Die Beiträge

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

Künstliche Intelligenz und Selbstbestimmung

Die Beiträge in Teil I gehen der Frage nach, in welcher Weise KI – sowohl vom theoretischen Konzept als auch von der Umsetzung her – einen Paradigmenwechsel in der Informationsverarbeitung bewirkt. Dabei steht im Vordergrund, welche neuen Herausforderungen sich damit für individuelle und gesellschaftliche Werte, insbesondere die Selbstbestimmung stellen.

Rainer Mühlhoff (Universität Osnabrück) argumentiert in seinem Kapitel, dass die zentrale Herausforderung des Datenschutzes im Zeitalter von KI darin liegt, die Vorhersage sensibler Informationen über Menschen und Gruppen rechtlich zu adressieren. Denn die „prädiktive Analytik" mache es möglich, aus der Verknüpfung von Verhaltensdaten (z. B. Nutzungs-, Tracking- oder Aktivitätsdaten) mit (überwiegend) anonymen oder anonymisierten Daten viele weitere Aussagen über persönliche Eigenschaften differenzierter Gruppen von Menschen zu machen – etwa über Kaufkraft, Geschlecht, Alter, sexuelle Orientierung, ethnische Zugehörigkeit etc. Dadurch hätten die Daten anderer Menschen Auswirkungen auf einen selbst und die eigenen Daten Auswirkungen auf andere Menschen – auch wenn die Daten als „nicht personenbezogene" Daten verarbeitet werden. Indem die nachfolgende gesellschaftliche Praxis einzelne Personen statistischen Gruppen zuordnet, werden die vorausgesagten statistischen Eigenschaften auf diese konkreten Personen angewendet. Die so entstehenden Missbrauchspotenziale würden vom geltenden Datenschutzrecht nicht reguliert und die Verwendung anonymisierter Massendaten finde in einem weitestgehend rechtsfreien Raum statt. Mühlhoff plädiert deswegen für einen datenschützerischen Ansatz, bei dem einerseits prädiktive Informationen rechtlich personenbezogenen Daten gleichgestellt werden und andererseits in definierten Anwendungsbereichen (z. B. bei Haftentscheidungen) die Herstellung prädiktiver Risiko-Modelle untersagt wird.

Rita Jordan geht in ihrem Kapitel ebenfalls von der Beobachtung aus, dass mit dem Einsatz selbstlernender Algorithmen nicht nur der Umfang und die Geschwindigkeit, mit der Daten erfasst, verarbeitet und ausgewertet werden, zunimmt, sondern auch die Abgrenzbarkeit zwischen personenbezogenen und nicht personenbezogenen Daten verschwimmt. Da-

durch gerieten die Zwecke des Datenschutzrechts (Persönlichkeitsschutz, informationelle und demokratische Selbstbestimmung) und seine Schutzprinzipien (u. a. Zweckbindung, Datenminimierung und Transparenz) in Spannung zu den Gewinninteressen datenbasierter Geschäftsmodelle und dem herrschenden Innovationsdruck. Die Abgrenzbarkeit von personenbezogenen und nicht-personenbezogenen Daten sei aber zentral für das dogmatische Fundament der EU-Datenschutz-Grundverordnung. Jordan macht deutlich, wie individuellen Nutzerinnen und Nutzern eine aufgeklärte Rechtsausübung praktisch erschwert wird, beispielsweise durch immer kleinteiligere Datenschutzerklärungen. Sie erläutert, wie sich dies bei der Digitalisierung von Städten manifestiert, wo sich die Innovationskraft algorithmischer Datenverarbeitung für Nachhaltigkeits- und Verkehrsziele mit der physischen Oberfläche urbaner Erfahrungs- und Handlungsräume verschränken soll. Wegen der Ubiquität der erfassten Daten und der damit einhergehenden Risiken für Privatheit und Selbstbestimmung sei eine grundlegende Rekonzeptualisierung des Datenschutzrechts sowie eine Demokratisierung der Technologieentwicklung -- insbesondere im Bereich KI-basierter Technologien – in städtischen Räumen notwendig.

