vergleich zum Status Quo", ergab eine signifikant schlechtere Einschätzung (4,6 von 7). Die anderen fünf Risikoformate schnitten schlechter (4,9 - 5,1) als das nicht-numerische Format ab, allerdings nicht statistisch signifikant schlechter. Die Tatsache, dass die Teilnehmenden ähnlich viel verstanden haben, sich aber schlechter informiert fühlten, legt nahe, dass Menschen bei der numerischen Risikokommunikation mehr Unterstützung benötigen, um die vermittelten Informationen in eine informierte Entscheidung einfließen lassen zu können.

Darüber hinaus haben wir den Einfluss persönlicher Merkmale auf das Risikoverständnis untersucht. Dabei konnte bestätigt werden, dass das objektive Verständnis von DP, das mit Kontrollfragen gemessen wurde, nicht von diesen Faktoren abhängt. Bei der Analyse der Selbsteinschätzungen zeigte sich jedoch ein Zusammenhang zwischen statistischen Kenntnissen und der Selbsteinschätzung: In einigen Varianten unserer UIs schätzen Teilnehmende mit geringeren statistischen Kenntnissen ihr Verständnis von DP signifikant höher ein als Teilnehmende mit höheren statistischen Kenntnissen. Dies ist, ähnlich dem Dunning Kruger-Effekt, dadurch erklärbar, dass Personen mit geringeren statistischen Kenntnissen sich ihrer Schwächen nicht bewusst sind. Diese Selbstüberschätzung verhindert eine informierte Entscheidung, da sich Personen mit niedrigen statistischen Kenntnissen sicherer fühlen, als es ihrem Verständnis des Privatsphäreschutzes entspricht. Dadurch besteht die Möglichkeit, dass sie ihre Daten mit einem höheren Privatsphärenrisiko weitergeben als beabsichtigt. Ohne

geeignete Gegenmaßnahmen könnte dieser Effekt zu einer Benachteiligung dieser Bevölkerungsgruppen führen[8].

4.2 Grafische Elemente der Risikokommunikation

In unserer zweiten Studie wurde untersucht, welche Elemente einer Benutzeroberfläche die Datengebenden unterstützen können, eine informierte Entscheidung zu treffen. Diese Elemente werden zusätzlich zu den textuellen Risikoinformationen eingesetzt. Um eine informierte Entscheidung zu messen, wurde der Zusammenhang zwischen Entscheidung und Privatsphärebedenken untersucht. In der Benutzeroberfläche, die sowohl Slider als auch Icon-Arrays enthält („Hybrid", siehe Abb. 5), konnte dieser Zusammenhang bestätigt werden. Datengebende, die sich bei dieser Benutzeroberfläche für eine Datenweitergabe entschieden haben, haben im Durchschnitt geringere Privatsphärebedenken (⌀ 5,6 von 7 Punkten) als Datengebende, die sich gegen eine Datenweitergabe entschieden haben (⌀ 6,25). Im Vergleich zu den anderen Benutzeroberflächen ist dieser Effekt drei- bis sechsmal größer (vgl. Abb. 6) und deutet darauf hin, dass die Datengebenden bei dieser Benutzeroberfläche die Risikoinformationen besser in ihre Entscheidung einbeziehen können.
Wir empfehlen daher die Verwendung von PD-UIs, die sowohl eine interaktive Risikoexploration als auch eine grafische Risikovisualisierung beinhalten.

Darüber hinaus haben wir untersucht, wie sich die Benutzeroberflächen auf die Bereitschaft zur Datenweitergabe auswirken: Der Anteil der Personen, die sich für die Datenweitergabe entschieden haben, ist unabhängig von der verwendeten Benutzeroberfläche in etwa gleich (63 %-72 %). Wir konnten in unserer Studie also keinen negativen Einfluss der Risikokommunikation auf die Bereitschaft zur Datenweitergabe feststellen. Stattdessen haben sich bei der Benutzeroberfläche mit Slider und Icon Array andere Teilnehmende, nämlich vor allem diejenigen mit weniger Privatsphärebedenken, für die Datenweitergabe entschieden.

