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.