Jörn Lamla (Universität Kassel) beleuchtet in seinem Kapitel über die KI als hybride Lebensform schließlich das Wechselverhältnis von Mensch und digitaler Anwendung: KI setze mit ihren Herausforderungen das humanistische Selbstverständnis unter Druck. Der Beitrag argumentiert, dass dies zurecht geschieht, dabei jedoch mit einer verkürzenden Gegenüberstellung operiert wird. Demnach seien KI-Technologien zwar paradigmatisch für die expansive Dynamik hybrider Lebensformen, die Menschen und Maschinen in Feedbackschleifen verklammern, deren Charakter werde aber immer noch verkannt. Die Technologie entwickle sich zu einem Paradigma, das nach Lamla drei Aspekte umfasst, die bei der Analyse des Verhältnisses von Mensch und Maschine und der gesellschaftlichen Auswirkungen zusammen gedacht werden müssten: 1) die sich verstärkende Hybridisierung von Mensch und Maschine, 2) die Datafizierung des Lebens und 3) eine Algorithmisierung, also eine permanente Weiterentwicklung und das Lernen von Algorithmen aus Hybridisierung und Datafizierung. Angesichts der zentralen Rolle, die Digitalisierung und insbesondere KI-Technologien in unserer Gesellschaft spielen, plädiert Lamla entgegen der vorherrschenden kybernetischen Sichtweise für eine Reflektion der Dominanzstruktur des digitalen Analogismus. Um dieser Entwicklung wirksam und kritisch entgegenzutreten, so die These, braucht es mehr als die Beschwörung humanistischer Werte: Es bedürfe eines besseren Verständnisses für die ontologische Heterogenität der gesellschaftlichen Existenzweisen, die in hybriden Lebensformen versammelt sind.

Künstliche Intelligenz, Profiling und Überwachung

Überwachung und Profiling (vor allem für staatliche Akteure wie Strafverfolgungsbehörden und Geheimdienste) sind seit langem treibende Kräfte bei der Entwicklung von KI-Verfahren. Die Beiträge in Teil II fokussieren auf die Fragen, welche Rolle KI hier spielen kann, wie effektiv Betroffenenrechte gewährleistet werden können und wie gut das entstehende europäische Recht auf die absehbaren Herausforderungen reagiert.

Stephan Schindler und *Sabrina Schomberg* (Universität Kassel) beleuchten den aktuellen Verordnungsentwurf der Europäischen Kommission zur Regulierung künstlicher Intelligenz (AI Act), mit dem ein einheitlicher Rechtsrahmen für die Entwicklung, Vermarktung und Verwendung künstlicher Intelligenz im Einklang mit den Werten der Europäischen Union geschaffen werden soll. Sie stellen dabei die Frage, ob es sich mit Blick auf Anwendungen der biometrischen Erkennung um einen großen Wurf oder lediglich um Symbolpolitik handelt. Die biometrische Erkennung nimmt im Verordnungsentwurf eine herausgehobene Stellung ein; insbesondere sieht sie ein Verbot der Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken vor. Von diesem Verbot gäbe es allerdings zahlreiche Ausnahmen, so dass die biometrische Echtzeit-Fernidentifizierung in vielen spezifischen Anwendungskontexten mit mehr oder weniger strikten Auflagen (Dokumentations- und Aufzeichnungspflichten, menschliche Aufsicht) doch betrieben werden könne. Insgesamt begrüßen Schomberg und Schindler den Verordnungsentwurf, kritisieren aber die Ausnahme in ihrer Vielzahl und Breite als problematisch und weisen darüber hinaus auf weitere offene Fragen hin, die insbesondere den Einsatz biometrischer Systeme durch staatliche Stellen zu Strafverfolgungszwecken betreffen.

Jasmin Schreyer (Universität Erlangen-Nürnberg) untersucht in ihrem Kapitel den Datenschutz als zentrale Machtfrage in der Plattformökonomie. Spätestens seit den Snowden-Enthüllungen sei klar, dass das Internet mit seinen scheinbar unbegrenzten Möglichkeiten zur Datensammlung ein Herrschaftsinstrument sei, das nicht nur von staatlichen Akteuren, sondern vor allem auch von international agierenden Datenunternehmen genutzt wird. Obwohl die früheren Hoffnungen auf eine demokratisierende Wirkung des Internet mittlerweile ad absurdum geführt worden seien, inszenierten sich die Plattformanbieter als neutrale Vermittlungsinstanzen und propagierten, dass ihre Datensammlungen eine Form der „höheren" Intelligenz ermögliche, die Wissen, Wahrheit und Objektivität generiere. Schreyer zeigt auf, welche Wirkung das von den Akteuren akkumulierte Wissen über vergangene, gegenwärtige und zukünftige Präferenzen, Ein-

stellungen und Verhalten auf die betroffenen Subjekte hat. Dies führe bei den betroffenen Subjekten zu einer Internalisierung des Machtverhältnisses sowie zu einer Selbstkontrolle und Normierung des Verhaltens. Die Autorin betont, dass sich dieser panoptische Zustand weiter verschärfen werde.