Auch in dieser Studie konnte ein Einfluss der statistischen Kenntnisse nachgewiesen werden: Bei einigen Benutzeroberflächen führte ein geringeres statistisches Vorwissen dazu, dass eher geteilt wurde, während bei

8 Mehr Details zu diesen Ergebnissen sind in unserer Veröffentlichung zu dieser Studie (Franzen u. a. 2022) verfügbar.

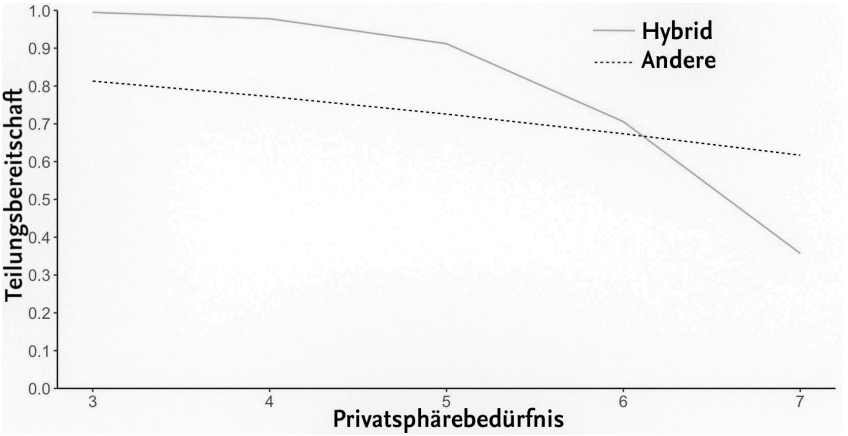

Abbildung 6: Zusammenhang zwischen Privatsphärebedenken und Weitergabebereitschaft

Quelle: Franzen u.a. 2024

Abbildungslegende: Das Diagramm zeigt den Zusammenhang zwischen Privatsphärebedenken (x-Achse) und der Weitergabebereitschaft (y-Achse). Die Benutzeroberfläche mit Slider und Icon-Arrays (Hybrid, durchgezogene Linie) zeigt einen deutlichen Zusammenhang im Vergleich zu den Daten aller anderen Benutzeroberflächen (gestrichelte Linie)

anderen Benutzeroberflächen eher Teilnehmende mit besseren statistischen Kenntnissen teilten. Darüber hinaus fanden wir weitere kleinere Effekte von persönlichen Merkmalen, die die Einprägsamkeit von Risikoinformationen und Zufriedenheit mit den angezeigten Informationen beeinflussen. Die Möglichkeit solcher Effekte sollte bei der Gestaltung von PD-UIs berücksichtigt werden[9].

5. Das Potenzial von DP für die Gesellschaft nutzbar machen.

Unsere Studien geben erste Einblicke wie Risikokommunikation die informierte Entscheidung von Datengebenden unterstützen kann. Diese Unterstützung hat das Potenzial große Datensätze zu generieren, die aus vielen einzelnen informiert gegebenen Datenpunkten bestehen. Diese können

9 Mehr Details zu der Methodik und den Ergebnissen dieser Studie sind in der Veröffentlichung zu dieser Studie verfügbar (Franzen u. a. 2024).

der Gesellschaft helfen, nötige Entscheidungen zu aktuellen Herausforderungen bedarfsgerecht und repräsentativ zu treffen. Um dieses Ziel zu erreichen, leiten wir aus den Ergebnissen unserer Studien nachfolgend Handlungsempfehlungen ab.

5.1 Transparente Kommunikation als Motivator zur Datenweitergabe

In unseren Studien zur Kommunikation von Privatsphärerisiken beim Einsatz von DP haben wir festgestellt, dass quantitative Privatsphärerisiken durchaus zu einer informierten Entscheidung beitragen. Befürchtungen, dass die Erklärung von Risiken das Verständnis von DP negativ beeinflussen könnte, konnten wir in unserer ersten Studie nicht feststellen. Auch die Teilungsbereitschaft wurde durch die transparente Kommunikation von Privatsphärerisiken in der zweiten Studie nicht negativ beeinflusst. Im Gegenteil konnten wir bei der Nutzung von interaktiven und grafisch visualisierten Risikobeschreibungen einen signifikanten Anstieg der Informiertheit der Entscheidung feststellen, d. h. eine Übereinstimmung der Entscheidung mit den Privatsphärebedenken. Diese Ergebnisse sehen wir als klares Zeichen, dass die transparente Kommunikation von Privatsphärerisiken praktikabel und sogar erstrebenswert für die Kommunikation mit Datengebenden ist. Wir sprechen uns daher klar für eine verbesserte transparente Kommunikation von Privatsphärerisiken aus. Transparenz kann perspektivisch das Vertrauen in Datensammlungen unterstützen und damit auch weitere Gruppe von Datengebenden motivieren, Daten zur Verfügung zu stellen.

