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

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

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

2. Die Beiträge

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

Fairness und Schutz schwacher Interessen

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

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

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

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

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

Fairer Wettbewerb in der Datenökonomie

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

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

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

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

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

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

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

Fairness und Governance

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

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

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

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

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

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

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

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

Desinformation

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

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

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

Technische Ansätze des Daten- und Identitätsmanagement

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

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

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

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

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