Matthias Marx und *Alan Dahi* berichten in ihrem Kapitel über praktische Erfahrungen bei der Durchsetzung von Betroffenenrechten beim US-amerikanischen Unternehmen Clearview AI, das sich auf KI-gestützte Gesichtserkennung spezialisiert hat. Im Jahr 2020 wurde bekannt, dass Clearview AI zum Zwecke der Gesichtserkennung rechtswidrig mehr als zwanzig Milliarden Fotos von Gesichtern im Internet gesammelt und ausgewertet hatte. Die Autoren zeichnen den Weg einer Beschwerde samt der dabei auftretenden Hindernisse nach, die beim Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit eingereicht wurde. Zudem beleuchten sie einige der rechtlichen Fragen, darunter die Anwendbarkeit der DSGVO, die Rechtmäßigkeit der Verarbeitung sowie die Handlungsmöglichkeiten der Aufsichtsbehörden. Schließlich werden Entscheidungen anderer europäischer Aufsichtsbehörden zu Clearview AI kurz vorgestellt. Der Beitrag demonstriert, wie schwierig die Wahrnehmung grundlegender Betroffenenrechte im Falle eines US-amerikanischen Unternehmens sein kann.

Schließlich befassen sich *Marianne von Blomberg* und *Hannah Klöber* (Universität Köln) in ihrem Beitrag mit dem chinesischen Sozialkreditsystem (SKS), das nicht nur die finanzielle Kreditwürdigkeit der Bürger, sondern deren Vertrauenswürdigkeit im weiteren Sinne ermitteln soll. Die Pläne sehen vor, dass Sozialkreditdossiers für natürliche Personen auf zentraler Ebene angelegt und darin Informationen über ordnungs- und gesetzeswidriges Verhalten gespeichert werden. Anders als ihre Vorgänger sollen die modernen Sozialkreditdossiers transparent, den betroffenen Personen zugänglich und von ihnen korrigierbar sein. Der Beitrag beleuchtet deshalb die lange Tradition personenbezogener Dossiers in China und fragt, ob sich das SKS fundamental von vorherigen Dossiersystemen unterscheidet. Dazu analysieren die Autorinnen den aktuellen Rechtsrahmen für personenbezogene Sozialkreditdossiers im Hinblick auf den Transparenzanspruch des SKS. Sie erläutern, dass eine wachsende Anzahl von lokalen und sektoralen Verordnungen die Verwaltung persönlicher Sozialkreditinformationen regulieren. Ihre Vielfältigkeit einerseits und die nicht standardisierte Sammlung und Verarbeitung von Informationen unter Einbeziehung verschiedener Akteure andererseits erschwerten jedoch das Einsehen und die Korrektur der Dossiers. Um dem Anspruch der Transparenz gerecht zu werden bedürfte es daher einer Vereinheitlichung

des rechtlichen Rahmens des SKS und einer eindeutigen Definition von „Sozialkredit".

Künstliche Intelligenz und Nutzendenverhalten

Die Beiträge in Teil III befassen sich mit der Frage, welche menschlichen Faktoren bei der Wahrung von Privatheit und Selbstbestimmung eine Rolle spielen. Dazu werden einerseits KI-basierte Möglichkeiten diskutiert, die typische menschliche Faktoren entweder ausnutzen oder die Nutzenden bei einem Datenschutz wahrenden Verhalten unterstützen können. Andererseits werden menschliche Faktoren im Umgang mit KI am Beispiel der Nutzung von Messenger-Diensten diskutiert.

Der Beitrag von *Hannah Ruschemeier* (Fernuniversität Hagen) dreht sich um das so genannte *Privacy Paradox*, welches beschreibt, dass Menschen zwar regelmäßig bekunden, wie wichtig ihnen Privatsphäre und Datenschutz ist, dieser Selbsteinschätzung aber keine entsprechenden Taten folgen lassen. Unternehmen nutzten dieses Phänomen aus oder förderten es sogar, so dass viele Personen trotz der betonten Wichtigkeit von Privatheit und Selbstbestimmung niedrigschwellig oder gar anlasslos persönlichste Informationen über sich preisgeben. Diese Diskrepanz zwischen Selbsteinschätzung und realem Verhalten sollte – so die Argumentation der Autorin – vom Recht nicht unbeachtet bleiben. Privatheit als Konzept in der Vorstellung vieler Menschen könne unendlich viele Facetten abdecken, die sich nur teilweise oder auch gar nicht mit konkreten persönlichen Verhaltensweisen überschneiden. Das Recht reflektiere diese realen Voraussetzungen von Privatheit jedoch bisher unzureichend, wie das Beispiel der datenschutzrechtlichen Einwilligung zeige. Zur Adressierung dieser Problemlage wird eine veränderte Ausrichtung des Datenschutzes von einem höchstpersönlichen Gut hin zur Regelung kollektiver Auswirkungen und institutioneller Verantwortung angeregt.