5.2 Gesellschaftlicher Lernprozess zu Privatsphärerisiken

Das Ziel unserer Forschung ist es, das Potenzial von DP für die Gesellschaft nutzbar zu machen. Nicht alle Datengebenden können über Nacht zu Risiko-Expert:innen werden. Vielmehr verfolgen wir eine mehrstufige Vision: Zunächst muss den Datengebenden während der Entscheidung zur Datenweitergabe die Information zu dem gewählten Kompromiss verständlich kommuniziert werden. Damit können Datengebende unterstützt werden bei der bewussten Entscheidung für oder gegen die Datenweitergabe. Neben individuellen Faktoren, wie momentane Aufmerksamkeit, Umgebungs-

einflüsse oder persönliche Kompetenzen, stellt die Risikokommunikation lediglich einen weiteren Einfluss auf die Privatsphäreentscheidung dar. Selbst bei optimaler Kommunikation kann nicht jede Entscheidung perfekt mit den Privatsphärebedenken der Datengebenden übereinstimmen. Die vorgeschlagene Gestaltung von Benutzeroberflächen für informierte Entscheidungen wird jedoch mit der Zeit mittels vieler solcher Entscheidungen in der Gesellschaft zur Entwicklung von Normen beitragen, die sinnvolle Werte für den Privatsphäreschutz für unterschiedliche Datenkategorien offenlegen. Beispielsweise könnte herausgestellt werden, ob das allgemeine Privatsphärebedürfnis in der Bevölkerung bei Mobilitätsdaten, die aus einzelnen anonymisierten Punkten bestehen, geringer ist als bei verbundenen Punkten, die mittels eines Pseudonyms zu einem umfassenderen Bewegungsprofil verknüpft werden können. In einem zweiten Schritt können diese etablierten Normen die Politik informieren, verpflichtende Mindestwerte für Anonymisierung in verschiedenen Datenkategorien zu formulieren (vgl. Dwork u. a. 2019). Die Einführung von Richtwerten für angemessene Anonymisierungsniveaus könnte auch rechtlich zu mehr Klarheit beitragen, beispielsweise hinsichtlich der Frage, welcher Grad der Anonymisierung erforderlich ist, um eine Beziehung zu einer identifizierbaren natürlichen Person auszuschließen (vgl. DSGVO Erwägungsgrund 26[10]).

In einem dritten Schritt könnten diese Richtwerte schließlich wieder in das Bewusstsein und die Intuition von Bürger:innen eingehen und so ein gemeinsames Verständnis von akzeptablen Risikoniveaus schaffen. Ein solches Verständnis würde im Endeffekt die Risikokompetenzen in der Gesellschaft stärken. Die neue Risikokompetenz könnte erfahrenen Datengebenden mittels einer Variante von DP, der lokalen DP (Kasiviswanathan u. a. 2008), sogar ermöglichen selbst das gewünschte Privatsphäreniveau auszuwählen, bevor Daten weitergegeben werden, und damit den Kompromiss für die individuellen Bedürfnisse zu optimieren: so privat wie nötig, aber so präzise wie damit möglich.

5.3 Individuelle Kompetenzen und Haltungen einbeziehen

Die PD-UIs, die in unseren Studien einen positiven Effekt auf die informierte Entscheidung bewiesen haben, enthalten viel Information und

10 https://dsgvo-gesetz.de/erwaegungsgruende/nr-26/ (zuletzt aufgerufen 4. Juni 2024)

Komplexität und sind daher nicht für alle Nutzer:innen gleichermaßen geeignet. Mit weiteren Erkenntnissen aus der Risikokommunikation in verwandten Forschungsbereichen könnte diese Komplexität möglicherweise noch reduziert werden. Aber selbst mit einfachen UI-Elementen haben unsere Studien an mehreren Stellen aufgezeigt, dass persönliche Eigenschaften einen Einfluss auf die Effektivität der Risikokommunikation haben können. Das könnte beispielsweise dazu führen, dass Datengebende mit geringen statistischen Kenntnissen benachteiligt werden, wie wir oben diskutiert haben. Um dem entgegenzuwirken, schlagen wir PD-UIs vor, die adaptiv auf persönliche Eigenschaften eingehen können. Im Bereich der Privacy Usability wurden Benutzeroberflächen mit unterschiedlichen Detailebenen umgesetzt (Schaub u. a. 2015). Hier werden standardmäßig einfach verständliche Privatsphäre-Icons angezeigt, die aber bei Interesse in einer weiteren Ansicht genauer erklärt werden. Für Nutzer:innen mit höherem Informationsbedürfnis werden auf der dritten Ebene detaillierte Dokumente verfügbar gemacht. Eine ähnliche Umsetzung könnte auch bei der Nutzung von DP die Informationsbedürfnisse von verschiedenen Datengebenden erfüllen, ohne zu überfordern.

Für besonders wichtige Entscheidungen könnten allerdings auch personalisierte UIs sinnvoll sein. Dazu ist zunächst eine Analyse der Kompetenzen der Datengebenden erforderlich. Auf Basis dieser Analyse könnte dann eine Benutzeroberflächenvariation ausgewählt werden, die spezifisch entworfen wurde, um Datengebende in diesem Kompetenzbereich optimal zu unterstützen. In einer typischen Entscheidungssituation ist sicherlich nicht genug Zeit, um zunächst ein persönliches Profil zu erstellen. In Fällen, in denen es um eine langfristige oder wiederholte detaillierte Aufzeichnung von Bewegungsdaten geht, könnte dieser Schritt jedoch angemessen sein. Beispielsweise könnte eine Erhebungsplattform, die einen Pool mit wiederkehrenden Teilnehmenden verwaltet, bei der Registrierung sinnvolle Kompetenzen mittels kurzer Befragungen ermitteln und daraufhin die PD-UIs individuell anpassen.

6. Fazit und Zusammenfassung

Differential Privacy ermöglicht, im Unterschied zu anderen Anonymisierungsverfahren, die präzise Kommunikation des Privatsphärenrisikos unabhängig vom Wissen der Angreifenden. Dadurch eröffnet sich ein enormes Potenzial, Datengebende in die Lage zu versetzen, eine (wirklich)

informierte Entscheidung zu treffen. Um dieses Potenzial jedoch nutzen zu können, muss der Privatsphäreschutz den Datengebenden verständlich kommuniziert werden. Unsere Studien legen nahe, dass eine Kombination aus interaktiver Exploration der Risiken mit grafischen Risikovisualisierungen dazu beitragen kann, Datengebende bei einer informierten Entscheidung zu unterstützen. Allerdings müssen bei der Umsetzung persönliche Kompetenzen berücksichtigt werden, um eine Benachteiligung bestimmter Gruppen zu vermeiden. Die Kombination dieser Ergebnisse verspricht eine verantwortungsvollere Datensammlung und somit eine nachhaltige Lösung für den seit jeher bestehenden Konflikt zwischen dem Schutz der Privatsphäre der Datengebenden und dem gesellschaftlichen Mehrwert, der durch die Daten generiert werden kann.

Literatur

Acquisti, Alessandro; Adjerid, Idris; Balebako, Rebecca; Brandimarte, Laura; Cranor, Lorrie Faith; Komanduri, Saranga; Leon, Pedro Giovanni; Sadeh, Norman; Schaub, Florian; Sleeper, Manya; Wang, Yang und Wilson, Shomir (2017): Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, *50*(3), 44:1-44:41. https://doi.org/10.1145/3054926

Bekker, Hilary; Thornton, Jim G.; Airey, Mark C.; Connelly, James B.; Hewison, Jenny; Robinson, M. B.; Lilleyman, J.; MacIntosh, M.; Maule, Alexander John und Michie, Susan. (1999): Informed decision making: an annotated bibliography and systematic review. *Health Technology Assessment*, *3*(1), 1–156.