Leen Al Kallaa und Kolleginnen und Kollegen (Universität Bochum) befassen sich in ihrem Kapitel mit der Rolle, die Datenschutz und Datensicherheit bei der Messenger-Auswahl und -Nutzung unter arabischsprachigen Nutzerinnen und Nutzer spielen. Wie bei anderen Nutzendengruppen gehörten Instant Messenger auch bei dieser Gruppe, die in anderen Untersuchungen meist unterrepräsentiert ist, zu den am häufigsten genutzten Smartphone-Apps. Im Rahmen einer empirischen Untersuchung fand das Autorenteam heraus, dass die Änderung wichtiger Datenschutzaspekte in den Nutzungbedingungen von Whatsapp im Frühjahr 2021 von der befragten Gruppe überwiegend nicht wahrgenommen wurde: Lediglich 8 %

der Befragten hätten einen Messenger-Wechsel erwogen. Insgesamt bestätigt die Studie, dass die Gründe gegen den Wechsel zu einem sichereren Messenger vor allem die Netzwerkeffekte sind: An erster Stelle steht die Frage, wie viele Bekannte man erreichen kann.

Künstliche Intelligenz, Desinformation und Deepfakes

Teil IV dreht sich um Fragen der Desinformation, zu deren Erstellung und Verbreitung seit einigen Jahren erfolgreich KI-Verfahren genutzt werden. Dies reicht von der Extraktion von Persönlichkeitsmerkmalen, über Social Bots und Verfahren des Mikrotargeting bis hin zu Deepfakes, also realistisch wirkende, aber synthetische Medieninhalte. Während bspw. der Einsatz von Mikrotargeting im US-Präsidentschaftswahl 2012 noch als modern und innovativ galt, wurde spätestens mit dem Fall „Cambridge Analytica" klar, welches Gefahrenpotenzial hier für die demokratischen Strukturen und Prozesse sowie deren Standards entsteht. Seither sind Bestrebungen im Gange die Gefahren mit unterschiedlichsten Mittel einzuhegen.

Zunächst widmen sich *Anna Louban* (HWR Berlin) und Kolleginnen und Kollegen dem relativ neuen Phänomen der Deepfakes, also durch KI-Methoden generierte oder manipulierte Bilder, Audios und Videos, die politische Desinformation und Propaganda in videographischer Form transportieren können. Sie fragen interdisziplinär aus den Perspektiven der Rechts- und Politikwissenschaft sowie der Informatik nach den Risiken für politische Entscheidungsprozesse, zu denen Deepfakes und ihre Nutzung für politische Desinformation führen können. Darauf basierend präsentiert der Beitrag Ansätze aus dem multidisziplinär ausgerichteten Forschungsprojekt FAKE-ID zur Erforschung KI-basierter Deepfake-Detektoren.

Lena Isabell Löber (Universität Kassel) untersucht die Möglichkeiten, die die KI bietet, um Dienstbetreiber bei der Erfüllung der gesetzlichen Pflichten zur Bekämpfung von Hasskriminalität im Netz zu unterstützen. KI-Lösungen können wirkungsvolle Instrumente sein, um schädlichen Inhalte und Manipulationstechniken wie Social Bots in sozialen Medien zu detektieren. Die mit ihrem Einsatz verbundenen Risiken für Kommunikationsgrundrechte und Meinungspluralität müssen aber durch manuelle Nachkontrollen automatisiert ermittelter Treffer und einen verfahrensorientierten Grundrechtsschutz eingehegt werden. Außerdem hält die Autorin schärfere Transparenzvorgaben und Aufsichtsstrukturen für erforderlich, um den Risiken der technisch-organisatorischen Gestaltungs- und