Cokely, Edward; Galesic, Mirta; Schulz, Eric; Ghazal, Saima und Garcia-Retamero, Rocio. (2012): Measuring Risk Literacy: The Berlin Numeracy Test. *Judgment and Decision Making*, *7*. https://doi.org/10.1037/t45862-000

Cummings, Rachel; Kaptchuk, Gabriel und Redmiles, Elissa M. (2021): "I need a better description":An Investigation Into User Expectations For Differential Privacy. *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, S. 3037–3052. https://doi.org/10.1145/3460120.3485252

de Montjoye, Yves-Alexandre; Hidalgo, César A.; Verleysen, Michel und Blondel, Vincent D. (2013): Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*, *3*(1), 1376. https://doi.org/10.1038/srep01376

Domingo-Ferrer, Josep; Sánchez, David und Blanco-Justicia, Alberto (2021): The limits of differential privacy (and its misuse in data release and machine learning). *Communications of the ACM*, *64*(7), 33–35. https://doi.org/10.1145/3433638

Douriez, Marie; Doraiswamy, Harish; Freire, Juliana und Silva, Cláudio T. (2016): Anonymizing NYC Taxi Data: Does It Matter? *2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, S. 140–148. https://doi.org/10.1109/DSAA.2016.21

Dwork, Cynthia (2006): Differential Privacy. In M. Bugliesi, B. Preneel, V. Sassone, & I. Wegener (Hrsg.), *Automata, Languages and Programming*. Berlin u.a.: Springer. S. 1–12. https://doi.org/10.1007/11787006_1

Dwork, Cynthia; Kohli, Nitin und Mulligan, Deirdre (2019): Differential Privacy in Practice: Expose your Epsilons! *Journal of Privacy and Confidentiality*, *9*(2), Article 2. https://doi.org/10.29012/jpc.689

Franzen, Daniel; Müller-Birn, Claudia und Wegwarth, Odette (2024): Communicating the Privacy-Utility Trade-off: Supporting Informed Data Donation with Privacy Decision Interfaces for Differential Privacy. *Proceedings of the ACM on Human-Computer Interaction*, *8*(CSCW1), 32, 1-32:56. https://doi.org/10.1145/3637309

Franzen, Daniel; Nuñez von Voigt, Saskia; Sörries, Peter; Tschorsch, Florian und Müller-Birn, Claudia (2022): Am I Private and If So, how Many? Communicating Privacy Guarantees of Differential Privacy with Risk Communication Formats. *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, S. 1125–1139. https://doi.org/10.1145/3548606.3560693

Friedman, Batya und Hendry, David G. (2019): *Value Sensitive Design: Shaping Technology with Moral Imagination*. Cambridge: MIT Press. https://doi.org/10.7551/mitpress/7585.001.0001

Kairouz, Peter; Oh, Sewoong und Viswanath, Pramod (2015): Extremal Mechanisms for Local Differential Privacy. *arXiv:1407.1338*. https://doi.org/10.48550/arXiv.1407.1338

Kasiviswanathan, Shiva Prasad; Lee, Homin K.; Nissim, Kobbi; Raskhodnikova, Sofya und Smith, Adam (2008): What Can We Learn Privately? *2008 49th Annual IEEE Symposium on Foundations of Computer Science*, 531–540. https://doi.org/10.1109/FOCS.2008.27

Kenny, Christopher T.; Kuriwaki, Shiro; McCartan, Cory; Rosenman, Evan T. R.; Simko, Tyler und Imai, Kosuke (o. J.): The use of differential privacy for census data and its impact on redistricting: The case of the 2020 U.S. Census. *Science Advances*, *7*(41), eabk3283. https://doi.org/10.1126/sciadv.abk3283

Kling, Rob und Star, Susan Leigh (1998): Human centered systems in the perspective of organizational and social informatics. *ACM SIGCAS Computers and Society*, *28*(1), S. 22–29. https://doi.org/10.1145/277351.277356

Kruger, Justin und Dunning, David (2000): Unskilled and Unaware of It: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments. *Journal of Personality and Social Psychology*, *77*: 1121–1134. https://doi.org/10.1037//0022-3514.77.6.1121

Lee, Jaewoo und Clifton, Chris (2011): How Much Is Enough? Choosing ε for Differential Privacy. In X. Lai, J. Zhou, & H. Li (Hrsg.), *Information Security*. Berlin u.a.: Springer. S. 325–340. https://doi.org/10.1007/978-3-642-24861-0_22

Leimstädtner, David; Sörries, Peter und Müller-Birn, Claudia (2023): Investigating Responsible Nudge Design for Informed Decision-Making Enabling Transparent and Reflective Decision-Making. *Proceedings of Mensch und Computer 2023*, S. 220–236. https://doi.org/10.1145/3603555.3603567

Mehner, Luise; Tschorsch, Florian und Nunez von Voigt, Saskia (2021): Towards Explaining Epsilon: A Worst-Case Study of Differential Privacy Risks. *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, S. 328–331. https://doi.org/10.1109/EuroSPW54576.2021.00041

Moggridge, Bill (2007): *Designing Interactions*. Cambridge: MIT Press.

Narayanan, Arvind und Shmatikov, Vitaly (2008): Robust De-anonymization of Large Sparse Datasets. *2008 IEEE Symposium on Security and Privacy (SP 2008)*, S. 111–125. https://doi.org/10.1109/SP.2008.33

Schaub, Florian; Balebako, Rebecca; Durity, Adam L. und Cranor, Lorrie Faith (2015): A Design Space for Effective Privacy Notices. *SOUPS 2015 Proceedings*, S. 1–17. https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

Sweeney, Latanya (2002): k-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, *10*(5): 557–570. https://doi.org/10.1142/S0218488502001648

Wang, Yue; Wu, Xintao und Hu, Donghui (2016): Using Randomized Response for Differential Privacy Preserving Data Collection. *Workshop Proceedings of the EDBT/ICDT 2016 Joint Conference*.

Xiong, Aiping; Wang, Tianhao; Li, Ninghui und Jha, Somesh (2020): Towards Effective Differential Privacy Communication for Users' Data Sharing Decision and Comprehension. *2020 IEEE Symposium on Security and Privacy (SP)*, S. 392–410. https://doi.org/10.1109/SP40000.2020.00088

Xiong, Aiping; Wu, Chuhao; Wang, Tianhao; Proctor, Robert W.; Blocki, Jeremiah; Li, Ninghui und Jha, Somesh (2022): Using Illustrations to Communicate Differential Privacy Trust Models: An Investigation of Users' Comprehension, Perception, and Data Sharing Decision. *arXiv:2202.10014*. http://arxiv.org/abs/2202.10014

Mitarbeiterinnen und Mitarbeiter dieses Bandes

Fabiola Böning

ist wissenschaftliche Mitarbeiterin am Fachgebiet für Öffentliches Recht, IT-Recht und Umweltrecht (Leiter: Prof. Dr. Gerrit Hornung, LL.M.) und am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel. E-Mail: f-boening@uni-kassel.de

Stefanie Brückner

ist wissenschaftliche Mitarbeiterin an der Professur für Medical Device Regulatory Science (Prof. Stephen Gilbert) am Else Kröner-Fresenius-Zentrum für Digitale Gesundheit (EKFZ) an der Technischen Universität Dresden. E-Mail: stefanie.brueckner@universitätsklinikum-dresden.de

Dr. Daniel Franzen

ist wissenschaftlicher Mitarbeiter in der Arbeitsgruppe Human-Centered Computing (HCC, Leiterin: Prof. Dr. Claudia Müller-Birn) am Institut für Informatik der Freien Universität Berlin. E-Mail: daniel.franzen@fu-berlin.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

Stefanie Fuchsloch

ist wissenschaftliche Referentin in der NFDI-Geschäftsstelle mit Sitz in Karlsruhe. E-Mail: stefanie.fuchsloch@nfdi.de

Dr. habil. Christian Geminn

ist Privatdozent für Öffentliches Recht und Recht der digitalen Gesellschaft sowie Geschäftsführer der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel und geschäftsführender Gesellschafter der Datenrecht Beratungsgesellschaft (DRBG). E-Mail: c.geminn@uni-kassel.de

Dr. Dagmar Gesmann-Nuissl

ist Professorin für Privatrecht und Recht des geistigen Eigentums an der Technischen Universität Chemnitz. Die Forschungsschwerpunkte der Professur liegen im Innovations- und Technikrecht. E-Mail: dagmar.gesmann@wiwi.tu-chemnitz.de

Dr. Stephen Gilbert

ist Professor für Medical Device Regulatory Science am Else Kröner-Fresenius-Zentrum für Digitale Gesundheit (EKFZ) an der Technischen Universität Dresden. E-Mail: stephen.gilbert@universitätsklinikum-dresden.de

Henrik Graßhoff

ist wissenschaftlicher Mitarbeiter in der Arbeitsgruppe Privacy and Security (PriSec) an der Universität Karlstad.