Entscheidungsmacht großer Anbieter von sozialen Netzwerken z. B. im Rahmen der algorithmischen Empfehlungssysteme zu begegnen. Betrachtet werden zu diesem Zweck die neuen Regelungen im Medienstaatsvertrag und Netzwerkdurchsetzungsgesetz, die zu mehr Transparenz für die Betroffenen führen sollten, aber gerade beim Themenkomplex Desinformation weitestgehend vage bleiben. Dem gegenübergestellt werden die auf EU-Ebene im Rahmen der Entwürfe für die KI-Verordnung und den Digital Services Act vorgesehenen Regelungen, die auch weitergehende Pflichten vorsehen und einen wichtigen Beitrag zu einem ganzheitlichen Ansatz im Umgang mit digitaler Desinformation leisten könnten.

Das Kapitel von *Nicole Krämer* (Universität Duisburg-Essen) und Kolleginnen und Kollegen diskutiert schließlich aus interdisziplinärer Perspektive die Probleme von Desinformation über Messengerdienste. Aus Sicht der Informatik, Journalistik, Medienpsychologie und Rechtswissenschaften werden jeweils der Stand der Forschung zur Fragestellung und zur Lösung durch denkbare Werkzeuge dargestellt, eigene Ansätze und Beiträge diskutiert und Fragestellungen herausgearbeitet, die als Grundlage für eine gemeinsame Forschung dienen können. So entsteht ein Überblick über die zahlreichen Perspektiven, mit denen an die Thematik herangegangen werden kann. Basierend darauf werden exemplarisch die Einflüsse datenschutzrechtlicher Projektentscheidungen auf die Projektarbeit diskutiert.

Einsatz von KI in Gesundheit und Pflege

Im abschließenden Teil V des Bandes werden in zwei Kapiteln Beispiele des Einsatzes von KI im Bereich von Gesundheit und Pflege genauer beleuchtet, also aus einem Bereich, wo sowohl die Erwartung an das Gemeinwohl aber auch die potenziellen Risiken für den Einzelnen am höchsten sind.

Roger von Laufenberg (Wiener Zentrum für sozialwissenschaftliche Sicherheitsforschung) betrachtet KI-Systeme in Pflegeeinrichtungen für ältere Menschen. Die Technisierung der Pflege sei vor allem eine Reaktion auf die alternde Bevölkerung und der damit einhergehenden Pflegekrise. Während dies in der Theorie durchaus erfolgversprechend scheint, beschreibt der Beitrag anhand einem Fallbeispiels (Sturzdetektion), dass die Entwicklung von KI-Pflegetechnologien häufig von der alltäglichen Lebensrealität älterer Personen entkoppelt ist. Dabei wird einerseits deutlich, wie in den unterschiedlichen Schritten in der Systementwicklung ein Bild von älteren Personen gezeichnet wird, das von Vulnerabilität geprägt ist. Andererseits erhielten ältere Personen als direkt Betroffene keine Möglichkeit, ihre

Sichtweisen in die Entwicklung und Implementierung mit einzubringen. Dadurch entstünden KI-Systeme, die den Anspruch von Fürsorge für ältere Menschen haben, dazu aber auf umfassende Überwachung ausgelegt sind und mögliche Risiken und negative Auswirkungen für Privatheit und Selbstbestimmung häufig ausblenden.

Im abschließenden Kapitel analysieren *Niël H. Conradie* (RWTH Aachen) und Kolleginnen und Kollegen, welche Auswirkungen intelligente Wearables – mit Bio-Sensoren ausgestattete kleine Computersysteme, die direkt am Körper getragen werden – auf die Entscheidungsfreiheit von schutzbedürftigen Personen haben. Der Markt für Wearables boomt seit einige Jahren und ist immer noch ein weitgehend unreguliertes Experimentierfeld für mehr oder weniger sinnvolle Anwendungen. Wie bei den meisten neu aufkommenden Technologien müssen die Vorteile und Risiken bewertet und gegeneinander abgewogen werden. Besonders wichtig ist diese Abwägung, wenn es sich um Anwendungen handelt, die schutzbedürftige Personengruppen betreffen, da diese oft und in besonderem Maße von Verletzungen der Selbstbestimmung betroffen sind. Dieser Beitrag untersucht aus einer explizit normativen und ethischen Perspektive die potenziellen Auswirkungen von Smart Wearables auf die Autonomie der Entscheidungsfindung in drei solchen Gruppen, nämlich: Kinder, ältere Erwachsene und Personen mit nicht altersbedingten Autonomieeinschränkungen.