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 und Open-source Entwickler im „Neo Collective". E-Mail: antonios.hazim@hiwarat.org

Dr. Gunnar Hempel

ist wissenschaftlicher Mitarbeiter der AG Digitale Dienstleistungssysteme und wissenschaftlicher Leiter Arbeitsgruppe ID-Ideal an der Hochschule für Technik und Wirtschaft Dresden. Email: gunnar.hempel@htw-dresden.de

Andrea Horch

ist wissenschaftliche Mitarbeiterin im Forschungsbereich Mensch-Technik-Interaktion am Fraunhofer Institut für Arbeitswirtschaft und Organisation IAO. E-Mail: andrea.horch@iao.fraunhofer.de

Paul C. Johannes, LL.M.

ist wissenschaftlicher Mitarbeiter in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informations-Technikgestaltung (ITeG) an der Universität Kassel. Er ist geschäftsführender Gesellschafter der Datenrecht Beratungsgesellschaft (DRBG) und Rechtsanwalt. E-Mail: paul.johannes@uni-kassel.de.

Dr. Murat Karaboga

ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für System- und Innovationsforschung ISI in Karlsruhe. E-Mail: murat.karaboga@isi.fraunhofer.de

Prof. Ulrich Kelber

war von Januar 2019 bis Juli 2024 der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Er ist Dipl.-Informatiker und war von 2000 bis 2019 Bundestagsabgeordneter für Bonn sowie vom Dezember 2013 bis April 2018 Parlamentarischer Staatssekretär im Bundesministerium der Justiz und für Verbraucherschutz.

Dr. Michael Kubach

ist Wissenschaftler im Team Identitätsmanagement des Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO in Stuttgart und Berlin. Email: michael.kubach@iao.fraunhofer.de

Uwe Laufs

ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO) in Stuttgart im Team Identitätsmanagement.

Stefanie Meyer

ist wissenschaftliche Mitarbeiterin an der Professur für Privatrecht und Recht des geistigen Eigentums (Prof. Dr. Dagmar Gesmann-Nuissl) an der Technischen Universität Chemnitz.
E-Mail: stefanie.meyer@wiwi.tu-chemnitz.de

Dr. Claudia Müller-Birn

ist seit 2019 Professorin am Institut für Informatik der Freien Universität Berlin und Leiterin der Arbeitsgruppe Human-Centered Computing (HCC). In ihrer interdisziplinären Forschung fokussiert sie sich auf Human-AI Collaboration und befasst sich aktuell vor allem mit Fragen der Privatsphäre bei Datenspenden und der Gestaltung von Erklärungen in datengetriebenen Systemen. E-Mail: clmb@inf.fu-berlin.de

Dr. Maxi Nebel

ist wissenschaftliche Mitarbeiterin in der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) am Wissenschaftlichen Zentrum für

Informationstechnik-Gestaltung (ITeG) an der Universität Kassel sowie geschäftsführende Gesellschafterin der Datenrecht Beratungsgesellschaft. E-Mail: m.nebel@uni-kassel.de

Dr. Crispin Niebel

ist wissenschaftlicher Referent bei acatech — Deutsche Akademie der Technikwissenschaften. E-Mail: niebel@acatech.de

Alexander Orlowski

ist ehemaliger wissenschaftlicher Mitarbeiter des Internationalen Zentrums für Ethik in den Wissenschaften der Universität Tübingen. Als Techniksoziologe erforschte er die Auswirkungen von Smart Homes und anderer KI-Technologien auf die Gesellschaft.

Dr. Andrea Pfennig

leitet den Forschungsbereich Psychiatrische Epidemiologie und Verlaufsforschung an der Klinik und Poliklinik für Psychiatrie und Psychotherapie des Universitätsklinikums Carl Gustav Carus der Technischen Universität Dresden. Sie ist Oberärztin der Station für Affektive Störungen und des Früherkennungszentrums dieser Klinik sowie der Tagesklinik für Junge Menschen am Zentrum für Seelische Gesundheit des Universitätsklinikums. E-Mail: andrea.pfennig @universitätsklinikum-dresden.de

Dr. Abel Reiberg

ist wissenschaftlicher Referent bei acatech — Deutschen Akademie der Technikwissenschaften. E-Mail: reiberg@acatech.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

Christopher Ruff

ist wissenschaftlicher Mitarbeiter, seit 2010 im Bereich Identity-Management am Fraunhofer Institut IAO in Stuttgart tätig. Herr Ruff ist Projektleiter des interdisziplinären Konsortialprojektes „DAMA", gefördert durch die Baden-Württemberg Stiftung. E-Mail: christopher.ruff@iao.fraunhofer.de

Dr. Stefan Schiffner

ist Professor für IT-Security und Rechnernetze an der Beruflichen Hochschule Hamburg. Zwischen 2013 und 2017 hat er für die Europäische Cybersicherheitsagentur ENISA gearbeitet. E-Mail: stefan.schiffner@bhh.hamburg.de

Dr. Stephan Schindler

ist wissenschaftlicher Mitarbeiter am Fachgebiet für Öffentliches Recht, IT-Recht und Umweltrecht (Leiter: Prof. Dr. Gerrit Hornung, LL.M.) und am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel. E-Mail: stephan.schindler@uni-kassel.de

Dr. Anna-Raphaela Schmitz

ist wissenschaftliche Referentin bei acatech — Deutsche Akademie der Technikwissenschaften. E-Mail: schmitz@acatech.de

Lukas Schmitz

ist wissenschaftlicher Mitarbeiter und Doktorand im interdisziplinären Forschungsprojekt "DIPCY –Disruptionen vernetzter Privatheit" an der TU Dresden. E-Mail: lukas.schmitz@tu-dresden.de

Dr. habil. Peter E. H. Schwarz

ist Professor für Prävention und Versorgung des Diabetes mellitus Typ 2 am Universitätsklinikum Carl Gustav Carus der Technischen Universität Dresden, Forschungsgruppenleiter am Paul-Langerhans-Institut Dresden und President-Elect der International Diabetes Federation. E-Mail: peter.schwarz@universitätsklinikum-dresden.de

Dr. York Sure-Vetter

ist Direktor des Vereins Nationale Forschungsdateninfrastruktur (NFDI) e.V. mit Sitz in Karlsruhe und Professor am KIT mit den Forschungsschwerpunkten Künstliche Intelligenz und Data Science. E-Mail: york.sure-vetter@nfdi.de

F. Gerrik Verhees

ist Arzt und wissenschaftlicher Mitarbeiter an der Klinik und Poliklinik für Psychotherapie und Psychosomatik am Universitätsklinikum Carl Gustav Carus der Technischen Universität Dresden. E-Mail: falkgerrik.verhees @universitätsklinikum-dresden.de

Dr. Oliver Vettermann

ist wissenschaftlicher Mitarbeiter bei FIZ Karlsruhe mit Expertise im Verfassungsrecht, Datenschutz- und IT-Sicherheitsrecht einschließlich feministischer und rechtsethischer Aspekte. E-Mail: oliver.vettermann@fiz-karlsruhe.de

Dr. Marco Wedel

ist Politologe und wissenschaftlicher Mitarbeiter am Lehrstuhl für Arbeitslehre, Technik und Partizipation, sowie am Lehrstuhl für Fachdidaktik Arbeitslehre. Seine Forschungstätigkeiten konzentrieren sich auf die Themen Digitalisierung, Künstliche Intelligenz und Medienkompetenz. Er ist Mitherausgeber des Journals „Innovation - The European Journal of Social Science Research" und Vorstandsmitglied der European Association for the Advancement of the Social Sciences. E-Mail: marco.wedel@tu-berlin.de

Alexandra Wudel

ist Geschäftsführerin der FemAI GmbH und berät Regierungen, NGOs und privatwirtschftliche Akteure bei der Erstellung und Umsetzung von KI-Ethik Richtlinien. 2024 wurde Sie mit dem „AI Person of the Year" Award ausgzeichnet. E-Mail: alexandra.wudel@fem-ai.com